Sistema de Gestión de Seguridad de la Información con estándares ISO/IEC 27001 y MAGERIT en la empresa SP Sistemas Palacios Ltda de la ciudad de Pasto.

Andrés Alejandro Ibarra Bolaños
Cesar Augusto Narváez Hernández

Universidad Mariana
Facultad de Ingeniería
Programa de Ingeniería de Sistemas
San juan de Pasto
2023

Sistema de Gestión de Seguridad de la Información con estándares ISO/IEC 27001 y MAGERIT en la empresa SP Sistemas Palacios Ltda de la ciudad de Pasto.

Andrés Alejandro Ibarra Bolaños
Cesar Augusto Narváez Hernández

Informe de investigación para optar al título de: Ingeniero de Sistemas

Asesor
MSc. José Javier Villalba Romero

Universidad Mariana
Facultad de Ingeniería
Programa de Ingeniería de Sistemas
San Juan de Pasto
2023

Artículo 71: los conceptos, afirmaciones y opiniones emitidos en el Trabajo de Grado son responsabilidad única y exclusiva del (los) Educando (s)

Reglamento de Investigaciones y Publicaciones, 2007
Universidad Mariana

Dedicatoria

Queremos dedicar este trabajo a nuestros padres, a nuestros hermanos quienes siempre nos han brindado su apoyo incondicional y sacrificio a lo largo de este arduo camino. Su constante aliento y confianza han sido nuestro principal motor para alcanzar este logro.

También dedicamos este trabajo a nuestros amigos y seres queridos, quienes han estado a nuestro lado en cada etapa de nuestra formación académica, brindándonos momentos de alegría, distracción y comprensión.

Agradecemos profundamente a nuestros profesores y mentores, cuya sabiduría y guía han sido fundamentales para nuestro crecimiento intelectual y profesional. Su paciencia y dedicación han dejado una huella imborrable en nuestro desarrollo.

Finalmente, dedicamos este trabajo a todas aquellas personas que luchan por la búsqueda del conocimiento y la mejora de nuestra sociedad. Que este trabajo contribuya de alguna manera al avance y bienestar de nuestra comunidad.

Andrés Alejandro Ibarra Bolaños
Cesar Augusto Narváez Hernández

Agradecimientos

Queremos expresar nuestro profundo agradecimiento a todas las personas que han contribuido de manera significativa en la realización de este trabajo. Sus aportes y apoyo han sido fundamentales para llevar a cabo este proyecto de investigación.

En primer lugar, agradecemos a nuestro asesor de tesis, Msc. José Javier Villalba Romero, por su orientación experta, paciencia y dedicación a lo largo de este proceso. Sus valiosos consejos y conocimientos han sido el faro que nos ha guiado en cada etapa.

Extendemos nuestro agradecimiento a nuestros profesores, quienes han enriquecido nuestras discusiones y aportando diferentes perspectivas a nuestro trabajo. Sus críticas constructivas nos han ayudado a mejorar y refinar nuestras ideas.

Nuestro agradecimiento también se dirige a nuestras familias y amigos, quienes han sido un constante soporte emocional en esta travesía. Sus palabras de aliento y comprensión nos han impulsado a seguir adelante, incluso en los momentos más desafiantes.

Agradecemos a la Universidad Mariana por brindarnos los recursos y facilidades necesarios para llevar a cabo nuestra investigación. Su entorno académico ha sido un ambiente propicio para el aprendizaje y el crecimiento.

Finalmente, queremos expresar nuestro reconocimiento a todas las fuentes bibliográficas y académicas que hemos consultado a lo largo de esta investigación. Sus contribuciones han enriquecido nuestra comprensión del tema y han sustentado nuestras conclusiones.

Con gratitud sincera,

Andrés Alejandro Ibarra Bolaños
Cesar Augusto Narváez Hernández

Contenido

Índice de Tablas

Índice de Figuras

Introducción

La información es uno de los activos más importantes en una organización según Martínez (2013), el valor real de esa información depende de cómo es gestionada, por tal razón en la época del conocimiento, comunicación y tecnología actual es de vital importancia contar con un sistema de seguridad adecuado para evitar que la información de las empresas sea vulnerada. Ante este panorama la Empresa SP Sistemas Palacios Ltda. No es ajena a esta situación, debido a que maneja información relevante y la afectación de la misma genera riesgos para la empresa.

Por consiguiente, esta investigación tiene como finalidad proponer un Sistema de Gestión de Seguridad de la Información bajo el estándar ISO/IEC 27001 en la empresa SP Sistemas Palacios Ltda., la cual parte con la realización de un diagnóstico de la seguridad informática en la organización mediante el uso de estándares que permiten determinar la vulnerabilidad y amenazas que afectan la disponibilidad, integridad, confidencialidad, autenticidad de la información que tiene la empresa, para así elaborar planes de mejoramiento que redunden en un mejor servicio de sus clientes tanto internos como externos. Lo que nos lleva a la pregunta ¿Cómo garantizar la seguridad de la información en la empresa SP Sistemas Palacios LTDA de la ciudad de Pasto para mejorar su gestión informática? Para lo cual se opta implementar un Sistema de Gestión de Seguridad de la Información SGSI con estándares ISO/IEC 27001 y MAGERIT que permita garantizar la seguridad de la información en la empresa SP Sistemas Palacios Ltda de la ciudad de Pasto.

Teniendo como objetivos analizar y describir el proceso de gestión de la información e incluir un inventario de activos el cual es la base para implementar la metodología MAGERIT la cual permite identificar amenazas, riesgos y vulnerabilidades y estas se clasifican en tablas para comprender que tan frecuente puede ser una amenaza, para ya una vez concluido se obtiene la propuesta estructurada del SGSI aprovechando la creciente preocupación por la fuga de información y la importancia de salvaguardar los activos de información han llevado a la necesidad de proponer un Sistema de Gestión de Seguridad de la Información basado en ISO/IEC 27001 en la empresa SP Sistemas Palacios Ltda. Esto permitirá implementar controles de seguridad para minimizar riesgos, siguiendo las directrices del Ministerio de Tecnologías de la

Información y las Comunicaciones (MINITIC) de Colombia. La investigación contribuirá a proteger la información confidencial. Enfocado en el Sistema de Gestión de Seguridad de la Información (SGSI) bajo ISO/IEC 27001 y su importancia. Se explora la seguridad informática, sistemas de información, pilares de seguridad de la información y métodos de gestión de riesgos, incluyendo MAGERIT.

La importancia y centralidad del tema de la seguridad de la información se reflejan en la creciente atención que ha recibido en investigaciones previas. Trabajos anteriores han destacado la necesidad de proteger la información en las organizaciones, especialmente en un mundo cada vez más interconectado y digitalizado. Investigaciones han demostrado que la falta de seguridad de la información puede resultar en pérdidas financieras significativas, daño a la reputación de la empresa y problemas legales. Para una comprensión clara del tema, es esencial definir los conceptos clave. En este contexto, la seguridad de la información se refiere a la protección de la disponibilidad, integridad, confidencialidad y autenticidad de los datos y sistemas de una organización. El Sistema de Gestión de Seguridad de la Información (SGSI) se refiere a un enfoque integral para gestionar la seguridad de la información en una organización, incluyendo políticas, procesos y controles.

La Empresa SP Sistemas Palacios Ltda. ha enfrentado problemas relacionados con la seguridad de los datos de sus clientes. En ocasiones, se ha evidenciado la pérdida o la falta de integridad en estos datos, lo que plantea riesgos significativos para la empresa. Esta situación subraya la necesidad de implementar un SGSI efectivo basado en la norma ISO/IEC 27001. La motivación detrás de esta investigación radica en la importancia de garantizar la seguridad de la información en un entorno empresarial altamente competitivo y tecnológicamente avanzado. La protección de los activos de información y la mitigación de los riesgos de seguridad son imperativos para mantener la confianza de los clientes y asegurar la continuidad de los negocios.

El resultado relevante esperado de esta investigación es la propuesta de un SGSI basado en la norma ISO/IEC 27001 para la Empresa SP Sistemas Palacios Ltda. Este sistema se basará en un diagnóstico exhaustivo de la seguridad informática en la organización y proporcionará planes de mejora específicos para abordar las vulnerabilidades y amenazas identificadas. Se espera que este

resultado tenga un impacto positivo en la seguridad de la información de la empresa y en su capacidad para satisfacer las expectativas de sus clientes.

Este documento se estructura en dos capítulos, siendo el primero, "Elementos del Proceso Investigativo". Este capítulo está dividido en subcapítulos que definen sistemáticamente los aspectos clave de la investigación. En primer lugar, se abordan los antecedentes internacionales, nacionales y regionales relacionados con el tema de investigación. A continuación, se presenta el título de la investigación, seguido de una descripción detallada del problema de investigación y su formulación. Además, se justifica la relevancia de la investigación. Para guiar el estudio de manera efectiva, se establecen objetivos específicos. Finalmente, se proporciona un marco teórico que respalda el proyecto, y se detalla la metodología que se seguirá, incluyendo el paradigma, el enfoque de investigación, la población y muestra, y las técnicas e instrumentos de recolección y procesamiento de información que se utilizarán.

El segundo capítulo, "Resultados", presenta hallazgos significativos de la investigación. Se comienza explorando la gestión de la información en el entorno organizacional de SP Sistemas Palacios Ltda. Este análisis se divide en áreas funcionales, como Administrativa y Financiera, Operaciones, Contact Center, Ingeniería y Gestión, Producto y Servicio, Talento Humano y Proyectos TI, y se incluye una clasificación de activos relevante. Luego, se evalúan amenazas, riesgos y vulnerabilidades utilizando el estándar MAGERIT, con una valoración de amenazas, identificación de vulnerabilidades y análisis de riesgos por activo y área administrativa. La propuesta de un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en ISO/IEC 27001 es otro componente esencial de los resultados. Esto incluye un resumen ejecutivo, objetivos, alcance de la propuesta, pasos en la evaluación y gestión de riesgos, análisis de riesgos y acciones de mitigación, implementación del Ciclo PHVA, principios del SGSI, planteamiento de objetivos de control, controles de seguridad y definición de políticas, estándares y procedimientos. Además, se describen los roles y responsabilidades en el SGSI y se propone un plan de socialización y capacitación.

1. Elementos del proceso investigativo

1.1 Antecedentes y estado del conocimiento

Atendiendo a la temática de investigación, se presenta una revisión de la literatura en la que se da constancia de investigaciones previas que abordan el Sistema de Gestión de Seguridad de la Información con estándar ISO/IEC 27001 su impacto en las empresas tanto a nivel regional y nacional como internacional.

A nivel internacional se encuentra la investigación sobre una "Propuesta de diseño de un Sistema de Gestión de la Seguridad de la Información según la NTP ISO/IEC 27001:2014 para la Universidad del Pacífico en el Perú", realizada por Vargas y Marchan (2019), quienes realizan este trabajo con la finalidad de proponer un diseño de un Sistema de Gestión de la Seguridad de la Información para la Universidad del Pacífico, el cual permitirá a dicha organización tener un estándar de seguridad a nivel mundial que esté alineada a la Norma Técnica ISO/IEC 27001:2014. Se diseñó la fase de planificación de esta norma, el cual permitió a la organización conocerse cómo se encuentra en la actualidad con respecto a los controles de la ISO/IEC 27002 y conocer cuáles son los riesgos a los que está expuesto con la finalidad de preservar la confidencialidad, integridad y disponibilidad de los activos de información. Para el desarrollo de esta propuesta se realizaron entrevistas, y observaciones con la finalidad de realizar una Auditoría inicial y así cumplir con la cláusula 4 de la norma el cual nos define el contexto de la organización. Con ello, se identificó la problemática y se definió el alcance de la investigación.

Esta investigación sirve de aporte al presente trabajo por medio de la propuesta que hacen los investigadores de unas plantillas que usaron para el diseño del SGSI el cual contiene política de seguridad, roles y responsabilidades, también se propuso políticas de seguridad que se orientaron a cinco controles de la ISO/IEC 27002 las cuales permitieron a la universidad atacar la problemática identificada.

También se relaciona el "Desarrollo de una propuesta de implementación de la ISO/IEC 27001, Sistema de Gestión de Seguridad de la Información, para la oficina funcional de

informática del gobierno regional Cusco" realizado por Ariasca y Quispe (2017), quienes realizan un análisis a la Oficina Funcional de Informática del Gobierno Regional del Cusco y evidencian que no cuenta con la implementación de controles eficientes, normas y estándares relacionados a seguridad de la información, siendo la información su activo más importante. Por tanto en respuesta a este problema se desarrolla las etapas de diseño y planificación de un Sistema de Gestión de Seguridad de la Información alineado a las especificaciones y requisitos de la NTP ISO/IEC 27001:2014, adaptando este proceso al contexto de la Oficina Funcional de Informática; para lo cual se adquirió y utilizó la NTP ISO/IEC 27001:2014 para su revisión e interpretación, logrando así identificar los procesos claves de las etapas de desarrollo del proyecto, las cuales son: Organización, Planificación, Despliegue, Revisión y Consolidación.

En este trabajo se puede identificar los procesos y actividades a llevarse a cabo en cada etapa del desarrollo del proyecto el cual es alineado a la metodología PHVA (Planificar, Hacer, Verificar y Actuar) y se puede identificar en el trabajo la documentación de los entregables que son exigidos en la norma.

Ahora bien, a nivel nacional se identifica un artículo sobre "Modelo Sistema de Gestión de Seguridad de la Información para instituciones educativas de nivel básico" de la Universidad Tecnológica de Pereira, realizado por Blandón y Benavides (2018), en donde se realiza un análisis de riesgos con base en la norma ISO/IEC 27005 identificando los activos críticos del área de secretaría académica de las instituciones educativas de nivel básico y los riesgos asociados, para generar un plan de tratamiento de riesgos que permita proponer una declaración de aplicabilidad, así mismo analizar la normatividad del Ministerio de Educación, del MINTIC y los requisitos de la norma NTC ISO/IEC 27001 que permitan proponer un modelo general que facilite la implementación de un SGSI en este tipo de instituciones.

El aporte de esta investigación es el modelo resultante que cumple con los requisitos obligatorios establecidos en la norma NTC ISO/IEC 27001, y constituye una base para garantizar la disponibilidad, integridad y confidencialidad de la información sensible de los niños, cumpliendo las disposiciones pertinentes del sector educación, sector TIC componente seguridad y privacidad de la información y sirve como aporte a la implementación de este sistema para

cualquier empresa.

Así mismo se relaciona un artículo científico sobre una "Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27001 Universidad Nacional de Colombia" realizada por Valencia y Orozco (2017), quienes proponen una metodología de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la familia de normas de la ISO/IEC 27000, con énfasis en la interrelación de cuatro normas fundamentales a través de las cuales se desarrollan las actividades requeridas para cumplir con lo establecido en la ISO/IEC 27001, los controles de seguridad presentados en la ISO/ IEC 27002, el esquema de riesgos de la ISO/IEC 27005 y los pasos recomendados en la ISO/IEC 27003. El aporte de esta investigación es el proceso metodológico que da respuesta al cómo abordar un proyecto de este nivel de importancia en el contexto actual de las organizaciones y basado en estándares internacionales. También este proceso metodológico representa un aporte a los profesionales que emprenden esta labor, y que buscan un método para una implementación exitosa de un SGSI.

Se referencia la investigación sobre "Un diseño del Sistema de Gestión de Seguridad de la Información-SGSI-para el proceso análisis de laboratorio de físico química de suelos de la corporación colombiana de investigación agropecuaria Agrosavia de Bogotá basado en la norma ICONTEC NTC-ISO/IEC 2700" realizado por Ramos y Morales (2020), llevan a cabo un análisis e identifican posibles riesgos, amenazas, vulnerabilidades y controles que contribuyan a asegurar la integridad, confidencialidad y disponibilidad de la información en el laboratorio de físico química de suelos de la corporación colombiana de investigación agropecuaria, permitiendo al laboratorio la prestación de sus servicios de análisis con altos estándares de calidad y eficiencia, para seguir posicionándose como uno de los mejores laboratorios del país y de américa latina. En esta investigación se pudo evidenciar que una vez surtida las estrategias se definieron las políticas de seguridad de la información basados en los controles de la norma NTC-ISO/IEC 27001:2013. Estas políticas preservan la confidencialidad, integridad y disponibilidad de la información.

Por último, la investigación sobre "Un Diseño del Sistema de Gestión de Seguridad de la Información (SGSI) para el centro de datos de la personería de Bogotá DC bajo las normas NTC-

ISO-IEC 27001: 2013" realizado por Acosta y León (2017), este proyecto tiene como propósito formular un diseño del Sistema de Seguridad de la Información SGSI para el Centro de Datos de la Personería de Bogotá y así contribuir y garantizar la adecuada gestión de la seguridad en la entidad, ya que el centro de datos de la Personería de Bogotá se concentran los servidores, aplicativos y dispositivos críticos que soportan el eje funcional de la entidad; la no disponibilidad de los mismos, puede causar consecuencias graves para la imagen institucional y el cumplimiento de su misión. Esta investigación sirve de aporte ya que se puede identificar el desarrollo los resultados producto del desglose de las etapas de Planificación, Ejecución, Seguimiento y Mantenimiento y se formulan varias oportunidades de mejora, dentro de las cuales se destacan como estrategias de continuidad del proyecto el autodiagnóstico del cumplimiento de compromisos, identificación de riesgos y contratación de consultorías para realizar mediciones objetivas de la ejecución del sistema, tomando como metodología para el análisis de riesgos MAGERIT.

Finalmente, a nivel regional, se encuentra la investigación sobre "Estudio para la implementación del sistema de gestión de seguridad de la información para la Secretaria de Educación Departamental de Nariño basado en la norma ISO/IEC 27001" realizado por Aguirre y Zambrano (2015), realizan un diagnóstico de la seguridad informática en el área financiera de la Secretaría de Educación Departamental de Nariño dado el continuo desarrollo de la tecnología y del acceso a los diferentes canales de comunicación, se mira pertinente que la entidad pueda contar con una herramienta que le aporte a la toma de decisiones tendientes a ajustar o eliminar las falencias que se presentan tanto en el sistema que soporta los procesos como en el manejo mismo de la información al interior del área y de la entidad, para lograr este objetivo se plantea el funcionamiento del área financiera de la Secretaría de Educación Departamental de Nariño y su proceso Tesorería para verificar su estado actual respecto a los controles de la norma ISO/IEC 27001 y basados en ISO/IEC 27002, se elaboró el plan de Auditoría que incluye todos los aspectos auditables en cuanto a la seguridad informática, los recursos necesarios y el cronograma de actividades y pruebas a desarrollarse en el proceso de tesorería del área financiera de la Secretaría de Educación Departamental de Nariño y finalmente se elaboró el informe final de los resultados obtenidos en la Auditoría, para determinar los posibles controles que apliquen en cada caso y el tratamiento de los mismos que permitan mitigar las amenazas y riesgos encontrados.

También el trabajo sobre "Un Diseño de un Sistema de Gestión de Seguridad de la Información para la Ferretería Argentina de la ciudad de Pasto" realizado por Pérez y Jurado (2018), quienes buscan que los procedimientos que se llevan a cabo a diario mejoren conservando así la integridad, confidencialidad y disponibilidad de la información, lo cual permita mayor protección de la información y los procesos, para lo cual en sus principios se realiza un inventario de los activos informáticos, el cual permita evaluar cuáles son los más importes y el lugar que estos tiene dentro de la organización, posteriormente de cada activo informático se elige las variables que se desean evaluar, una vez seleccionadas las variables a evaluar se seleccionan los métodos de evaluación, las medidas y herramientas, se procede a realizar el análisis de los resultados y la implementación de los controles pertinentes que permiten corregir las vulnerabilidades y amenazas detectadas, este proceso se realiza a través de los SGSI de forma continua y progresiva lo que permitirá a la empresa tener una mejora en la infraestructura IT y su seguridad para así poder resguardar y dar un mejor manejo a la información.

Los antecedentes mencionados anteriormente, sirven de soporte teórico para el desarrollo de la presente investigación ya que guían a los investigadores en el uso de la norma NTC-ISOIEC 27001, que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información.

1.2 Título

Sistema de Gestión de Seguridad de la Información con estándares ISO/IEC 27001 y MAGERIT en la empresa SP Sistemas Palacios Ltda de la ciudad de Pasto.

1.3 Problema de investigación

1.3.1 Descripción del problema

Actualmente, gran parte de las empresas tienen muchos retos relacionados con la seguridad de información, debido al constante intercambio de información entre la empresa y sus clientes, aparecen riesgos potenciales que pueden comprometer el éxito e incluso la subsistencia de la

organización, así lo menciona Villamizar (2013), hoy en día la mayor cantidad de ataques de seguridad de la información provienen del interior de sus propias empresas, a veces por empleados descontentos o por fraude interno, acceso no autorizado, falta de motivación, ausencia de entrenamiento organizacional, entre otras. Así mismo, se ejecutan ataques a través de la ingeniería social, que vulneran los sistemas de seguridad y cifrado, convirtiendo los ataques a la seguridad de la información cada vez más frecuentes, donde se hace difícil defenderse, es por ello la importancia establecer el modelo de seguridad para prevenir fallas y fugas en los sistemas.

Ahora bien, según el Modelo de Seguridad de la Información MSI (Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia [Min TIC], s.f.), las políticas de privacidad y seguridad de la información salvaguardan a la misma de grandes amenazas, garantizando el equilibrio y continuidad de los sistemas de información, minimizando riesgos, evitando daños y permitiendo que las entidades cumplan sus objetivos. Ante este hecho se analiza que la empresa Nariñense SP Sistemas Palacios LTDA., en la actualidad no cuenta con un sistema que le permita gestionar la seguridad de la información en la organización, lo cual genera falta de confianza por parte de los clientes, así como riesgos ante ataque informáticos que pueden afectar la disponibilidad, integridad y privacidad de los datos, tampoco la entidad ha definido políticas y estrategias que permitan mitigar la restauración de los sistemas, el control del personal, la seguridad de las instalaciones físicas y los accesos en un entorno de procesamiento de datos. Actualmente se ha tratado de mitigar el problema usando diferentes acciones, pero sin optar por un sistema concreto en la gestión de la seguridad de la información generando altos riesgos en la seguridad de la información. Ante este panorama es indispensable para la empresa un sistema de gestión de la información, ya que es el único medio que les ayudara a disminuir las amenazas, así lo explica El Ministerios Nacional de las Tecnologías de la información y las Comunicaciones (Min TIC, 2008):

El Sistema de Gestión de la Seguridad de Información SGSI, ayuda a gestionar de forma eficaz la seguridad de la información, evitando las acciones innecesarias, ineficientes o mal dirigidas que se producen por contrarrestar amenazas sin una evaluación previa, por desestimar riesgos, por la falta de contramedidas, por implantar controles desproporcionados y de un costo más elevado del necesario, por el retraso en las medidas de seguridad en relación con la dinámica

de cambio interno de la propia organización y del entorno.

Es precisamente esa falta de medidas en implementar controles de seguridad que ha generado en muchas ocasiones perdida de información importante para la empresa y aunque SP Sistemas Palacios Ltda posee recursos tecnológicos, según su gerente presenta problemas entre los que se destaca la inexistencia de procesos sobre gestión de la información, gestión de los recursos físicos, gestión de políticas de seguridad, manejo de inventarios, control de equipos y además no posee un mapa de análisis de riesgos y controles de los mismos, no cuenta con un sistema de gestión de incidentes de seguridad de la información que ha dejado la información con pocas medidas de confidencialidad inclusive dentro de la misma empresa.

1.3.2 Formulación del problema

¿Cómo garantizar la seguridad de la información en la empresa SP Sistemas Palacios Ltda de la ciudad de Pasto para mejorar su gestión informática?

1.4 Objetivos

1.4.1 Objetivo general

Implementar un Sistema de Gestión de Seguridad de la Información SGSI con estándares ISO/IEC 27001 y MAGERIT que permita garantizar la seguridad de la información en la empresa SP Sistemas Palacios Ltda de la ciudad de Pasto.

1.4.2 Objetivos específicos

- Describir el proceso de gestión de información en el entorno organizacional de SP Sistemas Palacios LTDA.

- Identificar amenazas, riesgos y vulnerabilidades a la información de la empresa SP Sistemas Palacios Ltda con el estándar MAGERIT.

- Estructurar la propuesta del Sistema de Gestión de la Seguridad de la Información SGSI para la empresa SP Sistemas Palacios Ltda basado en el estándar ISO/IEC 27001.

1.5 Justificación

Los riesgos en la fuga de información es un problema que ha venido tomando fuerza en los últimos tiempos, por esa razón para toda empresa la información es el activo más importante que proteger, debido a esto se considera necesario para la empresa SP Sistemas Palacios LTDA proponer un Sistema de Gestión de la Seguridad de la Información basado en el estándar ISO/IEC 27001, por medio del cual se puede implementar procedimientos o controles de seguridad los cuales ayuden a las organizaciones a minimizar los riesgos en su trabajo diario. Así lo menciona Pacheco (2010), un sistema de seguridad de la información implica crear el plan de diseño, implementación, y mantenimiento de una serie de procesos que permiten gestionar de manera eficiente la información, para asegurar la integridad, confidencialidad, y disponibilidad de la misma, es decir que por medio de un SGSI se puede conseguir una mayor eficiencia y garantía en la protección de los activos de información.

Ahora bien, teniendo en cuenta que la legislación colombiana indica el deber de la protección de la información y los datos, empresas como SP Sistemas Palacios Ltda debe implementar el modelo del Sistema de Gestión de Seguridad de la Información, para salvaguardar los activos informáticos, tal como lo menciona el Ministerio de Tecnologías de la Información y las Comunicaciones Min TIC bajo la resolución 00500 del 2021 “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital” (p. 12), donde se describe la gestión del riesgo de información y los objetivos de la seguridad de la información como es la confidencialidad, integridad y disponibilidad, de esta manera y a través de los controles que propone la norma la empresa podrá llegar a establecer el plan de tratamiento que se va a dar a los riesgos encontrados y el nivel de aceptación de riesgo que la empresa podrá asumir.

En este orden de ideas, se justifica esta investigación desde el punto de vista que será un aporte que beneficiará a la empresa, dado que, al encontrar los riesgos a los que se enfrenta la

empresa por falta de seguridad en la información, se podrán tomar controles para evitar que la información confidencial caiga en manos no deseadas que utilicen esta información inadecuadamente, causando demandas y pérdidas financieras que afecten directamente el buen nombre de la organización. Esta investigación también ayuda a afianzar el desarrollo profesional e intelectual de los estudiantes de ingeniería que realizan esta propuesta; de este modo se aplica el conocimiento adquirido durante todo el proceso educativo demostrando en el proceso las aptitudes y experiencia que se ha forjado a lo largo del aprendizaje recibido por parte de los docentes de la Universidad Mariana de la ciudad de Pasto.

1.6 Marcos de referencia

1.6.1 Marco teórico - conceptual

En esta investigación se tomará como referentes algunas teorías planteadas que explican claramente el tema de estudio, para lograr esto, se tendrá en cuenta las categorías y subcategorías de investigación planteadas según los objetivos propuestos.

Sistema de Gestión de Seguridad de la Información: partiendo de esta descripción: es importante iniciar el análisis con lo referente al SGSI, la cual según el portal ISO27000 es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos comerciales y/o de servicio. El alcance de un SGSI está en función de dónde se identifiquen y ubiquen los activos de información esenciales. Actualmente el ISO-27001 es el único estándar aceptado internacionalmente (Certificable) para la administración de la seguridad de la información y aplica a todo tipo de organizaciones, tanto por su tamaño como por su actividad.

Objetivos de la Norma ISO/IEC 27001: la norma se centra en permitir a la dirección monitorear, evaluar, asignar y gestionar los recursos necesarios para la seguridad de la información, por medio de la implementación de los siguientes objetivos según Normatividad Icontec (Norma ISO/IEC 27001, 2005).

Políticas de seguridad: deben existir reglas y procedimientos para que los usuarios puedan acceder a los recursos de la organización, para prevenir, proteger y manejar los riesgos.

Organización de la seguridad de la información: orientada a administrar la seguridad de la información dentro de la empresa y establecer un marco gerencial para controlar su implementación, así como para la distribución de funciones y responsabilidades.

Gestión de activos: la gestión o administración de activos está destinada a mantener una adecuada clasificación y protección de los activos del organismo, en esta también se clasifica la información para señalar su sensibilidad y criticidad.

Seguridad de los recursos humanos: orientado a reducir los riesgos de error humano, robo, fraude, o uso inadecuado de las instalaciones, además de definiciones de puestos de trabajo y asignación de recursos. La seguridad de los recursos humanos también debe garantizar que los usuarios estén al tanto de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la política de seguridad de la información de la organización en el transcurso de sus tareas normales.

Seguridad física y del entorno: destinada a impedir accesos no autorizados, daños e interferencia a las dependencias e información de la organización. Proteger el equipamiento de procesamiento de información crítica del organismo ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados.

Estructura del SGSI: la estructura del SGSI se basa bajo el modelo de procesos "Planear-Hacer-Verificar-Actuar". "Esta norma adopta el modelo de procesos "Planear-Hacer-Verificar-Actuar" (PHVA) que se aplica para estructurar los procesos del SGSI" (Buitrago et al., 2012).

La adopción del modelo PHVA refleja los principios establecidos en las directrices OCDE para la seguridad de sistemas y redes de información, esta norma brinda un modelo robusto para implementar los principios en aquellas directrices que controlan la evaluación de riesgos, diseño

e implementación de la seguridad, gestión y reevaluación de la seguridad.

Seguridad Informática: Ante este contexto es importante conocer sobre la seguridad de la información, la cual según el autor Gómez (2015) la define como como:

> Cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema (p. 14).

Es decir que este se considera un activo que requiere protección adecuada, pues el principal activo que poseen todas las organizaciones y con los avances de la tecnología, este es una herramienta que otorga grandes ventajas competitivas, sin embargo, Peñuela (2018), explica que en los últimos tiempos existen nuevas vulnerabilidades que traen aparejadas graves consecuencias, es por ello la seguridad informática tiene un papel tan importante en las organizaciones.

Sistemas de Información: los sistemas de información son analizados desde varios puntos de vista ya que existen antes de la creación de la tecnología de computación, pues tiene que ver con todo un conjunto organizacional de las empresas, así lo mencionan Laudon y Laudon (2012), desde una perspectiva de negocios, un sistema de información es una solución organizacional y administrativa basada en tecnología de información para resolver problemas y desafíos del entorno. Estos autores explican que existe tres dimensiones que le dan forma a los sistemas y permiten que los mismos funcionen efectivamente y generen valor. Estas dimensiones son:

- **Organización:** comprende al personal, estructura, procedimientos, cultura y políticas empresariales. Los sistemas de información forman parte de las organizaciones.

- **Administración**: comprende la planificación, asignación de recursos financieros y humanos, el establecimiento de estrategias para resolver los desafíos de negocio en el entorno, y la coordinación del trabajo para alcanzar el éxito.

- **Tecnología**: comprende el hardware, software, tecnología de almacenamiento de datos y tecnología de redes y telecomunicaciones. Todos estos elementos, junto con las personas que los operan y administran, constituyen la infraestructura de tecnología de información.

Según los autores, las organizaciones actuales utilizan sistemas informáticos basados en tecnología de la información para realizar sus actividades, lo que permite alcanzar los objetivos y metas estratégicas.

Componentes de un sistema de Información: ahora bien, en el mismo libro de Sistemas de Información Gerencial por los hermanos Laudon, un sistema de información es un conjunto de componentes interrelacionados cuyo objeto es la recolección de datos, su procesamiento y almacenamiento, y la distribución de información para la toma de decisiones y para el control organizacional. Está compuesto por tres actividades: entrada, proceso y salida.

- Entrada: donde se captura el elemento primario del sistema de información que es el dato. Los datos recolectados pueden ser internos o externos a la organización.

- Proceso: donde los datos se combinan con otros elementos y se vuelven significativos a través de su contextualización, de acuerdo con lo que sucede en la organización.

- Salida: donde se obtiene la información útil y significativa para las personas

Revisando los conceptos anteriores se observa que la empresa SP Sistemas Palacios Ltda emplea en su gestión empresarial diversos sistemas que le permiten capturar datos, procesarlos, almacenarlos y obtener información para la toma de decisiones y realización de sus actividades y que puede ser protegida ante amenazas y vulnerabilidades que permitan garantizar su seguridad.

Pilares de la seguridad de la Información: siendo la información uno de los activos más importantes del negocio, ya que conecta a cada una de las áreas, unifica procesos y guía tanto las operaciones como la productividad, según Vásquez (2022), este sistema cuenta con tres pilares de la seguridad de la información:

- **Confidencialidad**: Consiste en asegurar que solo el personal autorizado acceda a la información que le corresponde, para evitar que la información sea divulgada por personas o sistemas no autorizados.

- **Integridad**: Hace referencia a la cualidad de la información para ser correcta, es decir, que se mantengan los datos reales para los cuales fueron generados, sin haber sido modificados ilegalmente por terceros.

- **Disponibilidad**: Significa que los datos estén disponibles en el momento en el que se necesita acceder a ellos.

Administración de Riesgos: la administración de riesgos, según el Departamento Nacional de Planeación (DNP, 2016), es el proceso continuo, basado en el conocimiento, evaluación, manejo de los riesgos y sus impactos que mejora la toma de decisiones organizacionales. Es entonces el conjunto de pasos secuenciales, lógicos y sistemáticos que debe seguir el analista de riesgos para identificar, valorar y manejar los riesgos asociados a los procesos de la Organización, los cuales ejecutados en forma organizada le permiten encontrar soluciones reales a los riesgos detectados minimizando las pérdidas o maximizando las oportunidades.

Análisis de riesgos: el mismo documento explica que el análisis de riesgo es el estudio de las causas de las posibles amenazas y, los daños y consecuencias que éstas puedan producir. Este tipo de análisis es ampliamente utilizado como herramienta de gestión en estudios financieros y de seguridad para identificar riesgos (métodos cualitativos) y otras para evaluar riesgos (generalmente de naturaleza cuantitativa). El primer paso del análisis es identificar los activos a proteger o evaluar. La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo establecidos previamente, Con los resultados obtenido del análisis se podrá aplicar métodos para el tratamiento de los riesgos, que involucra identificar el conjunto de opciones que existen para tratar los riesgos, evaluarlas, preparar planes para este tratamiento y ejecutarlos (DNP, 2016).

Evaluación de riesgos: con la evaluación de riesgos se podrá comparar el nivel de riesgo

encontrado durante el proceso de análisis contra el criterio de riesgo establecido previamente, y decidir si los riesgos pueden ser aceptados. El análisis de riesgos y los criterios contra los cuales los riesgos son comparados en la valoración deben ser considerados sobre la misma base. Así, evaluaciones cualitativas incluyen la comparación de un nivel cualitativo de riesgo contra criterios cualitativos, y evaluaciones cuantitativas involucran la comparación de niveles estimados de riesgo contra criterios que pueden ser expresados como números específicos, tales como fatalidad, frecuencia o valores monetarios (DNP, 2016).

Gestión de riesgos: se realiza por medio de un enfoque estructurado para manejar la incertidumbre a una amenaza, a través de una secuencia de actividades que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular (DNP, 2016).

Metodología MAGERIT: esta es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, en el Portal de Administración Electrónica MAGERIT los responsables del proyecto Amutio y Candau (2012), explican que esta metodología es un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para de esta forma implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados. Además de esto, cuenta con todo un documento que reúne técnicas y ejemplos de cómo realizar el análisis de riesgos, según los autores los objetivos son los siguientes:

- Concientizar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.

- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).

- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo

control Indirectos.

- Preparar a la Organización para procesos de evaluación, Auditoría, certificación o acreditación, según corresponda en cada caso.

El análisis de estos ejes teóricos sirve para soportar por medio de referencias bibliográficas el tema objeto de estudio, con el fin de conocer de una forma más clara y precisa el tema en relación al Sistema de Gestión de Seguridad de la Información con estándares ISO/IEC 27001.

1.6.2 Marco legal

Para la presente investigación tomará y adoptará las leyes que rigen y orientan a los investigadores entre las que se encuentran:

Ley 527 de 1999 "Por medio de la cual se define y reglamenta el accegso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales" Artículo 6º. cualquier norma que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta. Esta ley servirá de soporte para esta investigación en cuanto al requisito establecido en esta norma y que constituye una obligación, en el caso de que la información conste por escrito (Ley 527, 1999).

Ley 599 de 2000 Por la cual se expide el Código Penal. Título VII. De la protección de la Información y de los Datos. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa Esta ley servirá de soporte para esta investigación en cuanto a la protección de los derechos de autor y las conductas relacionadas indirectamente con los delitos informáticos (Ley 599, 2000).

Ley 1341 de 2009 Por la cual se definen principios y conceptos sobre la sociedad de la

información y la organización de las Tecnologías de la Información y las Comunicaciones (TIC), se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

Artículo 1o. Objeto**.** La presente ley determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información.

Esta ley servirá de soporte para comprender los principios, conceptos y competencias sobre la organización de las tecnologías de información que son de interés general para las empresas (Ley 1341, 2009).

Ley 1712 2014 "Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones".

Artículo 1. Objeto**.** El objeto de la presente ley es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.

En este sentido esta ley establece los procedimientos para acceder a información y las garantías que tienen las personas para que se publique información de forma proactiva y con transparencia (Ley 1712, 2014).

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado "de la protección de la información y los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones,

entre otras disposiciones

Capitulo I. De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. Esta ley describe los delitos informáticos como una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que empresas como SP Sistemas Palacios Ltda se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales (Ley 1273, 2009).

Decreto 2578 de 2012 "Por el cual se reglamenta el Sistema Nacional de Archivos, se establece la red nacional de archivos, se deroga el decreto 2124 de 2004, y se dictan otras disposiciones relativas a la administración de los archivos del Estado". Que el fin esencial del Sistema Nacional de Archivos es la articulación, la modernización y la homogeneización metodológica de la función archivística del Estado y de los archivos de las entidades públicas en los diferentes niveles de la organización administrativa, territorial y por servicios. Por medio de este decreto se puede identificar la importancia de los procesos archivísticos y el manejo correcto que se debe tener como centros de información e instrumentos de transparencia y lucha contra la corrupción (Decreto 2578, 2012).

1.6.3 Marco contextual

Esta investigación se realizará en una empresa de la ciudad de Pasto llamada SP Sistemas Palacios LTDA que es es una ISP proveedora del servicio de Internet en el Departamento de Nariño, con una sola sede en la ciudad de Pasto y con más de 15 años de experiencia en el sector telecomunicaciones entregando conectividad residencial y corporativo con servicios de valor agregado; brinda servicios óptimos y con calidad para la satisfacción los clientes, contribuyendo así al crecimiento sustentable de la empresa, volviéndola económicamente próspera, comprometida con el desarrollo de su personal y de la comunidad.

Esta empresa se enfoca principalmente las siguientes actividades:

- Prestación de servicio de telecomunicaciones.

- Prestación del servicio de valor agregado y telemático a nivel nacional y con conexión en el exterior.

- Venta de computadores y accesorios.

- Suministros para computador.

- Desarrollo de páginas web y software, montaje de redes y venta de accesorios para redes, asesoría y consultoría de sistemas.

Su estructura organizacional se compone de la siguiente planificación estratégica:

Misión: Empresa proveedora del servicio de Internet en el Departamento de Nariño, con más de 15 años de experiencia en el sector telecomunicaciones, ofreciendo conectividad residencial y corporativa con servicios de valor agregado. Se brinda servicios óptimos y con calidad para la satisfacción de los clientes, contribuyendo así al crecimiento sustentable de la empresa, volviéndola económicamente próspera y comprometida con el desarrollo de su personal y de la comunidad.

Visión: La empresa SP Sistemas Palacios Ltda pretende para el año 2025, ser una de las mejores empresas en el mercado de telecomunicaciones en el Departamento de Nariño y construir una red en fibra óptica con el más amplio cubrimiento de la región, con el propósito de llevar a nuestros clientes la mayor calidad y velocidad del mercado.

Objetivos Corporativos:

- Ofrecer paquetes de internet corporativo y domiciliario con transmisión de datos.

- Brindar a nuestros clientes un servicio de calidad de acuerdo al avance de la tecnología.

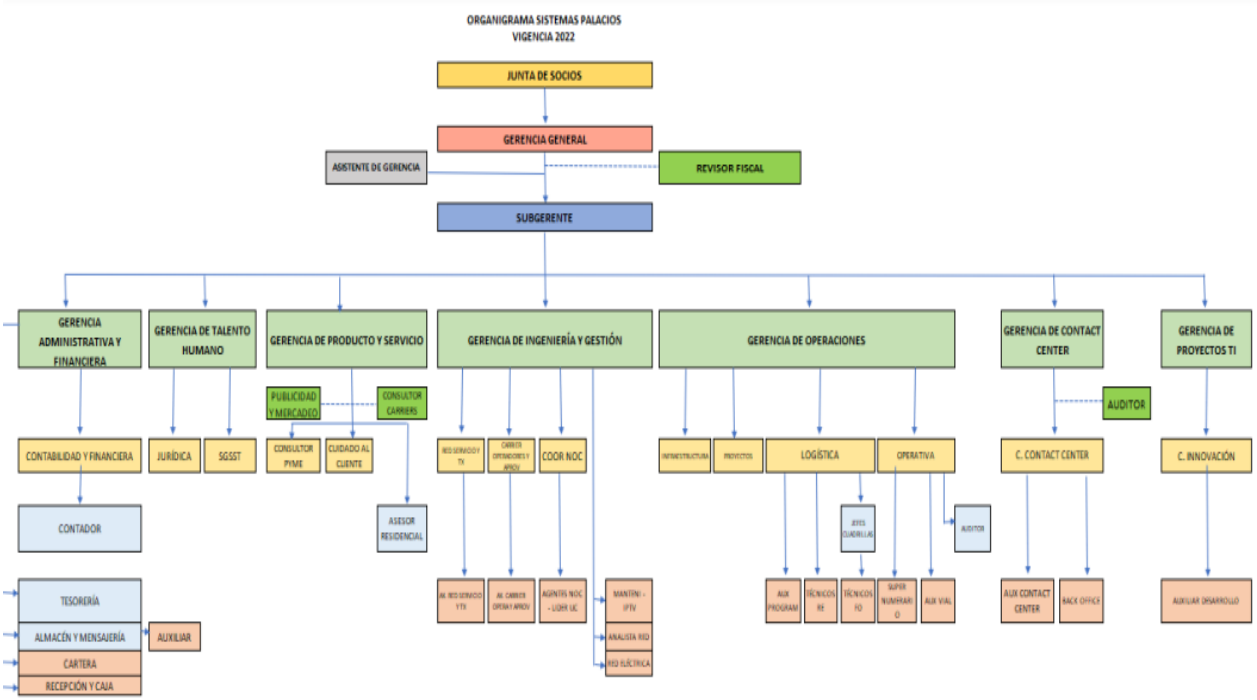
- Tener el mayor despliegue en fibra óptica, traducido en velocidad y disponibilidad del

servicio.

- Brindar una eficiente respuesta a nuestros usuarios para cualquier tipo de consulta de nivel domiciliario.

Figura 1

Organigrama



Fuente. Planificación Estratégica SP Sistemas Palacios LTDA.

Ubicación

SP Sistemas Palacios Ltda con número NIT 900163149-2, está ubicada en Pasto (Nariño, Colombia) en la Cl. 2 Sur #22-75 Barrio Bachue, Pasto, Nariño**.**

Figura 2

Instalaciones de SP Sistemas Palacios Ltda

1.7 Metodología

1.7.1 Paradigma, enfoque y tipo de investigación

El paradigma de investigación es cuantitativo, ya que busca recolectar, analizar, sintetizar mediante gráficos y estadísticas cada una de las áreas s funcionales de la empresa SP Sistemas Palacios Ltda de la ciudad de Pasto, según Hernández et al. (2014), la investigación cuantitativa tiene una gran amplitud de datos e interpretaciones que enriquecen el fin de la investigación. El alcance final del estudio cuantitativo consiste en implementar técnicas estadísticas que permitan comprobar las hipótesis formuladas. Por medio de este método se puede medir los resultados. Las características del paradigma cuantitativo de una investigación con paradigma cuantitativo son:

- Base epistemológica: Positivismo.
- Su énfasis: Medición objetiva, demostración de la causalidad
- En relación a la recogida de información: Estructurada y sistemática.
- Su análisis: Estadístico.

1.7.2 Enfoque

El enfoque de la investigación utilizado será empírico analítico, según Bungen (1981, como se citó en De La cruz, 2016), plantea que el enfoque empírico analítico trata de entender las situaciones en términos de las relaciones de sus componentes. Intenta descubrir los elementos que componen cada totalidad y las interconexiones que da cuenta de su integración. Es decir, en el tipo de investigación analítica, el resultado es la identificación de los aspectos ocultos a los que no puede llegarse con una mera descripción, que para el caso es determinar la importancia de un SGSI para la empresa SP Sistemas Palacios Ltda.

1.7.3 Tipo

Según Tamayo y Tamayo (2003), el de tipo descriptivo: "Comprende la descripción, registro, análisis e interpretación de la naturaleza actual, y la composición o proceso de los fenómenos. El enfoque se hace sobre conclusiones dominantes o sobre grupo de personas, grupo o cosas, se conduce o funciona en presente" (p. 35).

Es decir, en esta investigación se realizará una descripción de la situación actual frente a la falta de gestión de seguridad informática y la pertinencia de implementar un SGSI con estándares ISO/IEC 27001.

1.7.4 Técnica de investigación

La técnica utilizada en esta investigación fue la observación visual, donde se realizó una observación detallada del comportamiento del personal de la empresa. Durante el proceso se tomó nota de las actividades y procesos realizados por el personal, para posteriormente analizar y obtener conclusiones.

1.7.5 Línea y áreas temáticas de investigación

1.7.5.1 Línea de investigación. Ingeniería, informática y computación.

1.7.5.2 Áreas Temáticas de investigación. Tecnologías de información y comunicación TIC.

1.7.6 Población y muestra

1.7.6.1 Población. La población objeto de estudio de esta investigación será el personal que interactúan con el sistema de información de la empresa SP Sistemas Palacios Ltda de acuerdo con la infraestructura tecnológica.

1.7.6.2 Muestra. El proyecto usa un muestreo intencional por conveniencia. Según Requena (2022), el muestreo por conveniencia es una técnica de muestreo no probabilístico y no aleatorio utilizada para crear muestras de acuerdo a la facilidad de acceso, la disponibilidad de las personas de formar parte de la muestra, en un intervalo de tiempo dado o cualquier otra especificación práctica de un elemento particular.

Por lo tanto, se realizará una selección de empleados de acuerdo con el grado de experiencia y conocimiento en la empresa, para así obtener una información veraz y precisa, esta técnica es subjetiva ya que se encuentra sujeta al criterio de la persona que a través de su experiencia dentro de la empresa ayuda a seleccionar la muestra más indicada y representativa, este método es conveniente usar cuando la población no es muy grande como es el caso del proyecto.

1.7.7 Proceso de investigación

Tabla 1

Proceso de Investigación.

Objetivos específicos	Fuente	Técnica de recolección	Instrumento	Técnica de Procesamiento	Productos entregables
Describir el proceso de gestión de información en el entorno organizacional de SP Sistemas Palacios LTDA.	Áreas funcionales de la empresa.	Observación directa: Visitar las áreas funcionales y los procesos de información que serán objeto de estudio	Encuestas semiestructuradas	Análisis de la información	Informe del manejo de la información en áreas funcionales de la empresa.
Identificar amenazas, riesgos y vulnerabilidades a la información de la empresa SP Sistemas Palacios Ltda con el estándar MAGERIT	Recursos de la empresa a partir de la Infraestructura tecnológica de las áreas funcionales con las que cuenta la empresa.	Observación directa, encuesta.	Listas de chequeo y bitácoras de campo.	Análisis de datos de la información a través de matrices para el análisis de vulnerabilidades y riesgos.	Cuadros de análisis de amenazas, riesgos y vulnerabilidades definidas en MAGERIT.
Estructurar la propuesta del Sistema de Gestión de la Seguridad de la	NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA	Revisión documental por medio del análisis de la NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA	Bitácora de campo y matriz de vulnerabilidades	Análisis de la metodología y síntesis de resultados PHVA	Documento con propuesta del Sistema de Gestión de la Seguridad de

Objetivos específicos	Fuente	Técnica de recolección	Instrumento	Técnica de Procesamiento	Productos entregables
Información SGSI para la empresa SP Sistemas Palacios Ltda basado en el estándar ISO/IEC 27001.	27001	27001 - TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI).			la Información SGSI para la empresa SP Sistemas Palacios Ltda basado en el estándar ISO/IEC 27001

1.8 Presupuesto

Tabla 2

Presupuesto global

Rubros	**Total ($)**
Inversión en personal	$ 5.784.550
Otros rubros	$ 2.530.000
Total	$ 8.314.550

Tabla 3

Presupuesto en personal

Nombre Investigador	**Vr. Hora Investigador**	**Dedicación**	**Valor**
		Número total de horas	
José Javier Villalba Romero	$19.630	95	$ 1.864.850
Andrés Alejandro Ibarra Bolaños	$10.315	190	$ 1.959.850
Cesar Augusto Narváez Hernández	$10.315	190	$ 1.959.850
Total			$ 5.784.550
Vr. horas investigador Docente	4 SMLV/8		$ 19.630
Vr. horas investigador Estudiante	2 SMLV/8		$10.315

Tabla 4

Otros rubros

Rubro	**Justificación**	**Valor total**
Equipos	Depreciación de equipos	$ 500.000
Materiales	Material de oficina, resma de hojas, lapiceros, carpetas, grabadora, que servirá para realizar el diagnóstico.	$ 180.000

Rubro	**Justificación**	**Valor total**
Acceso y servicio de internet	Plan de servicio de internet.	$80.000
Ponencias en eventos	Inscripción y transporte.	$650.000
Publicación de artículo científico	Publicación en revista.	$320.000
Libros	Compra de libros ISO/IEC 27001 Handbook: Implementing and auditing an Information Security Management System in small and medium-sized businesses. Análisis y Gestión de Riesgos Implementando la Metodología MAGERIT: AGR-MAGERIT (Spanish Edition).	$800.000
Total		$ 2.530.000

2. Resultados

2.1 Gestión de la información en el entorno organizacional de SP Sistemas Palacios Ltda

Según el enfoque en la gestión de la información en el entorno organizacional de SP Sistemas Palacios LTDA, procede a realizar un estudio y toma de datos gracias a la observación directa en cada Área, donde se destaca el funcionamiento de cada una de ellas además de activos e información que cada una de ellas maneja.

2.1.1 Área Administrativa y Financiera

El área Administrativa y financiera es la encargada de elaborar y analizar los estados de cuenta de la empresa, para servir de apoyo en las actividades misionales de la empresa SP Sistemas Palacios LTDA. Sus principales actividades son recopilar, clasificar y registrar sistemática, ordenada y oportunamente los hechos económicos de acuerdo a los principios contables y normas legales y tributarias, las operaciones contables de la empresa, con el propósito de tener una información financiera real, razonable y oportuna con el fin de facilitar los controles, análisis y toma de decisiones de los administradores; realizar envíos de mercancía que la organización requiera para brindar el buen servicio a los clientes; realizar diligencias brindando apoyo a las actividades administrativas de la empresa; y liderar la administración de los inventarios de productos y bienes de la empresa en lo referente al Almacén de la Compañía. Atender al público y brindarle asesoría en cuanto a orientación desde la recepción.

En esta área se encuentran las siguientes unidades:

- Contabilidad y financiera
- Logística de almacén
- Tesorería
- Cartera
- Almacén y mensajería

- Caja y recepción
- Servicios generales

2.1.2 Área de operaciones

El área de operaciones es la encargada de planear y coordinar las operaciones técnicas del departamento técnico operacional, es decir su función principal es el mantener en funcionamiento la infraestructura física de la red. Entre sus funciones están; el instalar nuevos servicios, realizar mantenimientos a los clientes que ya existen y mantenerse al tanto ante posibles fallos para brindarles la solución más rápida posible. para brindar un servicio con calidad y oportuno a los clientes.

En esta área se encuentran las siguientes unidades:

- Logística
- Operativa
- Infraestructura
- Proyectos
- Gestión fibra
- Auditoria
- Seguridad vial
- Logística
- Técnicos instaladores

2.1.3 Contact center

El Contact Center o centro de contacto es el área encargada de la comunicación con el usuario, ya que esta área es la que recibe las llamadas continuas de los usuarios, siendo en primera instancia la primera comunicación que los clientes hacen con la empresa SP Sistemas palacios Ltda.

En esta área se encuentran las siguientes unidades:

- Gestor Contact Center
- Coordinador Contact Center

2.1.4 Área de ingeniería y gestión

El área de Ingeniería y Gestión es la encargada de manejar, analizar y coordinar cambios dentro de la red de SP SISTEMAS PALACIOS Ltda para el mejoramiento de la prestación del servicio que oferta ante todos sus clientes. Brinda soporte técnico a los clientes y atención al personal operativo para apoyar en las diferentes actividades del servicio que la empresa ofrece. Otras actividades son la realización y ejecución de análisis y monitoreo de red presentando informes, brindar soporte, mantenimiento, reparación, instalación de diferentes aplicaciones, y demás actividades encaminadas al mantenimiento de equipos informáticos de SP Sistemas Palacios Ltda y encargado del buen funcionamiento de la plataforma IPTV de la Compañía.

En esta área se encuentran las siguientes unidades:

- Ingeniería y Gestión
- NOC (*Network Operation Center*)
- Mantenimiento e IPTV.

2.1.5 Área de producto y servicio

El área de Producto y Servicio es la encargada de planificar, organizar, dirigir, controlar y coordinar eficientemente el sistema comercial de la empresa, diseñando estrategias que permitan el logro de los objetivos empresariales. Analizar e identificar clientes potenciales por los canales de venta directa y redes sociales, además de generar reportes diarios a la gerencia de producto. Atender los clientes de SP Sistemas Palacios Ltda, brindando información oportuna y resolver peticiones quejas o reclamos que tenga el cliente y dar solución oportuna a problemas planteados por el cliente.

En esta área se encuentran las siguientes unidades:

- Consultor PYME
- Cuidado al cliente
- Producto y servicio
- Ventas

2.1.6 Área de talento humano

El Área de Talento Humano cumple un rol estratégico en la organización al gestionar aspectos críticos relacionados con el personal. Su labor abarca desde la preselección de candidatos para asegurar la incorporación de talento adecuado hasta la administración de afiliaciones a la seguridad social integral, la custodia y seguimiento de hojas de vida, y la supervisión de exámenes ocupacionales en distintas etapas. En resumen, este departamento garantiza la disponibilidad de un equipo competente y saludable, fundamental para el éxito y el cumplimiento de objetivos organizacionales.

En esta área se encuentran las siguientes unidades:

- Jurídico
- SGSST (Sistema de Gestión de la Seguridad y Salud en el Trabajo)

2.1.7 Área de proyectos TI

El Área de Proyectos TI tiene un rol fundamental en la empresa SP Sistemas Palacios Ltda. Su función principal el desarrollo de software a la medida que garantice la agilidad y eficiencia de los procesos internos que conlleva las actividades diarias. También es encargada de garantizar la calidad de los proyectos de software siguiendo estándares de calidad. Además, supervisa de cerca las tres restricciones críticas: calidad, costo y tiempo, para asegurarse de una gestión efectiva de los proyectos. adaptándolos a las necesidades de la empresa. Esto incluye mejoras en los procesos internos y proyectos que impacten la imagen de la organización en el mercado.

En esta área se encuentran las siguientes unidades:

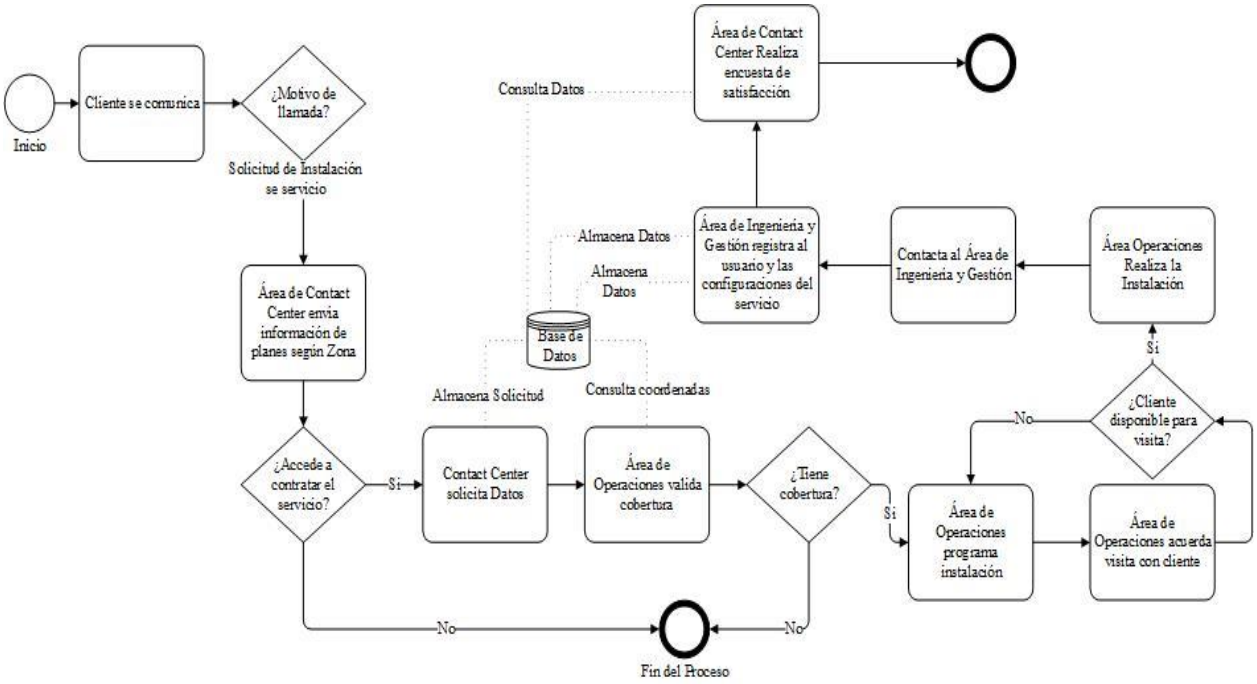
- Innovación

2.1.8 Flujos de información

A continuación, se tiene la figura 3 la cual es flujo del proceso de la instalación de un servicio nuevo, en el cual se ven con participación activa tanto el área de Contac Center, como el área de Ingeniería y gestión y el área de Operaciones.

Figura 3

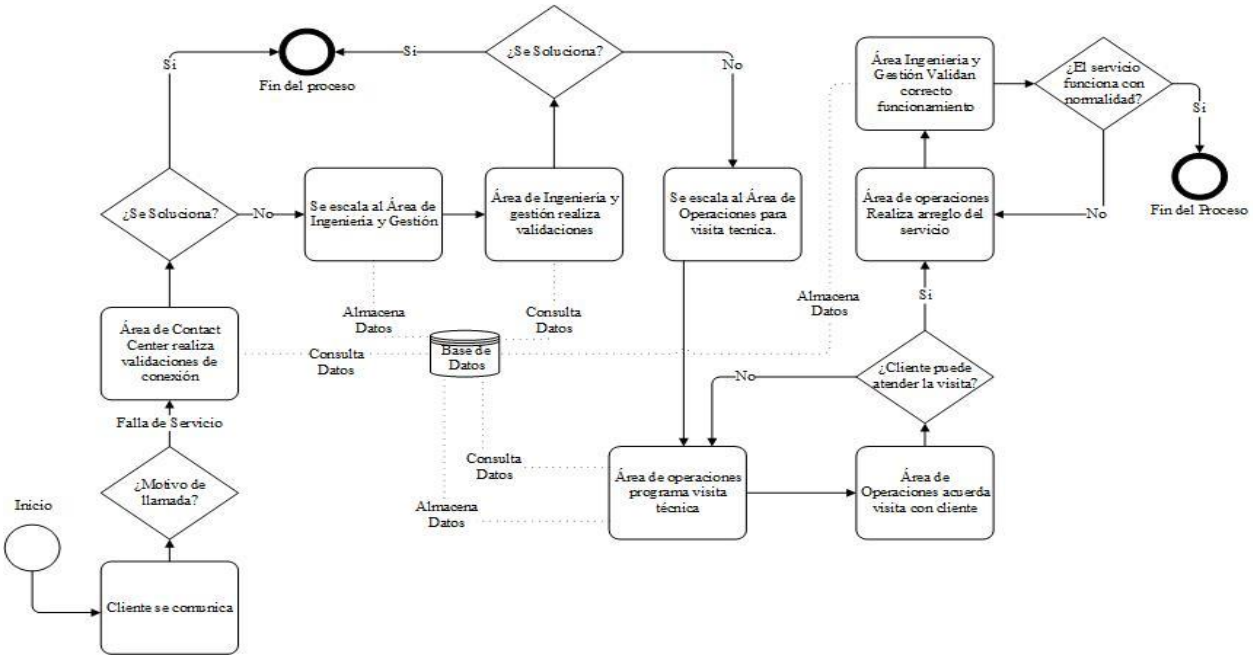
Flujo de instalación nueva



A continuación, se presenta la figura 4 el cual es el flujo del proceso de un cliente que presenta fallas en su servicio. En el proceso se involucran las áreas de Contact center, Operaciones e Ingeniería y Gestión.

Figura 4

Flujo de fallas de servicio



2.1.9 Clasificación de activos

En la Tabla 5 se enumera los diferentes tipos de activos según MAGERIT proporcionando una descripción concisa de cada uno y asignándoles un código de categorización único para su identificación y seguimiento en los procesos relacionados con la seguridad de la información y la gestión de riesgos.

Tabla 5

Caracterización de activos

Tipo	Descripción	Códigos de categorización
Datos	Datos críticos para la organización. Esto incluye información financiera, datos de clientes, documentos internos, propiedad intelectual y registros importantes.	[D]

Tipo	Descripción	Códigos de categorización
Servicios	Actividades y operaciones esenciales para el funcionamiento de la organización, como procesos de negocio, producción, ventas y logística.	[S]
Software	Aplicaciones y sistemas informáticos utilizados para gestionar datos e información, como software de contabilidad, sistemas de gestión de ventas software de recursos humanos.	[SW]
Hardware	Activos electrónicos vitales, instalaciones, servidores, equipos de red y otros bienes tangibles.	[HW]
Redes de comunicación	Incluye todos los componentes de la infraestructura de red utilizados para la comunicación de datos y voz en la organización, como routers, switches y firewalls.	[COM]
Soportes de información	Son medios físicos o lógicos que almacenan y respaldan datos críticos, como servidores de archivos y sistemas de almacenamiento en la nube.	[MEDIA]
Equipamiento auxiliar	Comprende dispositivos que facilitan las operaciones y el mantenimiento de sistemas, como impresoras, SAI y otros periféricos.	[AUX]
Instalaciones	Son lugares físicos donde se ubican activos tecnológicos y de información, como oficinas y centros de datos, y pueden incluir sistemas de seguridad física.	[L]
Personal	Se refiere a empleados y personal con acceso a sistemas y datos críticos, y también a quienes gestionan la seguridad de la información.	[P]

La tabla 6 tiene como objetivo ofrecer una clasificación organizativa de los activos informáticos y recursos críticos de la empresa SP Sistemas Palacios Ltda. Estas categorías desempeñan un papel fundamental en la gestión y seguridad de la información, así como en la operatividad general de la entidad. A través de una descripción detallada de cada categoría y su correspondiente código de categorización, se busca proporcionar una referencia clara y

sistemática que facilite la identificación, protección y seguimiento de estos activos.

La comprensión y gestión efectiva de estos activos son de vital importancia en el entorno actual, donde la información y la tecnología desempeñan un papel central en el éxito y la continuidad de las organizaciones. Esta tabla sirve como punto de partida para el desarrollo de estrategias de gestión de activos y seguridad de la información, permitiendo a las organizaciones salvaguardar sus recursos críticos y mantener un funcionamiento sólido y seguro.

Tabla 6

Inventario de activos

Tipo activo	Activo
Datos [D]	Base de Datos de Clientes
	Documentos Financieros
	Base de Datos de colaboradores
	Contratos de Clientes
	Proyectos de infraestructura
	Llamadas de clientes
	Infraestructura lógica de la red
	Campañas de marketing
	Contratos de colaboradores
	Hojas de Vida de los coladores
	Afiliaciones de los Colaboradores
	Código Fuente
Servicios [S]	Servicios Prestados:
	Servicios de Telecomunicaciones
	Registro de clientes
	Registro de pago de clientes
	Registro de equipos de telecomunicaciones
	Registro de infraestructura
	Atención al Cliente

Tipo activo	Activo
	Plataforma en Línea
	Seguridad de la Información
	Servicios de Facturación y Contabilidad
	Servicios Recibidos:
	Servicios de Energía y Suministros
	Almacenamiento en la nube
Software [SW]	Aplicación SP_Sistemas Palacios
	Aplicación viáticos modulo caja menor
	Aplicación viáticos modulo caja menor
	Aplicación rastreo satelital Mega7
	Aplicación actividades técnicos
	Aplicación de almacenamiento en la nube
	Suite de Software ofimático
	Aplicación gestión de llamadas
	Aplicación de administración de red
	Aplicación de monitoreo de red
	Aplicación CRM
Hardware [HW]	Equipos computadores de escritorio
	Equipos Computadores Portátiles
	Impresoras
	Celulares
	Servidor de aplicaciones
	Servidores de IPTV
	Servidores de llamadas
Redes de Comunicación [COM]	Equipos de red
	Cables y conexiones
	Puntos de acceso AP
	Servidores de comunicaciones
	Hardware de monitoreo de red Routerboard
	Hardware de gestión de red interna Routerboard

Tipo activo	Activo
	Documentación de red
	Dispositivos de seguridad
Equipamiento Auxiliar [AUX]	Sistemas de Alimentación Ininterrumpida (UPS)
	Sistemas de Climatización
	Sistemas de Control de Acceso
	Sistemas de Extinción de Incendios
	Sistemas de Vigilancia y CCTV
Instalaciones [L]	Centro de datos
	Áreas de trabajo
	Centro de operaciones de red
	Sala de Juntas
	Recepción
Personal [P]	Personal de Área de Operaciones
	Personal de Área Administrativa y financiera
	Personal de Área de Contact center
	Personal de Área de Producto y servicio
	Personal de Área de Ingeniería y gestión
	Personal de Área de Talento humano
	Personal de Área de Proyectos TI

2.2 Amenazas, riesgos y vulnerabilidades a la información de la empresa SP Sistemas Palacios LTDA. con el estándar MAGERIT

En las empresas modernas, la información y los equipos son esenciales para la prestación de servicios, sin embargo, con la gran cantidad de información y equipos, también aumenta la probabilidad de que se presenten riesgos y amenazas que puedan afectar el funcionamiento de la empresa. Es por eso que, en SP Sistemas Palacios Ltda se ha tomado la iniciativa de realizar un estudio de amenazas, riesgos y vulnerabilidades en todas sus áreas funcionales. La gestión adecuada de los riesgos es crucial para minimizar su impacto en la empresa. Una gestión de riesgos puede ayudar a prevenir pérdidas financieras, daños a la reputación de la empresa,

interrupciones en la prestación de servicios y otros problemas que puedan afectar negativamente el funcionamiento de la empresa.

En este sentido, se ha elegido utilizar la matriz de riesgo de MAGERIT, una herramienta ampliamente utilizada para la identificación, análisis y evaluación de riesgos en el ámbito de la seguridad de la información. La matriz de riesgo de MAGERIT se enfoca en evaluar los riesgos de forma sistemática, considerando los posibles impactos y la probabilidad de que ocurran. Al realizar este estudio de amenazas, riesgos y vulnerabilidades en todas las áreas funcionales de la empresa, se podrán identificar los posibles riesgos y vulnerabilidades en cada una de ellas, y así tomar medidas preventivas y correctivas para minimizar su impacto. De esta forma, se garantiza la continuidad del negocio y se protege la información crítica de la empresa. Al realizar el análisis existen amenazas y vulnerabilidades que están presentes en todas las áreas independientemente de su función y equipamiento dentro de la empresa SP Sistemas Palacios Ltda.

La metodología MAGERIT permite una gestión integral de los riesgos de la información en una organización. Mediante esta metodología, se establecen los pasos necesarios para realizar un análisis de los riesgos, amenazas y vulnerabilidades y con esto poder determinar medidas de mitigación. Estas medidas de mitigación pueden variar según la naturaleza y la gravedad de los riesgos identificados. Pueden incluir la implementación de políticas de seguridad de la información robustas, la adopción de controles técnicos avanzados, la capacitación del personal en prácticas seguras, y la revisión y actualización constante de los procedimientos operativos.

El proceso comienza con la identificación y valoración de las amenazas potenciales que podrían afectar el sistema de información de la empresa.

2.2.1 Valoración de amenazas

Una vez identificados los activos informáticos, la metodología plantea identificar amenazas, riesgos y vulnerabilidades la tabla 9 la cual contiene la caracterización de los activos, mencionando las amenazas latentes que se pueden presentar.

Degradación: la degradación en la valoración de amenazas se refiere al impacto negativo que una amenaza puede tener en un activo o recurso en caso de que se materialice. Se evalúa el grado de daño o pérdida que podría experimentar el activo en términos de funcionalidad, integridad, confidencialidad o disponibilidad. La degradación se mide en una escala que varía desde "Muy Baja" hasta "Muy Alta"

Frecuencia: se refiere a la probabilidad o la frecuencia con la que una amenaza específica puede materializarse y causar daño a un activo. Se evalúa cuán probable es que ocurra un evento o incidente que desencadene la amenaza. La frecuencia se mide en una escala que puede variar desde "Poco frecuente" hasta "Muy frecuente", y se utiliza para determinar la probabilidad de que ocurra una amenaza.

Tabla 7

Degradación

Nivel	**Degradación del Activo**
MB (Muy Baja)	Daño en el activo del 1 %
B (Baja)	Daño en el activo del 25 %
M (Media)	Daño en el activo del 50 %
A (Alta)	Daño en el activo del 75 %
MA (Muy Alta)	Daño en el activo del 100 %

Tabla 8

Frecuencia

Nivel	**Frecuencia de materialización**
PF (Poco frecuente)	Varios Años
FN (Frecuencia Normal)	Anual
(F) Frecuente	Mensual
MF (Muy Frecuente)	Diariamente

Tabla 9

Valoración de Amenazas

Tipo Activo	Activo	Amenazas	Degradación	Frecuencia
(Datos [D])	Base de Datos de Clientes	Acceso no autorizado, pérdida de datos, robo de información, ataques cibernéticos.	Media	Baja
	Documentos Financieros	Acceso no autorizado, pérdida de datos, robo de información, pérdida física.	Alta	Media
	Base de Datos de colaboradores	Acceso no autorizado, pérdida de datos, robo de información, fuga de datos personales.	Media	Baja
	Contratos de Clientes	Acceso no autorizado, pérdida de datos, robo de información, pérdida física, incumplimiento contractual.	Alta	Media
	Proyectos de infraestructura	Acceso no autorizado, pérdida de datos, robo de información, pérdida física, riesgos asociados a la infraestructura.	Media	Baja
	Llamadas de clientes	Intercepción de llamadas, escuchas ilegales, acceso no autorizado.	Baja	Alta
	Infraestructura lógica de la red	Ataques cibernéticos, malware, acceso no autorizado.	Alta	Alta
	Campañas de	Acceso no autorizado,	Media	Baja

Tipo Activo	Activo	Amenazas	Degradación	Frecuencia
	marketing	pérdida de datos, robo de información.		
	Contratos de colaboradores	Acceso no autorizado, pérdida de datos, robo de información, riesgos asociados a la relación laboral.	Media	Media
	Hojas de Vida de los colaboradores	Acceso no autorizado, pérdida de datos, robo de información, fuga de datos personales.	Baja	Baja
	Afiliaciones de los Colaboradores	Acceso no autorizado, pérdida de datos, robo de información, fuga de datos personales.	Baja	Baja
	Código Fuente	Acceso no autorizado, pérdida de datos, robo de información, fuga de propiedad intelectual.	Alta	Media
(Servicios [S])	Servicios Prestados	Interrupción del servicio, ataques de denegación de servicio (DDoS), fallas técnicas.	Alta	Media
	Servicios Recibidos	Interrupción del servicio, fallos en proveedores de servicios, incumplimiento contractual.	Alta	Media
(Software [SW])	Aplicación SP_Sistemas Palacios	Vulnerabilidades de software, ataques cibernéticos, pérdida de datos.	Media	Alta

Tipo Activo	Activo	Amenazas	Degradación	Frecuencia
(Hardware [HW])	Equipos computadores de escritorio	Robo de hardware, fallas técnicas, pérdida de datos.	Alta	Baja
	Equipos Computadores Portátiles	Robo de hardware, pérdida física, pérdida de datos.	Alta	Media
	Impresoras	Robo de hardware, acceso no autorizado, pérdida de datos.	Media	Baja
	Celulares	Pérdida o robo de dispositivos, acceso no autorizado, pérdida de datos.	Alta	Media
(Redes de Comunicación [COM])	Equipos de red	Ataques a la red, fallos técnicos, acceso no autorizado.	Alta	Media
	Cables y conexiones	Daño a la infraestructura de red, acceso no autorizado.	Media	Baja
	Puntos de acceso AP	Acceso no autorizado, ataques a la red, interceptación de datos.	Alta	Alta
	Servidores de comunicaciones	Ataques a servidores, pérdida de conectividad, fallos técnicos.	Alta	Media
(Equipamiento Auxiliar [AUX])	Sistemas de Alimentación Ininterrumpida (UPS)	Fallos en el suministro eléctrico, pérdida de energía.	Alta	Baja
	Sistemas de Climatización	Fallos en la climatización, sobrecalentamiento de equipos.	Media	Baja
	Sistemas de	Acceso no autorizado, fallos	Alta	Media

Tipo Activo	Activo	Amenazas	Degradación	Frecuencia
	Control de Acceso	en sistemas de seguridad.		
	Sistemas de Extinción de Incendios	Incendios, fallos en sistemas de extinción.	Alta	Baja
	Sistemas de Vigilancia y CCTV	Acceso no autorizado, fallos en sistemas de vigilancia.	Media	Baja
(Instalaciones [L])	Centro de datos	Incendios, inundaciones, fallos estructurales.	Alta	Baja
	Áreas de trabajo (Instalaciones [L])	Robo, acceso no autorizado, riesgos laborales.	Media	Alta
	Centro de operaciones de red (Instalaciones [L])	Fallos en operaciones críticas, acceso no autorizado.	Alta	Media

2.2.2 Vulnerabilidades según activos

A continuación, se muestra la tabla 10 la cual presenta vulnerabilidades que se obtienen a partir de la observación directa y entrevistas a los responsables de la información de cada área, tiene 5 atributos los cuales son: Tipo activo, que representa el tipo de activo según la clasificación de los mismos, también los activos que están clasificados según su tipo, de igual forma se presentan el tipo de vulnerabilidades.

- **Degradación de vulnerabilidades:** La degradación de vulnerabilidades se refiere a cómo una vulnerabilidad particular puede debilitar la seguridad de un activo o sistema. Puede variar desde una degradación menor que tiene un impacto mínimo en la seguridad hasta una degradación completa que permite a las amenazas explotar completamente la

vulnerabilidad. La degradación se evalúa considerando factores como la facilidad de explotación y el impacto potencial en la seguridad del activo.

- **Frecuencia de vulnerabilidades:** La frecuencia de vulnerabilidades se relaciona con la probabilidad de que una vulnerabilidad específica sea explotada en un período de tiempo determinado. Se evalúa cuán probable es que un atacante intente aprovechar la vulnerabilidad y cause un incidente de seguridad. La frecuencia se mide en una escala que puede variar desde "muy baja" hasta "muy alta", y se utiliza para determinar la probabilidad de que ocurra una explotación de vulnerabilidad en el entorno de la organización.

Tabla 10

Valoración de Vulnerabilidades

Tipo Activo	Activo	Vulnerabilidades	Degradación	Frecuencia
(Datos [D])	Base de Datos de Clientes	Vulnerabilidades de seguridad, acceso no autorizado, falta de cifrado.	Media	Baja
	Documentos Financieros	Falta de autenticación, permisos inadecuados, falta de auditoría.	Alta	Media
	Base de Datos de colaboradores	Vulnerabilidades de seguridad, acceso no autorizado, falta de cifrado.	Media	Baja
	Contratos de Clientes	Falta de autenticación, permisos inadecuados, falta de auditoría.	Alta	Media
	Proyectos de infraestructura	Vulnerabilidades de seguridad, acceso no autorizado, falta de cifrado.	Media	Baja
	Llamadas de	Vulnerabilidades de red,	Baja	Alta

Tipo Activo	Activo	Vulnerabilidades	Degradación	Frecuencia
	clientes	interceptación de comunicaciones, falta de encriptación.		
	Infraestructura lógica de la red	Vulnerabilidades de red, ataques cibernéticos, falta de detección de intrusiones.	Alta	Alta
	Campañas de marketing	Falta de autenticación, permisos inadecuados, falta de cifrado.	Media	Baja
	Contratos de colaboradores	Falta de autenticación, permisos inadecuados, falta de auditoría.	Media	Media
	Hojas de Vida de los colaboradores	Vulnerabilidades de seguridad, acceso no autorizado, falta de cifrado.	Baja	Baja
	Afiliaciones de los Colaboradores	Vulnerabilidades de seguridad, acceso no autorizado, falta de cifrado.	Baja	Baja
	Código Fuente	Vulnerabilidades de seguridad, acceso no autorizado, falta de cifrado.	Alta	Media
(Servicios [S])	Servicios Prestados	Vulnerabilidades de software, falta de parches, falta de actualización.	Alta	Media
	Servicios Recibidos	Falta de acuerdos contractuales, vulnerabilidades en proveedores, falta de auditoría.	Alta	Media
(Software	Aplicación	Vulnerabilidades de	Media	Alta

Tipo Activo	Activo	Vulnerabilidades	Degradación	Frecuencia
[SW])	SP_Sistemas Palacios	software, falta de parches, falta de actualización.		
(Hardware [HW])	Equipos computadores de escritorio	Vulnerabilidades de hardware, falta de actualización de firmware.	Alta	Baja
	Equipos Computadores Portátiles	Vulnerabilidades de hardware, falta de actualización de firmware.	Alta	Media
	Impresoras	Vulnerabilidades de hardware, falta de actualización de firmware.	Media	Baja
	Celulares	Vulnerabilidades de hardware, falta de actualización de firmware, falta de cifrado.	Alta	Media
(Redes de Comunicación [COM])	Equipos de red	Vulnerabilidades de red, falta de actualización de firmware, falta de detección de intrusiones.	Alta	Media
	Cables y conexiones	Daño físico, falta de protección, vulnerabilidades de red.	Media	Baja
	Puntos de acceso AP	Vulnerabilidades de red, falta de actualización de firmware, acceso no autorizado.	Alta	Alta
	Servidores de comunicaciones	Vulnerabilidades de servidores, falta de actualización de firmware, acceso no autorizado.	Alta	Media

Tipo Activo	Activo	Vulnerabilidades	Degradación	Frecuencia
(Equipamiento Auxiliar [AUX])	Sistemas de Alimentación Ininterrumpida (UPS)	Fallos técnicos, falta de mantenimiento, vulnerabilidades de hardware.	Alta	Baja
	Sistemas de Climatización	Fallos técnicos, falta de mantenimiento, vulnerabilidades de control.	Media	Baja
	Sistemas de Control de Acceso	Vulnerabilidades de control, falta de actualización de firmware, acceso no autorizado.	Alta	Media
	Sistemas de Extinción de Incendios	Fallos técnicos, falta de mantenimiento, vulnerabilidades de control.	Alta	Baja
	Sistemas de Vigilancia y CCTV	Vulnerabilidades de control, falta de actualización de firmware, acceso no autorizado.	Media	Baja
(Instalaciones [L])	Centro de datos	Incendios, inundaciones, falta de protección, vulnerabilidades de infraestructura.	Alta	Baja
	Áreas de trabajo	Robo, acceso no autorizado, falta de seguridad física, riesgos laborales.	Media	Alta
	Centro de operaciones de red	Fallos en operaciones críticas, acceso no autorizado, vulnerabilidades de infraestructura.	Alta	Media
	Sala de Juntas	Pérdida de	Media	Baja

Tipo Activo	Activo	Vulnerabilidades	Degradación	Frecuencia
		confidencialidad, acceso no autorizado, vulnerabilidades de infraestructura.		
	Recepción	Acceso no autorizado, vulnerabilidades de seguridad, falta de seguridad física.	Alta	Media

2.2.3 Riesgos según activos

Se presenta la tabla 11 la cual refleja los datos obtenidos después del proceso de investigación con cada una de las áreas de la empresa SP Sistemas Palacios Ltda.

- **Degradación de riesgos:** La degradación de riesgos se refiere a cómo la combinación de una amenaza, una vulnerabilidad y un activo específicos puede degradar la seguridad general de la organización. Se evalúa considerando factores como la probabilidad de que ocurra la amenaza, la probabilidad de que la vulnerabilidad sea explotada y el impacto potencial en la organización si se materializa el riesgo. La degradación se mide en una escala que puede variar desde "muy baja" hasta "muy alta", lo que indica la gravedad del riesgo.

- **Frecuencia de riesgos:** La frecuencia de riesgos se relaciona con la probabilidad de que ocurra un riesgo específico en un período de tiempo determinado. Se basa en la frecuencia de la amenaza y la vulnerabilidad, es decir, con qué regularidad la amenaza podría aprovechar la vulnerabilidad y afectar al activo. La frecuencia se mide en una escala que puede variar desde "muy baja" hasta "muy alta" y se utiliza para determinar cuán probable es que se materialice un riesgo en el entorno de la organización.

Tabla 11

Valoración de Riesgos

Tipo de Activo	Activo	Riesgos	Degradación	Frecuencia
(Datos [D])	Base de Datos de Clientes	Pérdida de datos, acceso no autorizado, robo de información.	Media	Baja
	Documentos Financieros	Fuga de información financiera, divulgación no autorizada, pérdida de confidencialidad.	Alta	Media
	Base de Datos de colaboradores	Acceso no autorizado a datos sensibles de empleados, robo de información personal.	Media	Baja
	Contratos de Clientes	Pérdida de contratos, divulgación no autorizada de acuerdos comerciales.	Alta	Media
	Proyectos de infraestructura	Divulgación de información estratégica, riesgo competitivo.	Media	Baja
	Llamadas de clientes	Interceptación de llamadas, escuchas ilegales, pérdida de privacidad.	Baja	Alta
	Infraestructura lógica de la red	Ataque cibernético, paralización de operaciones, pérdida de servicios.	Alta	Alta
	Campañas de marketing	Pérdida de estrategias de marketing, divulgación no	Media	Baja

Tipo de Activo	Activo	Riesgos	Degradación	Frecuencia
		autorizada de campañas.		
	Contratos de colaboradores	Acceso no autorizado a acuerdos laborales, conflicto laboral.	Media	Media
	Hojas de Vida de los colaboradores	Acceso no autorizado a información personal de empleados, riesgo de fraude.	Baja	Baja
	Afiliaciones de los Colaboradores	Acceso no autorizado a datos de afiliación, riesgo de phishing.	Baja	Baja
	Código Fuente	Pérdida de propiedad intelectual, divulgación no autorizada de código fuente.	Alta	Media
(Servicios [S])	Servicios Prestados	Interrupción de servicios, insatisfacción del cliente, pérdida de ingresos.	Alta	Media
	Servicios Recibidos	Incumplimiento de servicios contratados, riesgo de dependencia de proveedores.	Alta	Media
(Software [SW])	Aplicación SP_Sistemas Palacios	Fallos en la aplicación, pérdida de datos, impacto en la productividad.	Media	Alta
(Hardware [HW])	Equipos computadores de escritorio	Fallos de hardware, pérdida de datos, interrupción de operaciones.	Alta	Baja
	Equipos	Robo de equipos, pérdida	Alta	Media

Tipo de Activo	Activo	Riesgos	Degradación	Frecuencia
	Computadores Portátiles	de información confidencial, riesgo de seguridad.		
	Impresoras	Acceso no autorizado a impresoras, impresiones no deseadas, pérdida de confidencialidad.	Media	Baja
	Celulares	Pérdida de dispositivos, acceso no autorizado a datos móviles, riesgo de robo de información.	Alta	Media
(Redes de Comunicación [COM])	Equipos de red	Ataque a la red, paralización de la comunicación, pérdida de servicios críticos.	Alta	Media
	Cables y conexiones	Daño físico a la infraestructura de red, pérdida de conectividad.	Media	Baja
	Puntos de acceso AP	Acceso no autorizado a la red, riesgo de intrusión, pérdida de privacidad.	Alta	Alta
	Servidores de comunicaciones	Fallos en servidores, interrupción de la comunicación, pérdida de servicios.	Alta	Media
(Equipamiento Auxiliar [AUX])	Sistemas de Alimentación Ininterrumpida (UPS)	Fallos en el suministro eléctrico, pérdida de energía, riesgo de interrupción.	Alta	Baja
	Sistemas de	Fallos en la climatización,	Media	Baja

Tipo de Activo	Activo	Riesgos	Degradación	Frecuencia
	Climatización (Equipamiento Auxiliar [AUX])	sobrecalentamiento de equipos, pérdida de hardware.		
	Sistemas de Control de Acceso (Equipamiento Auxiliar [AUX])	Acceso no autorizado, riesgo de intrusión, pérdida de seguridad física.	Alta	Media
	Sistemas de Extinción de Incendios (Equipamiento Auxiliar [AUX])	Fallos en la extinción de incendios, riesgo de incendios no controlados.	Alta	Baja
	Sistemas de Vigilancia y CCTV (Equipamiento Auxiliar [AUX])	Fallos en la vigilancia, pérdida de control, riesgo de seguridad.	Media	Baja
(Instalaciones [L])	Centro de datos	Incendios, inundaciones, pérdida de infraestructura, riesgo de paralización.	Alta	Baja
	Áreas de trabajo	Robo, acceso no autorizado, riesgo laboral, pérdida de confidencialidad.	Media	Alta
	Centro de operaciones de red	Fallos en operaciones críticas, acceso no autorizado, riesgo de interrupción.	Alta	Media
	Sala de Juntas	Pérdida de privacidad, acceso no autorizado, riesgo de escuchas	Media	Baja

Tipo de Activo	Activo	Riesgos	Degradación	Frecuencia
		ilegales.		
	Recepción	Acceso no autorizado, pérdida de seguridad física, riesgo de intrusiones.	Alta	Media

2.2.4 Riesgos y valoración de activo por áreas administrativas

Una vez se culmina el análisis general de los activos de información de la empresa SP Sistemas Palacios Ltda se continua con el análisis del riesgo a los que se enfrenta cada área, resaltando la situación y el proceso de riesgo que estos tienen.

La metodología MAGERIT permite una gestión integral de los riesgos de la información en una organización. Mediante esta metodología, se establecen los pasos necesarios para realizar un análisis exhaustivo de los riesgos y determinar las medidas de mitigación adecuadas.

El proceso comienza con la identificación y evaluación de las amenazas potenciales que podrían afectar el sistema de información de la empresa. Luego, se procede a evaluar el impacto que cada amenaza podría tener en el funcionamiento de la organización. Esto incluye considerar la confidencialidad, integridad y disponibilidad de la información. Para realizar una escala descriptiva donde se estima la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo, se caracteriza los riesgos bajo los siguientes determinantes:

FR.: Frecuencia: Improbable **(I)**; Poco probable **(PP)**; Probable **(PR)**; Muy probable **(MP)**.
INT.: Intensidad: Baja **(B)**; Media **(Mda)**; Alta **(Al)**; Muy Alta **(MA)**.
COB.: Cobertura: Poca **(P)**; Mediana **(Mda)**; Alta **(A)**; Total **(T)**.

Una vez se identifique su caracterización se procede a calificar los riesgos:

Tabla 12

Calificación del riesgo

Bajo: Se debe implementar medidas preventivas las cuales ayudan a prevenir y reducir el riesgo, se le asigna el color verde.

Medio: Se requiere implementar medidas lo más pronto posible las cuales permitandisminuir el riesgo a un nivel bajo o muy bajo

Alto: Se requiere acciones inmediatas las cuales permitan reducir, compartir otransferir el riesgo

Fuente. Portal Administración Electrónica (PAE, 2012).

Para medir el nivel de confidencialidad de los activos de la empresa se tiene en cuenta la escala de valoración de las tres dimensiones, según el Portal Administración Electrónica (P.A. E, 2012) por medio de los criterios de confidencialidad, integridad y disponibilidad se puede valorar los equipos en una escala que consta desde el valor 0 al valor 5 los cuales tienen una valoración de despreciable y extremo respectivamente. A continuación, se muestra en la (Tabla 13) los valores que poseen cada uno de los valores en la escala:

Tabla 13

Criterios de valoración

Valor		Criterio
5	Extremo	Daño extremadamente grave
4	Muy alto	Daño muy grave
3	Alto	Daño grave
2	Medio	Daño importante
1	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

2.2.5 Riesgos del área Administrativa y financiera

Tabla 14

Matriz categorización de riesgos para el área administrativa y financiera

Situación	Procesos de riesgo	Activos afectados	Caracterización		Calificación	
			Fr	Int	Cob	Gama de color
Mantenimiento y prevención de riesgos en los equipos	Falta de mantenimiento en el sistema antincendios: perdida por incendio.	Equipos de cómputo, documentos importantes	PP	B	A	
	No se posee un amplio sistema de refrigeración: Sobrecalentamiento y daño de los equipos.	Equipos de cómputo	PP	PP		
	No existe control sobre las personas que ingresan y salen de las oficinas del Área administrativa y financiera: Robo	Documentos importantes	PR	MB		
	Error en la manipulación de las redes: conexiones inseguras	Equipos de cómputo	PP	B		
	No se tiene los equipos correctamente inventariados: Robos	Equipos de cómputo	PP	B	A	

Situación	Procesos de riesgo	Activos afectados	Caracterización		Calificación	
			Fr	Int	Cob	Gama de color
	Falta niveles de seguridad en los router	Equipos de cómputo	PP	MD	Mda	
S.O Windows	Errores en la configuración de seguridad, generando riesgo de ciberataques.	Datos importantes	PP	Mda	A	
	No posee una generación correcta de los roles, ni sistemas de control: perdida de información.	Información confidencial	PR	AL	T	
	Falta de políticas y personal encargado de generar la documentación., Mal uso de los equipos.	Documentos importantes	PP	MD	Mda	
	Interfaces de difícil manipulación produce Errores de uso.	Productividad	MP	MD	Mda	
	Falta de bloqueo del equipo al abandonar el puesto de trabajo, genera abuso de los equipos.	Productividad	MP	AL	T	
	No existencia de copias de seguridad, Mal funcionamiento del software.	Datos importantes	PR	AL	P	

Situación	Procesos de riesgo	Activos afectados	Caracterización		Calificación	
			Fr	Int	Cob	Gama de color
Personal de planta (Contabilidad y financiera, Logística de almacén, Tesorería, Contador, Cartera, Almacén y mensajería, Caja y recepción, Servicios generales)	Falta de controles de seguridad: Robo de documentación	Documentos importantes	PP	AL	T	
	Ausencia de personal calificado: No existe una correcta asignación en las responsabilidades.	Productividad	PP	AL	Mda	
	No existen políticas y control anti spam: Perdida de los datos.	Correo electrónico	MP	AL	A	
	Entrenamiento insuficiente del personal: Perdida de personal clave	Productividad	MP	AL	P	
Instalaciones	Los controles de acceso existentes son básicos: Acceso no autorizado.	Documentos importantes	PP	AL	Mda	
	Ausencia de protecciones digitales: Perdida de equipos.	Equipos de cómputo	PP	P	B	
	Redes eléctricas inestables: Cambios de voltaje o perdidas de energía.	Equipos de cómputo	MP	AL	T	

Fuente: Portal Administración Electrónica (PAE, 2012)

Según los datos obtenidos en la tabla 14 destacan diversos riesgos que deben ser considerados para garantizar la seguridad y el buen funcionamiento de esta área crucial en las organizaciones. En cuanto al mantenimiento y prevención de riesgos en los equipos, se identifican riesgos como la falta de mantenimiento en el sistema antincendios, lo cual podría resultar en la pérdida de equipos de cómputo y documentos importantes en caso de un incendio. Además, la ausencia de un amplio sistema de refrigeración puede llevar al sobrecalentamiento y daño de los equipos. En relación al sistema operativo Windows, se mencionan riesgos asociados a errores en la configuración de seguridad, lo que podría generar vulnerabilidades y ser aprovechado para ciberataques.

Asimismo, la falta de una correcta generación de roles y sistemas de control puede ocasionar la pérdida de información confidencial. En lo referente al personal de planta, se resaltan riesgos como la falta de controles de seguridad, lo cual podría dar lugar al robo de documentación importante. Además, la ausencia de personal calificado y una asignación incorrecta de responsabilidades puede impactar negativamente la productividad y eficiencia del área. Por otro lado, en relación a las instalaciones, se advierte sobre los riesgos asociados a los controles de acceso básicos, lo cual puede facilitar el acceso no autorizado a documentos importantes.

Además, la ausencia de protecciones digitales representa un riesgo de pérdida de equipos. Estos riesgos afectan diversos activos, como equipos de cómputo, documentos importantes, información confidencial, productividad y correo electrónico. La calificación de los riesgos se basa en una combinación de la probabilidad de ocurrencia y el impacto potencial, y se utiliza una gama de colores para indicar la gravedad de cada riesgo. Es importante tener en cuenta estos riesgos y adoptar medidas preventivas y de mitigación adecuadas para salvaguardar la integridad, confidencialidad y disponibilidad de la información, así como para garantizar el buen desempeño y la continuidad de las operaciones administrativas y financieras de la organización.

Tabla 15

Nivel de valoración equipos

Nombre del Activo	Ubicación	Valoración de la pérdida del activo			
		Confidencialidad	**Disponibilidad**	**Integridad**	**Total del impacto**
JANUS	Caja y recepción	2	4	2	3
Hewlett-Packard pro one 600	Tesorería	4	4	2	4
Hewlett-Packard pro one 600	Contador	4	4	3	4
Hewlett-Packard pro one 600	Contador	4	4	3	4
Hewlett-Packard pro one 600	Almacén y mensajería	3	4	3	3
Hewlett-Packard pro one 600	Logística de Almacén	3	4	2	3

En este análisis, en cuanto a la confidencialidad se evidencia que parte de los equipos de la empresa presenta un daño alto en cuanto a la confidencialidad, esto debido a la falta de protección de datos que tienen en su software, 4 de los equipos presentan una disponibilidad alta de información y 3 de los equipos tienen en su base de datos información integral para la empresa, el total de los activos presenta un impacto alto para la organización, es decir el nivel de daño que afectadas las dimensiones de confidencialidad, integridad y disponibilidad que posee cada uno de los activos al materializarse las amenazas.

Una vez analizada la situación de la seguridad en la cual se encuentra el área, donde se observa que las medidas de control son bajas y los planes para tratar los riesgos son escasos, se procede a proponer un sistema de gestión de seguridad de la información, para lo cual se toma en cuenta los criterios de aceptación del riesgo según la ISO/IEC 27001: 2013 norma desarrollada

por la ISO y la IEC.

2.2.6 Riesgos del área de operaciones

Tabla 16

Matriz categorización de riesgos

Situación	Procesos de riesgo	Activos afectados	Caracterización		Calificación	
			Fr	Int	Cob	Gama de color
Robo o extravío de dispositivos móviles o portátiles	Pérdida o robo de dispositivos móviles o portátiles, lo que puede dañar la información de la empresa o del cliente.	Dispositivos móviles y portátiles	PP	B	A	
Falta de protección de datos en redes publicas	Acceso no autorizado a la información de la empresa o del cliente por el uso de redes públicas no seguras.	Datos y comunicaciones	PR	MD	Mda	
Mal uso de la información	Incumplimiento de políticas de privacidad y seguridad de la información por parte del personal	Información confidencial de la empresa o del cliente	PP	B	A	

Situación	Procesos de riesgo	Activos afectados	Caracterización		Calificación	
			Fr	Int	Cob	Gama de color
	técnico.					
Falta de medidas de protección en las instalaciones de los clientes	Vulnerabilidad de los equipos e información de la empresa y del cliente ante amenazas externas (robo, vandalismo, etc.).	Equipos y datos de los clientes	PR	Mda	A	
Falta de medidas de control en los accesos	Riesgo de acceso no autorizado a los sistemas y datos de la empresa y del cliente por falta de medidas de control en los accesos.	Sistemas y datos	PP	B	A	
Mal uso de los sistemas de información	Incumplimiento de políticas de privacidad y seguridad de la información por parte del personal técnico.	Información confidencial de la empresa o del cliente	PP	MD	Mda	
Ausencia de políticas y personal encargado de generar la	No existe control sobre la documentación capturada en campo: Pérdida de	Información de la empresa y de los clientes	PP	Mda		

Situación	Procesos de riesgo	Activos afectados	Caracterización		Calificación	
			Fr	Int	Cob	Gama de color
documentación	información.					
Falta de controles de seguridad en los vehículos	Robo de los vehículos y los equipos de trabajo	Vehículos y equipos de trabajo	PR	AL	T	
Ausencia de protecciones digitales en los equipos móviles	Pérdida de los equipos móviles por robo	Equipos móviles	PP	MD	Mda	

Fuente: Portal Administración Electrónica (PAE, 2012).

Según los datos obtenidos de la tabla 16 destacan diversos riesgos que deben ser considerados para garantizar la seguridad y el correcto funcionamiento de esta área en las organizaciones. Uno de los riesgos identificados es el robo o extravío de dispositivos móviles o portátiles, lo cual puede resultar en la pérdida o robo de información empresarial o de clientes. Esto afecta a los dispositivos móviles y portátiles y se califica como un riesgo de alto impacto. Otro riesgo es la falta de protección de datos en redes públicas, lo cual puede permitir el acceso no autorizado a la información empresarial o de clientes a través del uso de redes públicas no seguras. Esto afecta a los datos y comunicaciones y se califica como un riesgo de impacto medio. El mal uso de la información es otro riesgo identificado, relacionado con el incumplimiento de políticas de privacidad y seguridad de la información por parte del personal técnico. Esto pone en riesgo la información confidencial de la empresa o de los clientes y se califica como un riesgo de alto impacto.

La falta de medidas de protección en las instalaciones de los clientes representa un riesgo de vulnerabilidad para los equipos e información de la empresa y los clientes ante amenazas externas, como robo o vandalismo. Esto afecta a los equipos y datos de los clientes y se califica como un riesgo de alto impacto. Además, se identifica el riesgo de falta de medidas de control en

los accesos, lo cual puede facilitar el acceso no autorizado a los sistemas y datos de la empresa y los clientes. Esto afecta a los sistemas y datos y se califica como un riesgo de alto impacto. El mal uso de los sistemas de información, el cual implica el incumplimiento de políticas de privacidad y seguridad por parte del personal técnico, es otro riesgo identificado. Esto pone en riesgo la información confidencial de la empresa o de los clientes y se califica como un riesgo de impacto medio.

Otros riesgos incluyen la ausencia de políticas y personal encargado de generar la documentación, lo cual puede resultar en la pérdida de información empresarial y de clientes; la falta de controles de seguridad en los vehículos, lo cual puede llevar al robo de vehículos y equipos de trabajo; y la ausencia de protecciones digitales en los equipos móviles, lo cual puede resultar en la pérdida de dichos equipos por robo. Estos riesgos afectan diversos activos, como dispositivos móviles y portátiles, datos y comunicaciones, información confidencial, equipos y datos de los clientes, sistemas y datos, y equipos móviles. La calificación de los riesgos se basa en una combinación de la probabilidad de ocurrencia y el impacto potencial. Es fundamental tomar en cuenta estos riesgos y adoptar medidas preventivas y de mitigación adecuadas para garantizar la protección de la información, la seguridad de los sistemas y la continuidad de las operaciones en el área de operaciones de la organización.

Tabla 17

Nivel de valoración equipos

Nombre del Activo	**Ubicación**	**Valoración de la pérdida del activo**			
		Confidencialidad	**Disponibilidad**	**Integridad**	**Total del impacto**
Hewlett-Packard pro one 600	Gerencia Operaciones	2	4	2	3
Hewlett-Packard pro one 600	Infraestructura	2	4	2	3

Nombre del Activo	**Ubicación**	**Valoración de la pérdida del activo**			
		Confidencialidad	**Disponibilidad**	**Integridad**	**Total del impacto**
ASUS P1440F	Operativo	3	4	3	3
Hewlett-Packard pro one 600	Proyectos	3	4	3	3
Hewlett-Packard pro one 600	Seguridad vial	2	4	2	3
Laptop DELL	Auditoria	3	3	2	3
Laptop Asus	Gestión fibra	3	3	2	3
Hewlett-Packard pro one 600	Logística	2	4	2	3
Hewlett-Packard RTL8723DE	Técnico	2	4	2	3

En este análisis, se pueden identificar vulnerabilidades en la información. En particular, se observa que algunos de los equipos de la empresa tienen un alto grado de exposición a riesgos relacionados con la protección de datos en su software. De estos equipos, 4 muestran una alta disponibilidad de información, mientras que 3 almacenan datos críticos para la empresa en sus bases de datos. En conjunto, todos los activos presentan un impacto significativo para la organización, lo que significa que existe un nivel considerable de vulnerabilidad que afecta las dimensiones de confidencialidad, integridad y disponibilidad en cada uno de estos activos cuando se materializan amenazas. Una vez analizada la situación de la seguridad en la cual se encuentra la empresa, donde se observa que las medidas decontrol son muy bajas y los planes para tratar los riesgos son escasos, se procede a proponer un sistema de gestión de seguridad de la información, para lo cual se toma en cuenta los criterios de aceptación del riesgo según la ISO/IEC 27001:

2013 norma desarrollada por la ISO y la IEC.

2.2.7 Riesgos del área de Contact center

Tabla 18

Matriz categorización de riesgos

Situación	Procesos de riesgo	Activos afectados	Caracterización		Calificación	
			Fr	Int	B	Gama de color
Interrupción del servicio eléctrico	Falla en la fuente de energía de los equipos.	Telefonía, computadoras, sistemas	PP	MD	A	
Interrupción del servicio de internet	Falla en la conexión a internet.	Telefonía, sistemas	PR	MD	Mda	
Interrupción del servicio telefónico	Falla en la red telefónica.	Telefonía	PP	B	A	
Falla en el sistema de grabación de llamadas	Pérdida de información.	Grabaciones de llamadas	PR	B	A	
Brecha de seguridad informática	Ataque de hackers o phishing.	Información de clientes y agentes, sistemas	PP	B	A	
Fuga de información	Acceso no autorizado a información confidencial.	Información de clientes y agentes	PP	MD	Mda	

Situación	Procesos de riesgo	Activos afectados	Caracterización		Calificación	
			Fr	Int	B	Gama de color
Falta de personal capacitado	Falta de habilidades para resolver problemas de los clientes.	Servicio al cliente	PP	Mda	A	
Falta de recursos tecnológicos	Falta de equipos o software adecuados	Telefonía, computadoras, sistemas	PP	MD	Mda	

Fuente: Portal Administración Electrónica (P.A. E. 2012)

Según los datos obtenidos den la tabla 18 se identifican varios riesgos que deben considerarse para garantizar el funcionamiento eficiente y seguro de este departamento en las organizaciones. Uno de los riesgos identificados es la interrupción del servicio eléctrico, que puede ocurrir debido a fallas en la fuente de energía de los equipos. Esto afecta a los activos de telefonía, computadoras y sistemas, y se califica como un riesgo de impacto medio. Otro riesgo es la interrupción del servicio de internet, que puede surgir debido a fallas en la conexión a internet. Esto afecta a los activos de telefonía y sistemas, y se califica como un riesgo de impacto medio a moderado. La interrupción del servicio telefónico es otro riesgo identificado, relacionado con fallas en la red telefónica. Esto afecta al activo de telefonía y se califica como un riesgo de alto impacto. La falla en el sistema de grabación de llamadas es un riesgo que puede resultar en la pérdida de información. Esto afecta al activo de grabaciones de llamadas y se califica como un riesgo de alto impacto.

La brecha de seguridad informática es un riesgo significativo que se relaciona directamente con ataques informáticos, como los ataques de phishing. Esto pone en peligro la información de clientes y agentes, así como los sistemas, y se califica como un riesgo de alto impacto. La fuga de información es otro riesgo que implica el acceso no autorizado a información confidencial de clientes y agentes. Se califica como un riesgo de impacto medio a moderado. La falta de personal

capacitado es otro riesgo identificado, lo cual implica la falta de habilidades para resolver problemas de los clientes en el servicio de atención al cliente. Se califica como un riesgo de alto impacto y moderada probabilidad de ocurrencia.

El ruido en el ambiente de trabajo es un riesgo que puede generar interrupciones en las llamadas y afectar la calidad de las mismas. Se califica como un riesgo de impacto medio a moderado. Finalmente, la falta de recursos tecnológicos es otro riesgo identificado, que implica la falta de equipos o software adecuados para el Contact Center. Esto afecta a los activos de telefonía, computadoras y sistemas, y se califica como un riesgo de impacto medio a moderado. Es esencial abordar estos riesgos y tomar las medidas adecuadas para mitigarlos y garantizar el funcionamiento seguro y eficiente del Contact Center. Esto implica la implementación de medidas de seguridad informática, capacitación del personal, disponibilidad de recursos tecnológicos adecuados y la adopción de medidas para garantizar la continuidad del servicio en caso de interrupciones en la energía eléctrica, internet o telefonía.

Tabla 19

Nivel de valoración equipos

Nombre del Activo	**Ubicación**	**Valoración de la pérdida del activo**			
		Confidencialidad	**Disponibilidad**	**Integridad**	**Total del impacto**
Hewlett-Packard 2B5A	Auxiliar Contact Center	2	4	2	3

En este análisis, se han identificado vulnerabilidades en la gestión de la información. Es evidente que varios de los sistemas informáticos de la empresa enfrentan riesgos considerables en cuanto a la seguridad de los datos. Entre estos sistemas, cuatro de ellos muestran una alta capacidad de recuperación de información, mientras que tres almacenan datos críticos para el funcionamiento de la empresa en sus bases de datos. En resumen, todos los activos evaluados tienen un impacto significativo en la organización, lo que significa que existe un nivel

considerable de vulnerabilidad que afecta la confidencialidad, la integridad y la disponibilidad de la información cuando se producen amenazas.

Una vez analizada la situación de la seguridad en la cual se encuentra la empresa, donde se observa que las medidas de control son muy bajas y los planes para tratar los riesgos son escasos, se procede a proponer un sistema de gestión de seguridad de la información, para lo cual se toma en cuenta los criterios de aceptación del riesgo según la ISO/IEC 27001: 2013 norma desarrollada por la ISO y la IEC.

2.2.8 Riesgos del área de Ingeniería y gestión

Una vez se identifique su caracterización se procede a calificar los riesgos:

Tabla 20

Matriz categorización de riesgos

Situación	Procesos de riesgo	Activos afectados	Caracterización		Calificación	
			Fr	Int	Cob	Gama de color
Mantenimiento y prevención de riesgos en los equipos	Falta de mantenimiento en el sistema antincendios: pérdida en un incendio	Hardware	PP	B	A	
	No se posee un amplio sistema de refrigeración: sobrecalentamiento y daño de los equipos	Hardware	PR	MD	Mda	

Situación	Procesos de riesgo	Activos afectados	Caracterización		Calificación	
			Fr	Int	Cob	Gama de color
	No existe control sobre las personas que ingresan y salen de las oficinas del área: robo	Equipos y dispositivos	I	B	A	
	Error en la manipulación de las redes: conexiones inseguras	Redes	PP	Mda	A	
	No se tienen los equipos correctamente inventariados: robos	Hardware	PP	B	A	
Comunicaciones	Ataques cibernéticos a través de correos electrónicos y mensajes instantáneos	Comunicaciones	PP	Mda	A	
	Escuchas telefónicas y grabaciones no autorizadas	Comunicaciones	PR	AL	T	
	Fugas de información a través de la transmisión de datos no segura	Datos	PP	MD	Mda	
	Mal uso de las herramientas de comunicación y	Herramientas de comunicación	MP	MD	Mda	

Situación	Procesos de riesgo	Activos afectados	Caracterización		Calificación	
			Fr	Int	Cob	Gama de color
	colaboración					
Infraestructura de red	Mal uso de las herramientas de administración de red	Herramientas de administración	pp	AL	Mda	

Fuente: Portal Administración Electrónica (PAE, 2012)

Según los datos obtenidos en la tabla 20, que se enfoca en el área de ingeniería y gestión, y tiene como objetivo identificar y clasificar los riesgos asociados a diferentes situaciones y procesos. Esta matriz es fundamental para comprender y gestionar los riesgos a los que se enfrenta una organización en esta área específica. En relación al mantenimiento y prevención de riesgos en los equipos, se identifican varios riesgos relacionados con el hardware. Entre ellos, se menciona la falta de mantenimiento en el sistema antincendios, lo que podría resultar en la pérdida de equipos en caso de un incendio. También se destaca la falta de un amplio sistema de refrigeración, lo que podría ocasionar sobrecalentamiento y daño a los equipos. Otro riesgo identificado es la ausencia de control sobre las personas que ingresan y salen de las oficinas del área, lo que podría llevar a robos de equipos y dispositivos.

Además, se mencionan errores en la manipulación de las redes, lo que podría resultar en conexiones inseguras, así como la falta de un inventario adecuado de los equipos, lo que aumenta el riesgo de robos. En cuanto a las comunicaciones, se destacan los ataques cibernéticos a través de correos electrónicos y mensajes instantáneos como una amenaza relevante. También se mencionan las escuchas telefónicas y grabaciones no autorizadas, así como las fugas de información a través de la transmisión de datos no segura. Además, se identifica el mal uso de las herramientas de comunicación y colaboración como un riesgo que debe ser abordado. En relación a la infraestructura de red, se señala el mal uso de las herramientas de administración de red como un riesgo significativo que podría afectar la gestión eficiente de la infraestructura.

Tabla 21

Nivel de valoración equipos

Nombre del Activo	Ubicación	Valoración de la pérdida del activo			
		Confidencialidad	Disponibilidad	Integridad	Total del impacto
Hewlett-Packard pro one 600	Ingeniería y gestión	2	4	2	3
Hewlett-Packard pro one 600	Analista de red	2	4	2	3
Hewlett-Packard pro one 600	Mantenimiento e IPTV	3	4	3	3
Hewlett-Packard pro one 600	Gerencia de ingeniería	3	4	3	3
Hewlett-Packard pro one 600	Noc (Network operation center)	3	3	3	3

En este análisis, se han identificado posibles debilidades en la gestión de la información. Es claro que algunos de los sistemas informáticos de la empresa enfrentan riesgos considerables en cuanto a la seguridad de los datos. De hecho, cuatro de estos sistemas tienen una alta capacidad de recuperación de información, mientras que tres almacenan datos críticos para el funcionamiento de la empresa en sus bases de datos. En resumen, todos los activos evaluados tienen un impacto significativo en la organización, lo que implica un nivel considerable de vulnerabilidad que afecta la confidencialidad, la integridad y la disponibilidad de la información cuando se producen amenazas.

Una vez analizada la situación de la seguridad en la cual se encuentra la empresa, donde se observa que las medidas de control son muy bajas y los planes para tratar los riesgos son escasos, se procede a proponer un sistema de gestión de seguridad de la información, para lo cual se toma en cuenta los criterios de aceptación del riesgo según la ISO/IEC 27001: 2013 norma desarrollada por la ISO y la IEC.

2.2.9 Riesgos del área de producto y servicio

Tabla 22

Matriz categorización de riesgos

Situación	**Procesos de riesgo**	**Activos afectados**	**Caracterización**		**Calificación**	
			Fr	**Int**	**Cob**	**Gama de color**
Protección de datos de clientes	Falta de medidas de seguridad en la transferencia de datos personales	Información de clientes	PP	B	A	
Robo o pérdida de equipos	Ausencia de medidas de seguridad física en la oficina	Equipos de cómputo	PP	MD	Mda	
Fugas de información confidencial	Falta de control de acceso a la información	Información confidencial de clientes (datos financieros, datos personales)	PP	B		
Malware y virus	Falta de actualización de antivirus y firewall	Sistemas y equipos de cómputo	PR	Mda	A	
Fraude y	Ausencia de	Personal y	PP	B	A	

Situación	Procesos de riesgo	Activos afectados	Caracterización		Calificación	
			Fr	Int	Cob	Gama de color
phishing	políticas claras y entrenamiento del personal en seguridad de la información	sistemas de información				

Fuente: Portal Administración Electrónica (PAE, 2012)

Según los datos obtenidos de la tabla 22, está enfocada en el área de producto y servicio tiene como objetivo identificar y clasificar los riesgos asociados a diferentes situaciones y procesos dentro de esta área específica. El análisis de riesgos es fundamental para garantizar la protección de los datos de los clientes, así como la seguridad de los equipos, la confidencialidad de la información y la prevención de fraudes y ataques cibernéticos. En relación a la protección de datos de clientes, se identifica como un riesgo importante la falta de medidas de seguridad en la transferencia de datos personales. Esto puede poner en peligro la información de los clientes. El robo o pérdida de equipos es un riesgo, especialmente cuando no se implementan medidas de seguridad física en la oficina.

Esto puede afectar los equipos de cómputo y comprometer la integridad de la información. Otro riesgo identificado es la posibilidad de fugas de información confidencial debido a la falta de control de acceso. Esto implica un riesgo para la información confidencial de los clientes, como datos financieros y personales. Además, se destaca la importancia de mantener actualizados los sistemas y equipos de cómputo con antivirus y firewall. La falta de actualización puede hacer que los sistemas sean vulnerables a malware y virus. Por último, se menciona el riesgo de fraude y phishing debido a la ausencia de políticas claras y entrenamiento del personal en seguridad de la información. Esto puede comprometer tanto al personal como a los sistemas de información de la organización.

Tabla 23

Nivel de valoración equipos

Nombre del Activo	Ubicación	Valoración de la pérdida del activo			
		Confidencialidad	Disponibilidad	Integridad	Total del impacto
Hewlett-Packard pro one 600	Consultor servicios empresariales	2	4	2	3
Hewlett-Packard pro one 600	Cuidado al Cliente	2	4	2	3
Hewlett-Packard pro one 600	Producto y servicio	3	4	3	3
Laptop DELL	Aseso Residencial	3	4	3	3

En este análisis, hemos identificado posibles áreas de vulnerabilidad en la gestión de la información. Es evidente que algunos de los sistemas informáticos de la empresa enfrentan riesgos considerables en cuanto a la seguridad de los datos. De hecho, cuatro de estos sistemas tienen una alta capacidad de recuperación de información, mientras que tres almacenan datos críticos para el funcionamiento de la empresa en sus bases de datos. En resumen, todos los activos evaluados tienen un impacto significativo en la organización, lo que implica un nivel considerable de vulnerabilidad que afecta la confidencialidad, la integridad y la disponibilidad de la información cuando se producen amenazas. Una vez analizada la situación de la seguridad en la cual se encuentra la empresa, donde se observa que las medidas de control son muy bajas y los planes para tratar los riesgos son escasos, se procede a proponer un sistema de gestión de seguridad de la información, para lo cual se toma en cuenta los criterios de aceptación del riesgo según la ISO/IEC 27001: 2013 norma desarrollada por la ISO y la IEC.

2.2.10 Riesgos del área de talento humano

Una vez se identifique su caracterización se procede a calificar los riesgos:

Tabla 24

Matriz categorización de riesgos

Situación	Procesos de riesgo	Activos afectados	Caracterización		Calificación	
			Fr	Int	Cob	Gama de color
Acceso a información de los empleados	Poco control de acceso a los sistemas	Bases de datos de empleados	PP	B	A	
Falta de políticas de privacidad	Fuga de información confidencial	Documentación y registros de empleados	PR	MD	Mda	
Errores en la gestión de permisos de acceso	Acceso no autorizado a información de empleados	Sistemas de información de empleados	PP	B	A	
Falta de protección de los datos de empleados	Pérdida o robo de datos de empleados	Copias de seguridad de información de empleados	PR	Mda	A	
Ausencia de protocolos de seguridad para la selección de personal	Ingreso de personal no confiable	Registros de selección de personal	PR	A	Mda	
Falta de protocolos de	Fuga de información	Registros de nómina	PR	MD	Mda	

Situación	Procesos de riesgo	Activos afectados	Caracterización		Calificación	
			Fr	Int	Cob	Gama de color
seguridad en la gestión de nóminas	financiera de los empleados					
Ausencia de medidas de seguridad para la transferencia de información	Pérdida de información al enviarla a terceros	Registros de transferencias de información	MP	Mda	A	

Fuente: Portal Administración Electrónica (PAE, 2012).

Según los datos obtenidos de la tabla 24 se puede evidenciar que su objetivo es identificar y clasificar los riesgos asociados a diferentes situaciones y procesos en esta área específica. El análisis de riesgos es esencial para garantizar la protección de la información confidencial de los empleados, establecer políticas de privacidad adecuadas y mitigar posibles amenazas. Uno de los riesgos identificados es el acceso no controlado a los sistemas, lo cual puede comprometer las bases de datos de empleados. Este riesgo se caracteriza por una frecuencia de probabilidad y una intensidad media, lo que indica la importancia de implementar medidas de control y restricción de acceso. La falta de políticas de privacidad también se destaca como un riesgo, ya que puede resultar en fugas de información confidencial relacionada con la documentación y los registros de los empleados. Este riesgo se caracteriza por una probabilidad probable y una intensidad moderada, lo que requiere la implementación de políticas adecuadas para proteger la confidencialidad de la información.

Los errores en la gestión de los permisos de acceso representan otro riesgo importante, ya que pueden conducir a un acceso no autorizado a la información de los empleados. Este riesgo se caracteriza por una probabilidad probable y una intensidad baja, lo que resalta la necesidad de establecer protocolos claros de gestión de permisos. Además, se identifica la falta de protección de los datos de los empleados como un riesgo significativo. Esto implica la posibilidad de pérdida

o robo de datos de los empleados almacenados en las copias de seguridad. Este riesgo se caracteriza por una probabilidad probable y una intensidad moderada, lo que enfatiza la importancia de implementar medidas de seguridad adecuadas para salvaguardar la información. La ausencia de protocolos de seguridad en la selección de personal es otro riesgo a tener en cuenta. Esto puede resultar en la incorporación de personal no confiable, lo que afectaría los registros de selección de personal. Este riesgo se caracteriza por una probabilidad probable y una intensidad alta, lo que destaca la necesidad de establecer protocolos rigurosos de seguridad en el proceso de selección. La falta de protocolos de seguridad en la gestión de nóminas también se considera un riesgo, ya que puede resultar en fugas de información financiera de los empleados a través de los registros de nómina.

Este riesgo se caracteriza por una probabilidad probable y una intensidad moderada, lo que indica la importancia de establecer controles adecuados en el manejo de la información financiera. Finalmente, se menciona la ausencia de medidas de seguridad para la transferencia de información como un riesgo significativo. Esto puede resultar en pérdida de información al enviarla a terceros a través de los registros de transferencias de información. Este riesgo se caracteriza por una probabilidad muy probable y una intensidad moderada, lo que subraya la necesidad de implementar medidas de seguridad efectivas en los procesos de transferencia.

Tabla 25

Nivel de valoración equipos

Nombre del Activo	**Ubicación**	**Valoración de la pérdida del activo**			
		Confidencialidad	**Disponibilidad**	**Integridad**	**Total del impacto**
Hewlett-Packard pro one 600	SST	2	4	2	3
Hewlett-Packard pro one 600	Jurídica	2	4	2	3

En este análisis, hemos identificado posibles vulnerabilidades en la gestión de la información.

Es evidente que algunos de los sistemas informáticos de la empresa enfrentan riesgos considerables en cuanto a la seguridad de los datos. De hecho, cuatro de estos sistemas tienen una alta capacidad de recuperación de información, mientras que tres almacenan datos críticos para el funcionamiento de la empresa en sus bases de datos. En resumen, todos los activos evaluados tienen un impacto significativo en la organización, lo que implica un nivel considerable de vulnerabilidad que afecta la confidencialidad, la integridad y la disponibilidad de la información cuando se producen amenazas.

Una vez analizada la situación de la seguridad en la cual se encuentra la empresa, donde se observa que las medidas de control son muy bajas y los planes para tratar los riesgos son escasos, se procede a proponer un sistema de gestión de seguridad de la información, para lo cual se toma en cuenta los criterios de aceptación del riesgo según la ISO/IEC 27001: 2013 norma desarrollada por la ISO y la IEC.

2.2.11 Riesgos del área de proyectos TI

Una vez se identifique su caracterización se procede a calificar los riesgos

Tabla 26

Matriz categorización de riesgos

Situación	Procesos de riesgo	Activos afectados	Caracterización		Calificación	
			Fr	Int	Cob	Gama de color
Desarrollo de software	Uso de librerías y componentes no confiables: Posible introducción de código malicioso.	Código fuente	PR	MD	A	
	Falta de revisión de código: Posibles	Código fuente	PR	MD	Mda	

Situación	Procesos de riesgo	Activos afectados	Caracterización		Calificación	
			Fr	Int	Cob	Gama de color
	errores y vulnerabilidades.					
	No se realizan pruebas de penetración: Posible explotación de vulnerabilidades.	Sistemas en producción	MP	MD	A	
	No se posee un correcto control de versiones: Pérdida de código fuente y posible contaminación del mismo	Código fuente	PR	Mda	A	
Administración de servidores	Falta de actualizaciones de seguridad: Posible explotación de vulnerabilidades	Servidores	PP	B	A	
	Configuración segura de servicios: Posible exposición de información sensible.	Servidores	PP	MD	Mda	
	Falta de monitoreo de los servicios: Posible compromiso de los mismos	Servidores	PP	B	A	 

Situación	Procesos de riesgo	Activos afectados	Caracterización		Calificación	
			Fr	Int	Cob	Gama de color
	No se posee un plan de contingencia: Posible pérdida de información	Información de los servidores	PP	B	Mda	
Seguridad en Red	Uso de contraseñas débiles: Posible compromiso de los sistemas	Uso de contraseñas débiles: Posible compromiso de los sistemas	MP	MD	Mda	
Gestión de proyectos	Falta de un plan de seguridad en el ciclo de vida de desarrollo de software: Posible introducción de vulnerabilidades	Ciclo de vida del proyecto	PP	B	Mda	
	No se posee una correcta gestión de riesgos en los proyectos: Posible exposición de información sensible	Proyectos	PP	B	P	

Fuente: Portal Administración Electrónica (PAE, 2012)

Según los datos obtenidos den la tabla 26 se puede evidenciar que su objetivo es identificar y clasificar los riesgos asociados a diferentes situaciones y procesos en esta área específica. El análisis de riesgos es esencial para garantizar la protección de la información confidencial de los empleados, establecer políticas de privacidad adecuadas y mitigar posibles amenazas. Uno de los riesgos identificados es el acceso no controlado a los sistemas, lo cual puede comprometer las

bases de datos de empleados. Este riesgo se caracteriza por una frecuencia de probabilidad y una intensidad media, lo que indica la importancia de implementar medidas de control y restricción de acceso. La falta de políticas de privacidad también se destaca como un riesgo, ya que puede resultar en fugas de información confidencial relacionada con la documentación y los registros de los empleados. Este riesgo se caracteriza por una probabilidad probable y una intensidad moderada, lo que requiere la implementación de políticas adecuadas para proteger la confidencialidad de la información.

Los errores en la gestión de los permisos de acceso representan otro riesgo importante, ya que pueden conducir a un acceso no autorizado a la información de los empleados. Este riesgo se caracteriza por una probabilidad probable y una intensidad baja, lo que resalta la necesidad de establecer protocolos claros de gestión de permisos. Además, se identifica la falta de protección de los datos de los empleados como un riesgo significativo. Esto implica la posibilidad de pérdida o robo de datos de los empleados almacenados en las copias de seguridad. Este riesgo se caracteriza por una probabilidad probable y una intensidad moderada, lo que enfatiza la importancia de implementar medidas de seguridad adecuadas para salvaguardar la información. La ausencia de protocolos de seguridad en la selección de personal es otro riesgo a tener en cuenta. Esto puede resultar en la incorporación de personal no confiable, lo que afectaría los registros de selección de personal.

Este riesgo se caracteriza por una probabilidad probable y una intensidad alta, lo que destaca la necesidad de establecer protocolos rigurosos de seguridad en el proceso de selección. La falta de protocolos de seguridad en la gestión de nóminas también se considera un riesgo, ya que puede resultar en fugas de información financiera de los empleados a través de los registros de nómina. Este riesgo se caracteriza por una probabilidad probable y una intensidad moderada, lo que indica la importancia de establecer controles adecuados en el manejo de la información financiera.

Tabla 27

Nivel de valoración equipo

Nombre del Activo	**Ubicación**	**Valoración de la pérdida del activo**			
		Confidencialidad	**Disponibilidad**	**Integridad**	**Total del impacto**
Hewlett-Packard pro one 600	Coordinador de innovación	2	4	2	3
Hewlett-Packard pro one 600	Auxiliar de innovación	2	4	2	3

En este análisis, hemos identificado potenciales vulnerabilidades en la gestión de la información. Es evidente que algunos de los sistemas informáticos de la empresa enfrentan riesgos considerables en cuanto a la seguridad de los datos. De hecho, cuatro de estos sistemas tienen una alta capacidad de recuperación de información, mientras que tres almacenan datos críticos para el funcionamiento de la empresa en sus bases de datos. En resumen, todos los activos evaluados tienen un impacto significativo en la organización, lo que implica un nivel considerable de vulnerabilidad que afecta la confidencialidad, la integridad y la disponibilidad de la información cuando se producen amenazas.

Una vez analizada la situación de la seguridad en la cual se encuentra la empresa, donde se observa que las medidas de control son muy bajas y los planes para tratar los riesgos son escasos, se procede a proponer un sistema de gestión de seguridad de la información, para lo cual se toma en cuenta los criterios de aceptación del riesgo según la ISO/IEC 27001: 2013 norma desarrollada por la ISO y la IEC. Se llevó a cabo un análisis exhaustivo de las amenazas que enfrentan las áreas funcionales de SP Sistemas Palacios Ltda. Para ello, se realizaron entrevistas a profundidad con el personal clave de cada área, y se aplicaron técnicas de análisis de riesgos para identificar los factores que podrían afectar negativamente el desempeño de la empresa en cada una de estas áreas.

Los resultados de este análisis permitieron identificar un conjunto de amenazas potenciales en cada una de las áreas funcionales de SP Sistemas Palacios Ltda. El análisis realizado objetivo permitió identificar un conjunto de amenazas potenciales en cada una de las áreas funcionales de SP Sistemas Palacios LTDA, lo que proporciona una base sólida para la toma de decisiones estratégicas en la empresa. Con esta información, la empresa puede enfocar sus esfuerzos en mitigar los riesgos asociados a estas amenazas, y aprovechar las oportunidades identificadas, para garantizar su éxito y sostenibilidad en el largo plazo.

2.3 Propuesta del Sistema de Gestión de la Seguridad de la Información SGSI para la empresa SP Sistemas Palacios LTDA. basado en el estándar ISO/IEC 27001

2.3.1 Resumen ejecutivo

La presente propuesta tiene como objetivo principal la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) en la empresa SP Sistemas Palacios Ltda, basado en la norma ISO/IEC 27001. El propósito de este SGSI es salvaguardar la confidencialidad, integridad y disponibilidad de la información crítica de la organización, así como asegurar el cumplimiento de los requisitos legales y regulatorios relacionados con la seguridad de la información.

2.3.2 Introducción

La seguridad de la información es un componente esencial en el entorno empresarial actual, donde la digitalización y la interconexión de sistemas desempeñan un papel central. La empresa SP Sistemas Palacios LTDA, al reconocer la crítica importancia de salvaguardar sus activos de información y datos confidenciales, ha iniciado un proceso clave: la creación de un Sistema de Gestión de la Seguridad de la Información (SGSI). Esta propuesta de SGSI se fundamenta en el estándar internacional ISO/IEC 27001, una guía probada y reconocida para la gestión de la seguridad de la información. Este trabajo se adentra en el análisis y diseño del SGSI para SP Sistemas Palacios LTDA, comenzando con una evaluación de riesgos integral. Basándose en la norma ISO/IEC 27001:2013, se siguen los principios del ciclo PHVA (Planificar, Hacer, Verificar, Actuar) para guiar la creación y evolución del SGSI.

A través de este enfoque, esta propuesta busca no solo identificar y mitigar riesgos de seguridad de la información, sino también establecer un proceso de mejora continua. Cada fase del ciclo PHVA, desde la planificación hasta la acción, se ejecutará de manera sistemática y basada en datos para asegurar que SP Sistemas Palacios Ltda alcance y mantenga los más altos estándares de seguridad de la información.

2.3.3 Objetivos

Objetivo General

Diseñar, implementar y mantener un Sistema de Gestión de la Seguridad de la Información (SGSI) en la empresa SP Sistemas Palacios Ltda, basado en la norma ISO/IEC 27001, que garantice la confidencialidad, integridad y disponibilidad de la información, y promueva una cultura de seguridad informática en toda la organización.

Objetivos Específicos

- Identificar y Evaluar Riesgos: Realizar un análisis exhaustivo de los riesgos de seguridad de la información a los que está expuesta la empresa, utilizando la metodología MAGERIT, para determinar las amenazas y vulnerabilidades críticas.
- Definir Políticas de Seguridad: Establecer políticas y procedimientos de seguridad de la información que cumplan con los requisitos de la norma ISO/IEC 27001, considerando las especificidades y necesidades de SP Sistemas Palacios LTDA.
- Diseñar Controles de Seguridad: Identificar y diseñar controles de seguridad adecuados para mitigar los riesgos identificados en el análisis de riesgos, centrándose en los niveles medio, alto y muy alto.
- Implementar el SGSI: Llevar a cabo la implementación del Sistema de Gestión de la Seguridad de la Información, incluyendo la instalación de controles, la capacitación del personal y la difusión de las políticas de seguridad.
- Realizar Auditorías Internas: Realizar auditorías internas periódicas para evaluar el cumplimiento de los controles de seguridad y la efectividad del SGSI, identificando áreas

de mejora.

- Mejora Continua: Basándose en los resultados de las auditorías y en las retroalimentaciones del personal, aplicar medidas correctivas y preventivas para mejorar constantemente el SGSI y su desempeño.
- Promover la Conciencia de Seguridad: Fomentar una cultura de seguridad informática entre el personal de SP Sistemas Palacios Ltda a través de programas de concienciación y capacitación.
- Cumplimiento Legal y Regulatorio: Asegurar que el SGSI cumpla con todas las leyes y regulaciones aplicables relacionadas con la seguridad de la información.
- Gestión de Incidentes de Seguridad: Establecer un procedimiento de gestión de incidentes de seguridad que permita responder de manera eficiente a posibles violaciones de la seguridad de la información.
- Evaluación Externa: Preparar y coordinar la evaluación externa del SGSI por parte de organismos de certificación reconocidos, con el objetivo de obtener la certificación ISO/IEC 27001.

2.3.4 Alcance de la propuesta

Esta propuesta tiene como objetivo principal la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) en la empresa SP Sistemas Palacios Ltda, siguiendo las pautas y requisitos establecidos en la norma ISO/IEC 27001.

2.3.5 Áreas involucradas

- Área administrativa y financiera.
- Área de operaciones.
- Área de Contact Center.
- Área de ingeniería y gestión.
- Área de producto y servicio.
- Área de talento humano.
- Área de proyectos TI.

2.3.6 Objetivos del SGSI

El SGSI tiene como objetivos fundamentales:

- Identificar y evaluar los riesgos de seguridad de la información en cada área de la organización.
- Definir políticas y procedimientos de seguridad de la información que cumplan con los estándares de la norma ISO/IEC 27001:2013.
- Establecer controles de seguridad adecuados para garantizar la confidencialidad, integridad y disponibilidad de la información.
- Cumplir con los requisitos legales y regulaciones aplicables en materia de seguridad de la información.
- Promover una cultura de seguridad de la información entre los empleados de la empresa.

2.3.7 Alcance de los controles de seguridad

Los controles de seguridad de la información se implementarán en todas las áreas de la organización y abordarán aspectos como:

- Control de acceso físico y lógico a instalaciones y sistemas.
- Gestión de activos de información.
- Evaluación y tratamiento de riesgos de seguridad.
- Políticas y procedimientos de seguridad de la información.
- Planificación de la continuidad del negocio y recuperación ante desastres.
- Gestión de proveedores y terceros.
- Monitoreo y respuesta a incidentes de seguridad.

2.3.8 Recursos y cronograma

El proyecto requerirá recursos humanos, tecnológicos y de capacitación. El cronograma estimado de implementación es de [indicar la duración estimada].

2.3.9 Certificación ISO/IEC 27001

El proyecto buscará obtener la certificación ISO/IEC 27001:2013 una vez que se haya completado la implementación del SGSI. Esto incluirá la auditoría por parte de un organismo de certificación externo.

2.3.10 Mantenimiento y Mejora Continua

Después de la implementación inicial, se establecerá un proceso continuo de monitoreo, mantenimiento y mejora del SGSI para asegurar su efectividad a lo largo del tiempo.

Tomando en cuenta el estándar ISO/IEC 27001 de la norma se inicia con la propuesta con los siguientes pasos:

2.3.11 Pasos en la Evaluación y Gestión de Riesgos de Seguridad de la Información según ISO/IEC 27001

- **Análisis de riesgos:** Según la norma ISO/IEC 27001 se debe partir de la realización de un análisis de riesgos y de la planificación e implantación de la respuesta a los mismos para su mitigación. Existen cuatro opciones que ayudan a dar un correcto tratamiento a los riesgos, como los siguientes:

- **Aceptación del riesgo**: se debe tener un constante monitoreo y revisión periódica de los mismos con el fin de responder oportunamente ante su materialización

- **Reducción del riesgo**: Cuando el nivel de riesgo es superior al criterio de aceptación se debe realizar una correcta selección de controles los cuales ayuden a disminuir el riesgo.

- **Transferencia del riesgo**: cuando el riesgo se lo puede compartir o transferir a una entidad externa la cual pueda manejar este riesgo de una forma más eficiente.

- **Evitación del riesgo**: se procede a evitar por completo este tipo de riesgos, por lo cual se procede a eliminar o modificar las actividades o procedimientos que pueden ser la causa de dichos riesgos

- **Criterios para el tratamiento del riesgo:** Con las cuatro opciones antes mencionadas se procede a establecer el tratamiento correspondiente a cada una de las zonas que se pudo determinar mediante el cálculo del riesgo.

- **Acciones correctivas para el tratamiento del riesgo:** Como los riesgos a los cuales están expuestos los activos que dispone la empresa son de diferente nivel las acciones propuestas también se deben centrar en los niveles medio, alto y muy alto

2.3.12 Análisis de riesgos y acciones de mitigación en SP Sistemas Palacios Ltda: enfoque en la seguridad de la información

En el caso de la empresa SP Sistemas Palacios Ltda, se llevó a cabo el análisis de riesgos utilizando la metodología MAGERIT, la cual permitió identificar las zonas de riesgo de los activos de la empresa. En base a esta información, se establecieron criterios para el tratamiento correspondiente a cada zona de riesgo. Las acciones propuestas se centraron en los niveles medio, alto y muy alto de riesgo El criterio de aceptación del riesgo implicó un constante monitoreo y revisión periódica de los mismos con el fin de responder oportunamente ante su materialización. En el caso de la reducción del riesgo, se seleccionaron controles que ayudaron a disminuir el riesgo hasta un nivel que se considerara aceptable y manejable para la organización. En este contexto, "disminuir el riesgo hasta un nivel adecuado" significa implementar medidas de control que reduzcan la probabilidad de que un riesgo se materialice y/o minimicen el impacto en caso de que ocurra, de manera que el riesgo restante sea coherente con los objetivos y recursos de la organización, y no represente una amenaza significativa para sus operaciones y activos.

El análisis de riesgos y la planificación de la respuesta a los mismos para su mitigación son esenciales para garantizar la seguridad de la información de la empresa SP Sistemas Palacios LTDA. Este proceso permitió establecer los criterios adecuados para el tratamiento de los riesgos

identificados y asegurar la implementación de controles necesarios para disminuir el nivel de riesgo a niveles aceptables. Durante el proceso de evaluación de riesgos en la empresa SP Sistemas Palacios Ltda, se identificaron diversos procesos que representan un riesgo significativo para la seguridad de la información.

Según el análisis realizado en cada una de las áreas se puede deducir lo siguiente en cada una de ellas:

2.3.13 Área administrativa y financiera

Se han identificado varios procesos de riesgo que afectan los activos críticos de la organización en diferentes áreas. En la infraestructura física, la falta de mantenimiento en el sistema antincendios representa una amenaza directa, ya que podría ocasionar la pérdida de equipos de cómputo y documentos importantes. Para mitigar este riesgo, se deben implementar medidas de mantenimiento y prevención adecuadas en el sistema antincendios. Además, la carencia de un amplio sistema de refrigeración aumenta el riesgo de sobrecalentamiento y daño de los equipos, por lo que se requiere una solución de refrigeración eficaz. Asimismo, la falta de control sobre el acceso a las oficinas del área administrativa y financiera podría dar lugar a robos de documentos importantes. Para abordar este problema, se deben establecer controles de acceso y seguridad adecuados. La gestión inadecuada de las conexiones de red y la ausencia de un inventario completo de equipos también incrementan la vulnerabilidad de la organización, lo que destaca la necesidad de controles de seguridad en la manipulación de redes y un inventario preciso de activos.

En el ámbito del sistema operativo Windows, se han detectado errores en la configuración de seguridad, lo que genera riesgos de ciberataques. Para contrarrestar este problema, es crucial realizar una revisión exhaustiva de la configuración de seguridad y corregir los errores identificados. La falta de generación correcta de roles y sistemas de control plantea preocupaciones adicionales, ya que podría resultar en la pérdida de información confidencial. Para abordar esta vulnerabilidad, se debe establecer un proceso de gestión de roles y controles efectivo. Además, se ha notado la ausencia de políticas claras y personal designado para la

gestión de documentación, lo que aumenta la exposición a riesgos. La implementación de políticas de gestión de documentos y la asignación de responsabilidades claras pueden ayudar a resolver este problema. La dificultad en la manipulación de las interfaces del sistema puede generar errores y la falta de bloqueo de los equipos al abandonar el puesto de trabajo puede ocasionar un uso indebido de los mismos. Para mejorar la usabilidad y la seguridad, se deben realizar capacitaciones y establecer políticas de bloqueo de equipos. La inexistencia de copias de seguridad y el mal funcionamiento del software son riesgos adicionales que pueden impactar la integridad de los datos cruciales. Para proteger los datos importantes, es esencial implementar políticas de copia de seguridad y mantener un software adecuadamente actualizado y funcional.

En lo que respecta al personal de planta, se ha identificado la falta de controles de seguridad, lo que podría permitir el robo de documentación importante. La implementación de controles de seguridad adecuados y la supervisión continua son esenciales para abordar esta amenaza. La carencia de personal calificado y la ausencia de políticas y controles anti spam también han sido identificados como riesgos, con potencial para afectar la productividad y la seguridad de los datos. Para mejorar la formación y la seguridad del personal, se deben ofrecer programas de capacitación y establecer políticas anti spam efectivas. Por último, en cuanto a las instalaciones, se ha notado que los controles de acceso actuales son básicos, lo que representa un riesgo de acceso no autorizado a documentos importantes. Para fortalecer la seguridad de las instalaciones, se deben implementar controles de acceso más avanzados y medidas de protección digital. La presencia de redes eléctricas inestables es otro riesgo que podría causar la pérdida de equipos y problemas relacionados con la electricidad. Para abordar este riesgo, se deben realizar mejoras en la infraestructura eléctrica y considerar sistemas de respaldo.

Falta de Mantenimiento en el Sistema Antincendios:

- *Amenaza:* Incendio

    - Activos Afectados: Datos, Hardware, Servicios
    - Descripción del Riesgo: La falta de mantenimiento en el sistema antincendios aumenta el riesgo de pérdida de equipos y documentos importantes en caso de incendio.

- Medidas de Salvaguarda: Se implementará un programa regular de mantenimiento del sistema antincendios. Se llevarán a cabo simulacros de evacuación.
- Nivel de Efectividad Estimado: Alto

Falta de un Amplio Sistema de Refrigeración:

- *Amenaza:* Sobrecalentamiento y daño de los equipos

  - Activos Afectados: Hardware
  - Descripción del Riesgo: La carencia de un sistema de refrigeración adecuado puede ocasionar el sobrecalentamiento y daño de los equipos de cómputo.
  - Medidas de Salvaguarda: Se instalará un sistema de refrigeración adecuado en las áreas críticas. Se realizarán controles de temperatura regulares.
  - Nivel de Efectividad Estimado: Moderado

Falta de Control sobre el Acceso a las Oficinas:

- *Amenaza:* Robo de documentos importantes

  - Activos Afectados: Datos
  - Descripción del Riesgo: La falta de control sobre el acceso a las oficinas aumenta el riesgo de robos de documentos importantes.
  - Medidas de Salvaguarda: Se implementarán sistemas de control de acceso y cámaras de seguridad. Se establecerán políticas de seguridad para el acceso.
  - Nivel de Efectividad Estimado: Alto

Errores en la Manipulación de las Redes Internas:

- *Amenaza:* Conexiones inseguras

  - *Activos Afectados:* Redes y comunicaciones

- *Descripción del Riesgo:* Errores en la manipulación de las redes internas pueden resultar en conexiones inseguras y comprometer la seguridad de los equipos.
- *Medidas de Salvaguarda:* Se proporcionará capacitación en seguridad de redes. Se establecerán políticas de configuración segura.
- *Nivel de Efectividad Estimado:* Alto

Falta de Inventario Adecuado de Equipos:

- *Amenaza:* Robos de equipos

    - Activos Afectados: Hardware
    - Descripción del Riesgo: La falta de inventario aumenta el riesgo de pérdida de equipos por robos.
    - Medidas de Salvaguarda: Se implementará un sistema de inventario electrónico. Se realizarán auditorías de inventario periódicas.
    - Nivel de Efectividad Estimado: Moderado

Errores en la Configuración de Seguridad de Windows:

- *Amenaza:* Ciberataques

    - Activos Afectados: Datos
    - Descripción del Riesgo: Errores en la configuración de seguridad pueden exponer datos importantes a ciberataques.
    - Medidas de Salvaguarda: Se realizarán auditorías de seguridad en el sistema Windows. Se implementarán políticas de seguridad robustas.
    - Nivel de Efectividad Estimado: Alto

Falta de Generación Correcta de Roles y Sistemas de Control:

- *Amenaza:* Pérdida de información confidencial

- Activos Afectados: Datos
- Descripción del Riesgo: La falta de roles y sistemas de control adecuados puede llevar a la pérdida de información confidencial.
- Medidas de Salvaguarda: Se establecerán políticas de gestión de roles y sistemas de control. Se designarán responsabilidades claras para su implementación.
- Nivel de Efectividad Estimado: Moderado

Falta de Políticas y Personal Responsable de la Documentación:

- *Amenaza:* Pérdida o mal uso de documentos importantes

  - Activos Afectados: Datos
  - Descripción del Riesgo: La falta de políticas y personal responsable de la documentación puede resultar en pérdida o mal uso de documentos importantes.
  - Medidas de Salvaguarda: Se implementarán políticas de gestión documental y se designará personal responsable. Se proporcionará capacitación sobre el uso adecuado de los equipos.
  - Nivel de Efectividad Estimado: Moderado

2.3.14 Área de operaciones

Presenta varios procesos de riesgo que afectan a diferentes activos y pueden tener graves consecuencias para la empresa y sus clientes. Uno de los principales riesgos es el robo o extravío de dispositivos móviles o portátiles, lo que puede resultar en la pérdida de información confidencial de la empresa o de los clientes. Asimismo, la falta de protección de datos en redes públicas puede permitir el acceso no autorizado a la información sensible de la empresa o del cliente. Otro riesgo importante es el mal uso de la información, ya que el incumplimiento de políticas de privacidad y seguridad por parte del personal técnico puede poner en peligro la información confidencial de la empresa y de los clientes. Además, la falta de medidas de protección en las instalaciones de los clientes y de control en los accesos pueden permitir el acceso no autorizado a los sistemas y datos de la empresa y del cliente.

Por otro lado, la ausencia de políticas y personal encargado de generar la documentación puede provocar la pérdida de información crítica, lo que afecta tanto a la empresa como a los clientes. Además, la falta de controles de seguridad en los vehículos y la ausencia de protecciones digitales en los equipos móviles pueden resultar en el robo de los vehículos y equipos de trabajo, así como en la pérdida de los equipos móviles. En general, se requieren medidas de prevención y mantenimiento en el área de operaciones para mitigar estos riesgos y proteger adecuadamente los activos y la información crítica de la empresa y de los clientes. Es necesario implementar políticas y medidas de seguridad adecuadas y contar con el personal capacitado para su implementación y mantenimiento.

Robo o Extravío de Dispositivos Móviles o Portátiles:

- *Amenaza:* Pérdida o robo de dispositivos móviles o portátiles.

    - Activos Afectados: Hardware, Datos
    - Descripción del Riesgo: La pérdida o robo de dispositivos móviles o portátiles puede resultar en daño a la información de la empresa o del cliente.
    - Medidas de Salvaguarda: Se implementará un sistema de seguimiento y bloqueo remoto de dispositivos. Se establecerán políticas de seguridad para el manejo de dispositivos móviles.
    - Nivel de Efectividad Estimado: Alto

Falta de Protección de Datos en Red Interna:

- *Amenaza:* Acceso no autorizado a la información por la red.

    - *Activos Afectados:* Redes y comunicaciones, Datos
    - *Descripción del Riesgo:* La falta de protección de datos en redes públicas puede permitir el acceso no autorizado a información sensible de la empresa o del cliente.
    - *Medidas de Salvaguarda:* Se establecerán políticas de uso seguro de redes. Se promoverá el uso de redes privadas virtuales (VPN) para conexiones externas.

- *Nivel de Efectividad Estimado:* Moderado

Mal Uso de la Información:

- *Amenaza:* Incumplimiento de políticas de privacidad y seguridad de la información.

  - Activos Afectados: Datos
  - Descripción del Riesgo: El mal uso de la información por parte del personal técnico puede resultar en incumplimiento de políticas de privacidad y seguridad.
  - Medidas de Salvaguarda: Se proporcionará capacitación en políticas de privacidad y seguridad. Se establecerán controles de acceso a la información confidencial.
  - Nivel de Efectividad Estimado: Alto

Falta de Medidas de Control en los Accesos:

- *Amenaza:* Riesgo de acceso no autorizado a sistemas y datos.

  - Activos Afectados: Datos
  - Descripción del Riesgo: La falta de medidas de control en los accesos aumenta el riesgo de acceso no autorizado a sistemas y datos.
  - Medidas de Salvaguarda: Se implementarán sistemas de control de acceso físico y lógico. Se establecerán políticas de contraseñas seguras.
  - Nivel de Efectividad Estimado: Alto

Mal uso de los Sistemas de Información:

- *Amenaza:* Incumplimiento de políticas de privacidad y seguridad.

  - Activos Afectados: Datos
  - Descripción del Riesgo: El mal uso de los sistemas de información puede resultar en incumplimiento de políticas de privacidad y seguridad.

- Medidas de Salvaguarda: Se proporcionará capacitación en el uso adecuado de los sistemas de información. Se establecerán controles de acceso y auditorías.
- Nivel de Efectividad Estimado: Moderado

Ausencia de Políticas y Personal Responsable de la Documentación:

- *Amenaza:* Pérdida de información capturada en campo.

  - Activos Afectados: Datos
  - Descripción del Riesgo: La falta de políticas y personal responsable de la documentación puede resultar en la pérdida de información capturada en campo.
  - Medidas de Salvaguarda: Se designará personal responsable de la documentación. Se establecerán políticas de gestión de documentos.
  - Nivel de Efectividad Estimado: Moderado

Ausencia de Protecciones Digitales en los Equipos Móviles:

- *Amenaza:* Pérdida de equipos móviles por robo

  - Activos Afectados: Hardware
  - Descripción del Riesgo: La ausencia de protecciones digitales en los equipos móviles aumenta el riesgo de pérdida por robo.
  - Medidas de Salvaguarda: Se implementarán soluciones de seguridad en los equipos móviles. Se establecerán políticas de reporte de equipos robados.
  - Nivel de Efectividad Estimado: Moderado

2.3.15 Área de contact center

Los hallazgos más significativos en el análisis de riesgos del área de Contact Center son las interrupciones en los servicios eléctricos, de internet y telefónico, así como la falta de recursos tecnológicos y personal capacitado. Estas amenazas pueden impactar en la calidad del servicio al

cliente y en la pérdida de información confidencial de clientes y agentes. Además, la fuga de información y las brechas de seguridad informática también representan riesgos significativos que requieren de medidas de control adecuadas. Para mitigar estos riesgos, es necesario implementar medidas de seguridad que aseguren la protección de la información confidencial de los clientes y agentes.

Es importante establecer políticas de seguridad informática claras, realizar capacitaciones constantes al personal y garantizar que los equipos y software utilizados sean adecuados para el desempeño de las funciones requeridas. Así mismo, es fundamental contar con planes de contingencia para hacer frente a situaciones de interrupción en los servicios eléctricos, de internet y telefónico, y para garantizar la continuidad del servicio al cliente. Con estas medidas, se pueden minimizar los riesgos y garantizar la calidad y seguridad del servicio al cliente en el área de Contact Center.

Interrupción del Servicio Eléctrico:

- *Amenaza:* Falla en la fuente de energía de los equipos.

    - Activos Afectados: Servicios
    - Descripción del Riesgo: Una interrupción del servicio eléctrico puede resultar en la pérdida de funcionalidad de los sistemas y la interrupción de las operaciones.
    - Medidas de Salvaguarda: Se implementarán sistemas de alimentación ininterrumpida (UPS) y generadores de respaldo. Se establecerán políticas de recuperación ante desastres.
    - Nivel de Efectividad Estimado: Alto

Interrupción del Servicio de Internet:

- *Amenaza:* Falla en la conexión a internet.

    - Activos Afectados: Servicios

- Descripción del Riesgo: Una interrupción del servicio de internet puede afectar la comunicación y las operaciones del contact center.
- Medidas de Salvaguarda: Se contarán con conexiones a internet redundantes. Se implementarán sistemas de conmutación por error.
- Nivel de Efectividad Estimado: Moderado

Interrupción del Servicio Telefónico:

- *Amenaza:* Falla en la red telefónica.

  - Activos Afectados: Servicios
  - Descripción del Riesgo: La interrupción del servicio telefónico puede afectar la capacidad de realizar llamadas y atender a los clientes.
  - Medidas de Salvaguarda: Se establecerán planes de contingencia para redireccionar las llamadas en caso de falla. Se implementará una red telefónica redundante.
  - Nivel de Efectividad Estimado: Alto

Falla en el Sistema de Grabación de Llamadas:

- *Amenaza:* Pérdida de información.

  - Activos Afectados: Datos
  - Descripción del Riesgo: La falla en el sistema de grabación de llamadas puede resultar en la pérdida de registros importantes.
  - Medidas de Salvaguarda: Se implementarán sistemas de respaldo de grabaciones. Se realizarán pruebas periódicas de recuperación.
  - Nivel de Efectividad Estimado: Alto

Brecha de Seguridad Informática:

- *Amenaza:* Ataque de hackers o phishing.

- Activos Afectados: Datos
- Descripción del Riesgo: Una brecha de seguridad informática puede comprometer la información confidencial y la integridad de los sistemas.
- Medidas de Salvaguarda: Se implementarán soluciones de seguridad de red y capacitación en seguridad cibernética. Se establecerán políticas de detección y respuesta a incidentes.
- Nivel de Efectividad Estimado: Alto

Fuga de Información:

- *Amenaza:* Acceso no autorizado a información confidencial.

  - Activos Afectados: Datos
  - Descripción del Riesgo: La fuga de información puede resultar en la divulgación no autorizada de datos sensibles.
  - Medidas de Salvaguarda: Se establecerán controles de acceso estrictos. Se implementarán soluciones de cifrado de datos.
  - Nivel de Efectividad Estimado: Moderado

Falta de Personal Capacitado:

- *Amenaza:* Falta de habilidades para resolver problemas de los clientes.

  - Activos Afectados: Servicio, Datos
  - Descripción del Riesgo: La falta de personal capacitado puede afectar la calidad de atención al cliente.
  - Medidas de Salvaguarda: Se proporcionará capacitación continua al personal. Se establecerán estándares de servicio y procedimientos de resolución de problemas.
  - Nivel de Efectividad Estimado: Alto

Ruido en el Ambiente de Trabajo:

- *Amenaza:* Interrupciones en las llamadas.

  - Activos Afectados: Servicio
  - Descripción del Riesgo: El ruido en el ambiente de trabajo puede afectar la calidad de las llamadas y la experiencia del cliente.
  - Medidas de Salvaguarda: Se implementarán medidas de control de ruido en el centro de contacto. Se establecerán políticas de comportamiento en el lugar de trabajo.
  - Nivel de Efectividad Estimado: Moderado

2.3.16 Área de ingeniería y gestión

En los equipos, se identificaron diversas amenazas, riesgos y vulnerabilidades que necesitan mayor control. Entre ellas, destacan la falta de mantenimiento en el sistema antincendios, lo que puede provocar pérdida de hardware en caso de incendio, y la falta de un amplio sistema de refrigeración, lo que puede generar sobrecalentamiento y daño de los equipos. Asimismo, se encontró que no existe un control adecuado sobre las personas que ingresan y salen de las oficinas del área, lo que podría derivar en robos de equipos y dispositivos. En el área de comunicaciones, se identificaron amenazas como los ataques cibernéticos a través de correos electrónicos y mensajes instantáneos, las escuchas telefónicas y grabaciones no autorizadas, y las fugas de información a través de la transmisión de datos no segura. Además, se encontró que el mal uso de las herramientas de comunicación y colaboración puede generar riesgos para la seguridad de los datos y la información

Amenazas y Riesgos en el Área de Ingeniería y Gestión:

Mantenimiento y Prevención de Riesgos en los Equipos:

- *Amenaza:* Falta de mantenimiento en el sistema antincendios.

- Activos Afectados: Hardware
- Descripción del Riesgo: La falta de mantenimiento en el sistema antincendios puede resultar en la pérdida de hardware en caso de un incendio.
- Medidas de Salvaguarda: Se implementarán inspecciones y mantenimiento regulares del sistema antincendios. Se establecerán políticas de evacuación.
- Nivel de Efectividad Estimado: Alto

- *Amenaza:* Falta de un amplio sistema de refrigeración.

  - Activos Afectados: Hardware
  - Descripción del Riesgo: La falta de refrigeración adecuada puede provocar el sobrecalentamiento y daño de los equipos.
  - Medidas de Salvaguarda: Se instalará un sistema de refrigeración eficiente y se monitoreará su funcionamiento. Se realizarán inspecciones periódicas de hardware.
  - Nivel de Efectividad Estimado: Moderado

- *Amenaza:* Falta de control sobre el acceso a las oficinas del área.

  - Activos Afectados: Hardware, Datos
  - Descripción del Riesgo: La falta de control de acceso puede resultar en robos de equipos y dispositivos.
  - Medidas de Salvaguarda: Se implementarán sistemas de control de acceso físico. Se establecerán políticas de seguridad para el manejo de equipos.
  - Nivel de Efectividad Estimado: Alto

- *Amenaza:* Error en la manipulación de las redes, conexiones inseguras.

  - *Activos Afectados:* Redes y comunicaciones
  - *Descripción del Riesgo:* Errores en la manipulación de las redes pueden conducir a conexiones inseguras y vulnerabilidades en la red.

- *Medidas de Salvaguarda:* Se proporcionará capacitación en seguridad de redes. Se realizarán auditorías regulares de seguridad.
- *Nivel de Efectividad Estimado:* Alto

- *Amenaza:* Falta de inventario adecuado de los equipos.

  - Activos Afectados: Hardware
  - Descripción del Riesgo: La falta de inventario adecuado puede aumentar el riesgo de robos y dificultar la gestión de activos.
  - Medidas de Salvaguarda: Se implementará un sistema de gestión de activos. Se realizarán auditorías de inventario periódicas.
  - Nivel de Efectividad Estimado: Alto

Comunicaciones:

- *Amenaza:* Ataques cibernéticos a través de correos electrónicos y mensajes instantáneos.

  - *Activos Afectados:* Redes y Comunicaciones
  - *Descripción del Riesgo:* Los ataques cibernéticos pueden comprometer la integridad de las comunicaciones.
  - *Medidas de Salvaguarda:* Se implementarán soluciones de seguridad de correo electrónico y mensajería instantánea. Se proporcionará capacitación en seguridad cibernética.
  - *Nivel de Efectividad Estimado:* Alto

2.3.17 Área de producto y servicio

Se identificaron varias amenazas y riesgos relacionados con la protección de datos de clientes, la seguridad física de los equipos, la falta de control de acceso a la información, la falta de actualización de antivirus y firewall, y la ausencia de políticas claras y entrenamiento del personal en seguridad de la información. La falta de medidas de seguridad en la transferencia de

datos personales de los clientes y la falta de control de acceso a la información confidencial de los clientes son riesgos significativos que necesitan mayor control. Además, la ausencia de medidas de seguridad física en la oficina puede aumentar el riesgo de robo o pérdida de equipos y la falta de actualización de antivirus y firewall aumenta el riesgo de ataques de malware y virus. Por último, la ausencia de políticas claras y entrenamiento del personal en seguridad de la información puede llevar a fraudes y phishing. Es importante que se implementen medidas de control adecuadas para abordar estos riesgos y garantizar la seguridad de los datos y sistemas de información.

Protección de Datos de Clientes:

- *Amenaza:* Falta de medidas de seguridad en la transferencia de datos personales.

    - Activos Afectados: Datos
    - Descripción del Riesgo: La falta de seguridad en la transferencia de datos personales puede comprometer la privacidad de los clientes.
    - Medidas de Salvaguarda: Se implementarán medidas de cifrado y seguridad en la transferencia de datos. Se capacitará al personal en el manejo seguro de datos.
    - Nivel de Efectividad Estimado: Alto

Robo o Pérdida de Equipos:

- *Amenaza:* Ausencia de medidas de seguridad física en la oficina.

    - Activos Afectados: Hardware
    - Descripción del Riesgo: La falta de seguridad física puede resultar en el robo o pérdida de equipos de cómputo.
    - Medidas de Salvaguarda: Se implementarán sistemas de seguridad física, como cerraduras y sistemas de alarma. Se respaldarán regularmente los datos.
    - Nivel de Efectividad Estimado: Moderado

Fugas de Información Confidencial:

- *Amenaza:* Falta de control de acceso a la información.

  - Activos Afectados: Datos
  - Descripción del Riesgo: La falta de control de acceso puede dar lugar a fugas de información confidencial.
  - Medidas de Salvaguarda: Se establecerán políticas de control de acceso. Se implementarán sistemas de autenticación y autorización.
  - Nivel de Efectividad Estimado: Alto

Malware y Virus:

- *Amenaza:* Falta de actualización de antivirus y firewall.

  - Activos Afectados: Datos
  - Descripción del Riesgo: La falta de actualización de antivirus y firewall puede dejar los sistemas vulnerables a malware y virus.
  - Medidas de Salvaguarda: Se implementará un programa de seguridad informática que incluya actualizaciones regulares de antivirus y firewall. Se realizarán escaneos de seguridad periódicos.
  - Nivel de Efectividad Estimado: Alto

Fraude y Phishing:

- *Amenaza:* Ausencia de políticas claras y entrenamiento del personal en seguridad de la información.

  - Activos Afectados: Personal, Datos
  - Descripción del Riesgo: La falta de políticas y capacitación en seguridad de la información puede dejar al personal vulnerable al fraude y al phishing.

- Medidas de Salvaguarda: Se establecerán políticas claras de seguridad de la información. Se proporcionará capacitación en reconocimiento de amenazas de seguridad.
- Nivel de Efectividad Estimado: Alto

2.3.18 Área de talento humano

La gestión del talento humano es una tarea crítica en cualquier organización, y como tal, debe ser protegida de riesgos y amenazas que puedan afectar a la integridad de los datos y la privacidad de los empleados. En este sentido, se identificaron una serie de procesos de riesgo que pueden poner en peligro la información de los empleados, como la falta de control de acceso a los sistemas que contienen la base de datos de empleados, la falta de políticas de privacidad, errores en la gestión de permisos de acceso y la falta de protección de los datos de los empleados.

Además, la selección de personal puede ser un área de riesgo si no se cuenta con protocolos de seguridad adecuados, lo que puede resultar en la contratación de personal no confiable. Por otro lado, la gestión de la nómina es otro aspecto que debe ser protegido, ya que una fuga de información financiera de los empleados puede tener graves consecuencias. Finalmente, la transferencia de información también representa un riesgo, ya que la pérdida de información al enviarla a terceros puede comprometer la privacidad de los empleados. En resumen, se debe prestar especial atención a estos procesos de riesgo para proteger la información y privacidad del talento humano de la organización.

Acceso a Información de los Empleados:

- *Amenaza:* Poco control de acceso a los sistemas.

  - Activos Afectados: Datos
  - Descripción del Riesgo: La falta de control de acceso puede permitir que personal no autorizado acceda a información confidencial de los empleados.
  - Medidas de Salvaguarda: Se implementará un control de acceso más estricto y se

revisarán regularmente los permisos de acceso.

- Nivel de Efectividad Estimado: Moderado

Falta de Políticas de Privacidad:

- *Amenaza:* Fuga de información confidencial.

  - Activos Afectados: Datos
  - Descripción del Riesgo: La falta de políticas de privacidad puede resultar en la fuga de información confidencial de los empleados.
  - Medidas de Salvaguarda: Se establecerán políticas de privacidad claras y se capacitará al personal en su cumplimiento.
  - Nivel de Efectividad Estimado: Alto

Errores en la Gestión de Permisos de Acceso:

- *Amenaza:* Acceso no autorizado a información de empleados.

  - Activos Afectados: Datos
  - Descripción del Riesgo: Errores en la gestión de permisos pueden permitir el acceso no autorizado a información sensible de empleados.
  - Medidas de Salvaguarda: Se revisarán y ajustarán los permisos de acceso de manera regular. Se implementará un proceso de revisión y aprobación de permisos.
  - Nivel de Efectividad Estimado: Moderado

Falta de Protección de los Datos de Empleados:

- *Amenaza:* Pérdida o robo de datos de empleados.

  - Activos Afectados: Datos.
  - Descripción del Riesgo: La falta de protección de datos de empleados puede resultar en

la pérdida o robo de información crítica.

- Medidas de Salvaguarda: Se implementarán medidas de seguridad física y lógica para proteger las copias de seguridad de los datos de empleados.
- Nivel de Efectividad Estimado: Moderado

Ausencia de Protocolos para la Selección de Personal:

- *Amenaza:* Ingreso de personal no confiable.

  - *Activos Afectados:* Personal, Servicios
  - *Descripción del Riesgo:* La falta de protocolos de seguridad en la selección de personal puede permitir el ingreso de personal no confiable.
  - *Medidas de Salvaguarda:* Se establecerán protocolos de selección de personal que incluyan verificaciones de antecedentes y referencias.
  - *Nivel de Efectividad Estimado:* Alto

Falta de Protocolos de Seguridad en la Gestión de Nóminas:

- *Amenaza:* Fuga de información financiera de los empleados.

  - Activos Afectados: Datos.
  - Descripción del Riesgo: La falta de protocolos de seguridad en la gestión de nóminas puede resultar en la fuga de información financiera de los empleados.
  - Medidas de Salvaguarda: Se implementarán medidas de seguridad para proteger los registros de nómina y se establecerán procedimientos de manejo seguro de información financiera.
  - Nivel de Efectividad Estimado: Alto

Ausencia de Medidas de Seguridad para la Transferencia de Información:

- *Amenaza:* Pérdida de información al enviarla a terceros.

- Activos Afectados: Datos
- Descripción del Riesgo: La falta de medidas de seguridad puede resultar en la pérdida de información al enviarla a terceros.
- Medidas de Salvaguarda: Se establecerán protocolos de seguridad para la transferencia de información y se utilizarán métodos seguros de transmisión.
- Nivel de Efectividad Estimado: Moderado

2.3.19 Área de proyectos TI

Se destacó el riesgo de introducción de código malicioso al utilizar librerías y componentes no confiables, así como la falta de revisión de código y la ausencia de pruebas de penetración y control de versiones adecuados. En la administración de servidores, se identificó la falta de actualizaciones de seguridad y una configuración inadecuada de los servicios como los riesgos más significativos. Asimismo, la falta de monitoreo y la ausencia de un plan de contingencia también se presentaron como riesgos de importancia.

En cuanto a la seguridad en red, el uso de contraseñas débiles fue identificado como un riesgo significativo. Finalmente, en la gestión de proyectos, se destacó la falta de un plan de seguridad en el ciclo de vida del desarrollo de software y la gestión inadecuada de riesgos en los proyectos como los principales riesgos.

Desarrollo de Software:

- *Amenaza:* Uso de librerías y componentes no confiables: Posible introducción de código malicioso.

  - Activos Afectados: Datos, Software.
  - Descripción del Riesgo: El uso de librerías no confiables puede introducir código malicioso en el software.
  - Medidas de Salvaguarda: Se implementará un proceso de revisión de librerías y componentes antes de su uso en el desarrollo.

- Nivel de Efectividad Estimado: Alto

- *Amenaza:* Falta de revisión de código: Posibles errores y vulnerabilidades.

  - Activos Afectados: Datos, Software.
  - Descripción del Riesgo: La falta de revisión de código puede resultar en la presencia de errores y vulnerabilidades en el software.
  - Medidas de Salvaguarda: Se establecerá un proceso de revisión de código antes de la implementación.
  - Nivel de Efectividad Estimado: Alto

- *Amenaza:* No se realizan pruebas de penetración: Posible explotación de vulnerabilidades.

  - *Activos Afectados:* Servicios, Software.
  - *Descripción del Riesgo:* La falta de pruebas de penetración puede permitir la explotación de vulnerabilidades en los sistemas en producción.
  - *Medidas de Salvaguarda:* Se realizarán pruebas de penetración regulares en los sistemas.
  - *Nivel de Efectividad Estimado:* Alto
- *Amenaza:* No se posee un correcto control de versiones: Pérdida de código fuente y posible contaminación del mismo.

  - *Activos Afectados:* Datos, Servicios, Software.
  - *Descripción del Riesgo:* La falta de control de versiones puede resultar en la pérdida o contaminación del código fuente.
  - *Medidas de Salvaguarda:* Se implementará un sistema de control de versiones adecuado.
  - *Nivel de Efectividad Estimado:* Moderado

Administración de Servidores:

- *Amenaza:* Falta de actualizaciones de seguridad: Posible explotación de vulnerabilidades.

    - *Activos Afectados:* Datos, Servicios.
    - *Descripción del Riesgo:* La falta de actualizaciones de seguridad puede permitir la explotación de vulnerabilidades en los servidores.
    - *Medidas de Salvaguarda:* Se establecerá un proceso regular de aplicar actualizaciones de seguridad.
    - *Nivel de Efectividad Estimado:* Moderado

- *Amenaza:* Configuración segura de servicios: Posible exposición de información sensible.

    - Activos Afectados: Datos.
    - Descripción del Riesgo: La configuración incorrecta de servicios puede exponer información sensible.
    - Medidas de Salvaguarda: Se configurarán los servicios de manera segura y se revisarán periódicamente.
    - Nivel de Efectividad Estimado: Moderado

- *Amenaza:* Falta de monitoreo de los servicios: Posible compromiso de los mismos.
    - *Activos Afectados:* Datos, Servicios.
    - *Descripción del Riesgo:* La falta de monitoreo de servicios puede resultar en el compromiso de los mismos.
    - *Medidas de Salvaguarda:* Se implementará un sistema de monitoreo constante.
    - *Nivel de Efectividad Estimado:* Alto

- *Amenaza:* No se posee un plan de contingencia: Posible pérdida de información.

    - Activos Afectados: Datos.

- Descripción del Riesgo: La falta de un plan de contingencia puede resultar en la pérdida de información crítica.
- Medidas de Salvaguarda: Se desarrollará un plan de contingencia y se realizarán pruebas periódicas.
- Nivel de Efectividad Estimado: Alto

Seguridad en Red:

- *Amenaza:* Uso de contraseñas débiles: Posible compromiso de los sistemas.

  - Activos Afectados: Software.
  - Descripción del Riesgo: El uso de contraseñas débiles puede permitir el compromiso de sistemas y redes.
  - Medidas de Salvaguarda: Se implementarán políticas de contraseñas seguras y se capacitará al personal en su uso.
  - Nivel de Efectividad Estimado: Moderado

Gestión de Proyectos:

- *Amenaza:* Falta de un plan de seguridad en el ciclo de vida de desarrollo de software: Posible introducción de vulnerabilidades.

  - Activos Afectados: Servicios.
  - Descripción del Riesgo: La falta de un plan de seguridad puede permitir la introducción de vulnerabilidades en el software durante el desarrollo.
  - Medidas de Salvaguarda: Se desarrollará un plan de seguridad en el ciclo de vida del desarrollo de software.
  - Nivel de Efectividad Estimado: Alto

- *Amenaza:* No se posee una correcta gestión de riesgos en los proyectos: Posible exposición de información sensible.

- Activos Afectados: Servicios.
- Descripción del Riesgo: La falta de gestión de riesgos puede resultar en la exposición de información sensible durante los proyectos.
- Medidas de Salvaguarda: Se implementará un proceso de gestión de riesgos en todos los proyectos.
- Nivel de Efectividad Estimado: Moderado

2.4 Implementación del Ciclo PHVA en SP Sistemas Palacios Ltda: Un Enfoque en la Gestión de la Seguridad de la Información según ISO/IEC 27001

Es importante destacar que la evaluación de riesgos se realizó utilizando la metodología MAGERIT, lo que permitió identificar los procesos y activos de la empresa que presentan un mayor riesgo y definir las medidas de control y mitigación necesarias para garantizar la seguridad de la información. Se recomienda que se tomen medidas adecuadas para reducir el impacto de estos riesgos y se implementen controles efectivos para mantener la seguridad de la información en la empresa. Con base en lo anterior una vez identificadas las vulnerabilidades y riesgos en cada una de las áreas funcionales de la empresa SP Sistemas Palacios Ltda se procede a estructurar el Sistema de Gestión de Seguridad de la Información (SGSI) basado en lo definido en la norma ISO/ IEC 27001 desde el ciclo PHVA. La ISO/IEC 27001 se basa en la teoría de gestión de la calidad PHVA (también conocida como ciclo de Deming), también se le llama ciclo de Deming porque su autor es Edwards Deming o ciclo de mejora continua. El nombre de ciclo PHVA se deriva de las siglas Plan, Hacer, Verificar, Actuar. Esta metodología describe los cuatro pasos básicos que se deben implementar de manera sistemática para lograr la mejora continua es decir la reducción de fallas, mejora de la eficiencia y efectividad, resolución de problemas y eliminación de riesgos potenciales.

2.4.1 Planificar (Plan)

Para la empresa SP Sistemas Palacios Ltda, la planificación del ciclo PHVA comienza por identificar los procesos críticos para el cumplimiento de los objetivos y metas de la organización. Se definen los objetivos específicos y los indicadores de desempeño que se utilizarán para medir

el progreso en la implementación del SGSI. Se elabora un plan detallado que describe las acciones necesarias para alcanzar los objetivos, incluyendo los plazos y responsables correspondientes. La planificación del Sistema de Gestión de Seguridad de la Información (SGSI) requiere de un análisis exhaustivo del contexto de la organización. Este análisis permite a la empresa SP Sistemas Palacios Ltda identificar los riesgos y oportunidades asociados a la seguridad de la información, y definir las acciones necesarias para gestionarlos de manera efectiva. En este sentido, el contexto de la organización es un factor clave para la planificación del SGSI, ya que proporciona una comprensión profunda de los objetivos, las políticas y los requisitos legales y regulatorios que deben ser considerados en el diseño e implementación del SGSI. Por lo tanto, el análisis del contexto de la organización se convierte en el primer paso del ciclo PHVA (Plan, Do, Check, Act) en la planificación del SGSI, permitiendo a la empresa SP Sistemas Palacios Ltda establecer los objetivos y metas específicas del SGSI, así como las estrategias y planes de acción necesarios para alcanzarlos.

2.4.2 Hacer (Do)

En la etapa de "Hacer", se implementan las acciones definidas en la planificación. Se establecen los procedimientos y controles necesarios para garantizar la adecuada gestión de la seguridad de la información. Se realizan pruebas y simulaciones para evaluar la efectividad de los controles y se llevan a cabo las capacitaciones necesarias para asegurar que el personal esté capacitado y consciente de sus responsabilidades en cuanto a la seguridad de la información. Durante la etapa de "Hacer", se implementan las acciones y medidas de seguridad definidas en la fase de planificación del SGSI en la empresa SP Sistemas Palacios LTDA. Para ello, se establecen los procedimientos y controles necesarios para garantizar la adecuada gestión de la seguridad de la información. Además, se llevan a cabo las capacitaciones necesarias para asegurar que el personal esté capacitado y consciente de sus responsabilidades en cuanto a la seguridad de la información.

Además, se realizan pruebas y simulaciones para evaluar la efectividad de los controles implementados y se monitorea el desempeño de los mismos. Asimismo, se recopilan y analizan los datos generados durante esta etapa para su posterior evaluación en la fase de "Verificar".

2.4.3 Verificar (Check)

En esta etapa, se monitorean y miden los resultados obtenidos en la etapa anterior, comparándolos con los objetivos y metas definidos en la fase de planificación. Se realiza una Auditoría interna del SGSI para identificar posibles desviaciones y se llevan a cabo revisiones periódicas del plan para asegurar su adecuación. Durante la etapa de "Verificar", se realiza una revisión detallada de los resultados obtenidos en la fase anterior. Es decir, se comparan los resultados y desempeño de los controles implementados con los objetivos y metas definidos en la fase de planificación. En esta etapa, se lleva a cabo una Auditoria interna del SGSI para identificar posibles desviaciones o no conformidades que puedan afectar la seguridad de la información. Asimismo, se realizan revisiones periódicas del plan para asegurar su adecuación y se llevan a cabo las acciones necesarias para corregir cualquier desviación identificada.

2.4.4 Actuar (Act)

En esta etapa, se toman las acciones necesarias para corregir cualquier desviación o no conformidad identificada en la fase de "Verificar". Se llevan a cabo acciones de mejora continua y se actualizan los procedimientos y controles según sea necesario. También se realiza una revisión global del ciclo PHVA y se inicia una nueva iteración para seguir mejorando el SGSI en la empresa SP Sistemas Palacios LTDA. En la etapa de "Actuar", se toman las acciones necesarias para corregir cualquier desviación o no conformidad identificada en la fase de "Verificar". Es decir, se llevan a cabo las acciones correctivas y preventivas necesarias para mejorar la eficacia y eficiencia del SGSI en la empresa SP Sistemas Palacios Ltda.

Además, se promueve la mejora continua del sistema, se actualizan los procedimientos y controles según sea necesario y se asegura la participación activa del personal en este proceso de mejora. Finalmente, se realiza una revisión global del ciclo PHVA y se inicia una nueva iteración para seguir mejorando el SGSI en la empresa. Con respecto a la ISO/IEC 27001: 2013 se establece que la Gestión de la Mejora Continua es obligatoria, Teniendo en cuenta que el ciclo PHVA y el enfoque de uso están incluidos en ISO/IEC 27001: 2013 se propone un enfoque basado en los procesos, lo cual alinea la mejora continua con los objetivos de alcanzar el más alto

nivel de desempeño en la empresa.

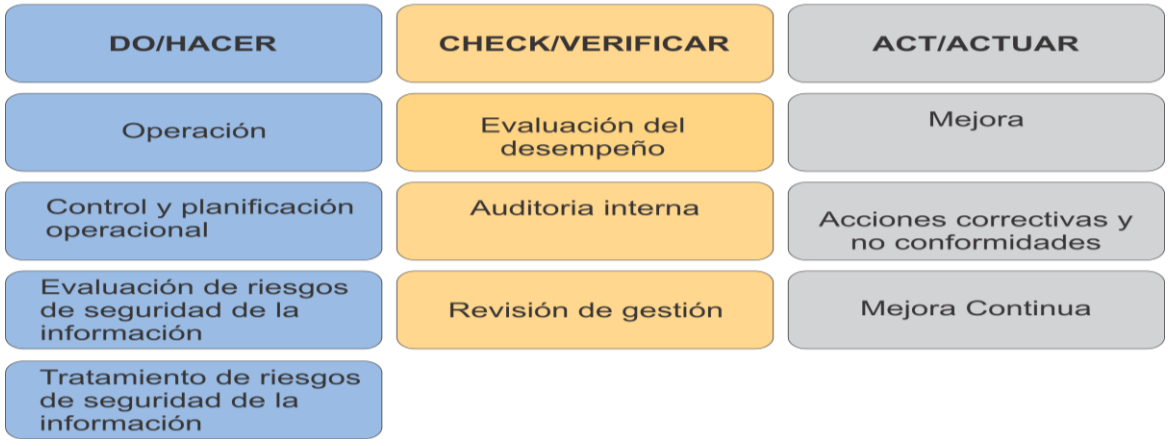
A continuación, en la Figura 5 se muestra una representación gráfica del ciclo PHVA y la relación que este tiene con la estructura general de ISO/IEC 27001: 2013:

Figura 5

Ciclo PHVA en la empresa SP Sistemas Palacios Ltda

Figura 6

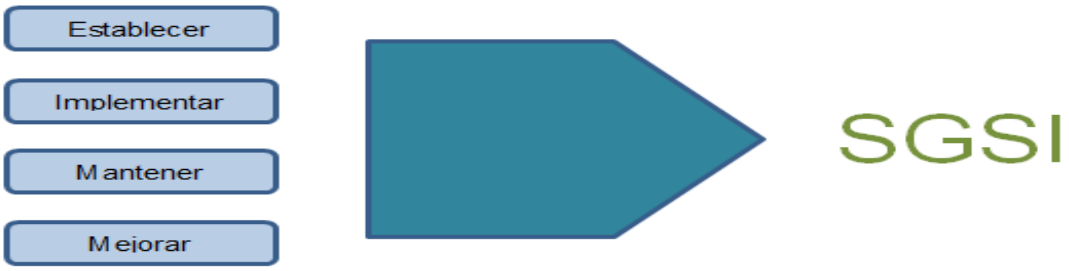
Do/ Check/ Act.



Una vez que se han adoptado medidas para prevenir riesgos, es importante que la organización diseñe un plan para proteger su información, la cual es un activo crucial para la empresa. En este sentido, SP Sistemas Palacios Ltda debe seguir este principio y asegurar que sus activos estén protegidos, seguros y resguardados. Para lograr este objetivo, la norma ISO/IEC 27001 ofrece un modelo para organizar un sistema de gestión de seguridad de la información, el cual se basa en un conjunto de procesos que permiten establecer, implementar, mantener y mejorar el SGSI de las empresas. Este modelo tiene como objetivo asegurar la confidencialidad, integridad y disponibilidad de la información, así como de los sistemas y aplicaciones que la manejan (ISO/IEC 27001, 2013). La Figura 7 muestra más detalles sobre este proceso. Ver figura 7.

Figura 7

Procesos ISO/IEC 27001, 2013



Durante la fase de planeación, se definieron los riesgos y se identificaron las medidas preventivas necesarias para minimizarlos. Se establecieron los objetivos y metas de seguridad de la información, así como los recursos y responsabilidades necesarios para implementar el SGSI. Como resultado, se elaboró un plan de seguridad de la información que establece los lineamientos y procedimientos a seguir.

Durante la fase de hacer, se implementaron las medidas preventivas y se definieron los controles necesarios para asegurar la confidencialidad, integridad y disponibilidad de la información. Se establecieron objetivos de control y se implementaron medidas de seguridad técnicas y organizativas. Además, se desarrollaron políticas y procedimientos para asegurar que los controles se mantengan en operación.

En la fase de verificación, se realizarán Auditorías internas y externas para verificar la efectividad de los controles implementados y la conformidad con los estándares y normas de seguridad de la información. Se llevarán a cabo pruebas de seguridad para identificar posibles vulnerabilidades y se evaluará la efectividad de las medidas de seguridad implementadas.

En la fase de actuar, se tomarán acciones correctivas y preventivas para mejorar continuamente el SGSI. Se implementarán mejoras en los controles y se actualizarán las políticas y procedimientos de seguridad de la información en función de los resultados de las Auditorias y pruebas de seguridad. Además, se llevarán a cabo revisiones periódicas del SGSI para asegurar su eficacia y eficiencia en la protección de la información de la organización.

2.4.5 Alcance

El alcance del Sistema de Gestión de Seguridad de la Información (SGSI) de la empresa SP Sistemas Palacios LTDA se define como el conjunto de procesos y actividades que permitirán garantizar la protección y confidencialidad de la información, además de asegurar su disponibilidad y la integridad de los sistemas y servicios que la soportan. El SGSI cubre todas las áreas de la organización, incluyendo los procesos de negocio, los sistemas de información, los datos y la infraestructura tecnológica.

El alcance del SGSI incluye la identificación y análisis de los riesgos asociados a la seguridad de la información, la implementación de controles y medidas de seguridad para mitigar los riesgos identificados, la realización de pruebas y simulaciones para evaluar la efectividad de los controles, y la formación y capacitación del personal de la organización en relación a las políticas y procedimientos del SGSI. Las cuales se implementarán en las diferentes áreas de la empresa SP Sistemas Palacios LTDA como lo son: Área de Operaciones, Contact Center, Área Administrativa y Financiera, Área de Ingeniería y Gestión, Área de producto y servicio, Área de talento humano, Área de proyectos TI, además, el sistema contemplará los controles y objetivos de control necesarios para asegurar la adecuada gestión de la seguridad de la información en cada una de estas áreas.

El SGSI está dirigido a todos los interesados en la seguridad de la información de la empresa, incluyendo gerentes, empleados, clientes y proveedores. Asimismo, el alcance del SGSI aborda la necesidad de cumplir con las leyes y regulaciones aplicables a la protección de la información, así como las políticas y requisitos internos de la organización.

Es importante destacar que el SGSI no solo aborda la protección de los activos de información, sino que también se enfoca en la mejora continua de los controles de seguridad y en la gestión de los riesgos de seguridad de la información. Para lograr esto, se debe seguir el ciclo PHVA (Planear, Hacer, Verificar, Actuar) de manera constante y llevar a cabo un análisis de riesgos, que permita identificar los riesgos y establecer los controles necesarios para mitigarlos.

2.4.6 Objetivo

El objetivo principal del SGSI de la empresa SP Sistemas Palacios LTDA es garantizar la protección, confidencialidad, disponibilidad e integridad de la información, sistemas y servicios de la organización. Este objetivo se logrará a través de la identificación y mitigación de riesgos de seguridad, la implementación de controles adecuados, la capacitación del personal y el cumplimiento de leyes y regulaciones pertinentes. Además, se buscará la mejora continua de los controles de seguridad mediante el ciclo PHVA y la gestión proactiva de los riesgos de seguridad de la información.

El SGSI está dirigido a todos los interesados en la seguridad de la información de la empresa, incluyendo gerentes, empleados, clientes y proveedores. Asimismo, el alcance del SGSI aborda la necesidad de cumplir con las leyes y regulaciones aplicables a la protección de la información, así como las políticas y requisitos internos de la organización.

Es importante destacar que el SGSI no solo aborda la protección de los activos de información, sino que también se enfoca en la mejora continua de los controles de seguridad y en la gestión de los riesgos de seguridad de la información. Para lograr esto, se debe seguir el ciclo PHVA (Planear, Hacer, Verificar, Actuar) de manera constante y llevar a cabo un análisis de riesgos, que permita identificar los riesgos y establecer los controles necesarios para mitigarlos.

2.4.7 Ámbito de aplicación

El SGSI se aplica a todas las áreas de la organización, lo que incluye procesos de negocio, sistemas de información, datos e infraestructura tecnológica. Esto abarca todas las operaciones de la empresa en diferentes áreas, como Operaciones, Contact Center, Administrativa y Financiera, Ingeniería y Gestión, Producto y Servicio, Talento Humano y Proyectos de TI. El SGSI también considera los controles y objetivos de control específicos necesarios para garantizar la seguridad de la información en cada una de estas áreas.

2.4.8 Partes interesadas

El SGSI está dirigido a todas las partes interesadas en la seguridad de la información, lo que incluye a gerentes, empleados, clientes y proveedores de SP Sistemas Palacios LTDA. Reconoce la importancia de cumplir con las leyes, regulaciones y políticas internas relacionadas con la protección de la información.

2.4.9 Enfoque en la mejora continua

El SGSI no se limita únicamente a la protección de los activos de información, sino que también pone un fuerte énfasis en la mejora continua de los controles de seguridad y la gestión de riesgos de seguridad de la información. Para lograr esto, se utiliza el ciclo PHVA (Planear, Hacer, Verificar, Actuar) de manera constante. Esto implica la planificación de medidas de seguridad, su implementación, monitoreo y evaluación, y la toma de acciones correctivas si es necesario. Un análisis de riesgos periódico es fundamental para identificar riesgos y determinar los controles necesarios para mitigarlos.

2.4.10 Principios del SGSI

- Concienciación y formación: Proporcionar capacitación y concienciación periódica a los empleados sobre las prácticas seguras de manejo de la información y los riesgos asociados.

- Evaluación y mejora continua: Realizar evaluaciones periódicas del SGSI para identificar áreas de mejora y establecer planes de acción correctivos. La mejora continua es un aspecto clave para mantener la eficacia del SGSI a lo largo del tiempo.

- Liderazgo y compromiso: El liderazgo de la alta dirección debe respaldar y comprometerse con la implementación del SGSI. Esto implica asignar responsabilidades, asignar recursos adecuados y establecer una cultura de seguridad de la información en toda la organización.

2.4.11 Planteamiento de los objetivos de control

Después de realizar la evaluación de los riesgos del capítulo anterior y haber verificado el nivel de impacto y riesgos a los cuales están expuestos los activos y el tratamiento adecuados para lograr la mitigación de los riesgos, se propone los siguientes objetivos para el control del SGSI:

2.4.12 Objetivos de control

- Establecer e implementar un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 en la empresa SP Sistemas Palacios LTDA, con el objetivo de asegurar la protección adecuada de la información de la organización.
- Desarrollar políticas y procedimientos de seguridad de la información consistentes con los requisitos de la norma ISO/IEC 27001 y apropiados para la empresa SP Sistemas Palacios LTDA, con el objetivo de establecer un marco sólido para la gestión de la seguridad de la información.
- Realizar una evaluación de riesgos de seguridad de la información en la empresa SP Sistemas Palacios LTDA, con el objetivo de identificar y gestionar los riesgos asociados con la información manejada por la organización, de acuerdo con los requisitos de la norma ISO/IEC 27001.
- Implementar controles de seguridad de la información apropiados en la empresa SP Sistemas Palacios LTDA, con el objetivo de mitigar los riesgos identificados en la evaluación de riesgos y cumplir con los requisitos de la norma ISO/IEC 27001.

- Establecer un proceso de gestión de incidentes de seguridad de la información en la empresa SP Sistemas Palacios LTDA, con el objetivo de detectar, responder, resolver y dar seguimiento a los incidentes de seguridad de manera eficiente y efectiva.
- Realizar auditorías internas periódicas del SGSI implementado en la empresa SP Sistemas Palacios LTDA, con el objetivo de asegurar el cumplimiento de los requisitos de la norma ISO/IEC 27001 y la efectividad de los controles implementados.
- Implementar un programa de concientización y capacitación en seguridad de la información para todo el personal de la empresa SP Sistemas Palacios LTDA, con el objetivo de crear una cultura de seguridad de la información y promover buenas prácticas en el manejo de la información.
- Establecer y mantener un proceso de revisión y mejora continua del SGSI basado en la norma ISO/IEC 27001 en la empresa SP Sistemas Palacios LTDA, con el objetivo de asegurar su eficacia y eficiencia a lo largo del tiempo y adaptarlo a los cambios en el entorno y las necesidades de la organización.
- Cumplir con los requisitos legales, regulaciones y normativas aplicables relacionadas con la seguridad de la información en la empresa SP Sistemas Palacios LTDA, con el objetivo de asegurar el cumplimiento de las obligaciones legales y reglamentarias en materia de seguridad de la información.

2.4.13 Controles de seguridad

Establecer e implementar un Sistema de Gestión de la Seguridad de la Información (SGSI):

Dominio 1: Política de Seguridad de la Información

- **Control:** Política de seguridad de la información.

Dominio 2: Información de Referencia y de Apoyo

- **Control:** Información de referencia y de apoyo.

Dominio 3: Proceso de Gestión de Riesgos de Seguridad de la Información

- **Control:** Proceso de gestión de riesgos de seguridad de la información.
- **Control:** Evaluación de riesgos de seguridad de la información.
- **Control:** Tratamiento de riesgos de seguridad de la información.
- **Control:** Evaluación de impacto en la protección de datos personales.

Dominio 4: Evaluación del Desempeño del SGSI

- **Control:** Evaluación del desempeño del SGSI.

Dominio 5: Proceso de Gestión de Incidentes de Seguridad de la Información

- **Control:** Proceso de gestión de incidentes de seguridad de la información.

Dominio 6: Evaluación de Cumplimiento

- Control: Evaluación de cumplimiento.
- Control: Cumplimiento legal.

Dominio 7: Compromiso de la Dirección

- **Control:** Compromiso de la dirección.
- **Control:** Revisión de la política de seguridad de la información.

Dominio 8: Objetivos de Seguridad de la Información y Planificación para su Logro

- **Control:** Objetivos de seguridad de la información y planificación para su logro.

Dominio 9: Responsabilidades y Funciones en Seguridad de la Información

- **Control:** Responsabilidades y funciones en seguridad de la información.

- **Control:** Organización de la seguridad de la información.
- **Control:** Gestión de recursos humanos.

Dominio 10: Seguridad en la Gestión de Activos

- **Control:** Seguridad en la gestión de activos.

Dominio 11: Control de Accesos

- **Control:** Control de accesos.

Dominio 12: Criptografía

- **Control:** Criptografía.

Dominio 13: Seguridad Física y del Entorno

- **Control:** Seguridad física y del entorno.

Dominio 14: Seguridad de las Operaciones

- **Control:** Seguridad de las operaciones.

Dominio 15: Comunicaciones

- **Control:** Comunicaciones.

Dominio 16: Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

- **Control:** Adquisición, desarrollo y mantenimiento de sistemas de información.

Dominio 17: Relaciones con Proveedores

- **Control:** Relaciones con proveedores.

Dominio 18: Responsabilidades y Procedimientos Operativos

- **Control:** Responsabilidades y procedimientos operativos.

Dominio 19: Rendimiento del SGSI

- **Control:** Rendimiento del SGSI.
- **Control:** Mejora continua.

Dominio 20: Documentación de la Política de Seguridad de la Información

- **Control:** Documentación de la política de seguridad de la información.

2.4.14 Definición de Políticas, estándares y procedimientos

La planificación de sistema se inicia con la definición de políticas institucionales de seguridad de la información y políticas tácticas que abarcan las diferentes áreas de la empresa, con ello se definen objetivos, estrategias, acciones y responsables de la seguridad de la información. La política institucional de SP Sistemas Palacios LTDA es: *"Protegiendo la información, construimos confianza"*.

Esta política alinea la misión y visión de la compañía y compromete a todas las áreas en la implementación del SGSI que garantice la disponibilidad, integridad, accesibilidad y confidencialidad de los datos de la empresa.

Objetivos

- Garantizar la confidencialidad de la información en la compañía mediante el establecimiento de políticas y procedimientos adecuados.
- Asegurar la disponibilidad de la información en todo momento a través de una adecuada gestión de riesgos y continuidad de negocio.
- Preservar la integridad de la información mediante el establecimiento de medidas de protección para prevenir el acceso no autorizado o la manipulación de la información.

Estrategias

- Desarrollar un plan de seguridad de la información que incluya políticas, procedimientos y estándares de seguridad.
- Realizar una evaluación de riesgos de seguridad de la información y establecer medidas de mitigación de riesgos.
- Proporcionar capacitación y concientización en seguridad de la información a todos los empleados de la empresa.

Procesos

- Identificar los activos de información críticos de la compañía y evaluar su riesgo de seguridad.
- Establecer medidas de control para proteger los activos de información críticos.
- Establecer un plan de contingencia de seguridad de la información para abordar situaciones de interrupción del negocio.

Procedimientos

- Establecer procedimientos para la gestión de acceso a la información crítica.
- Desarrollar procedimientos para la gestión de contraseñas y autenticación de usuarios.
- Establecer procedimientos para la gestión de incidentes de seguridad de la información.

- SP Sistemas Palacios LTDA se compromete a asegurar la confidencialidad, disponibilidad e integridad de la información en la compañía, lo que contribuye a la imagen interna y externa de la empresa.

Políticas

- **Política de gestión de contraseñas:** Esta política establece las reglas y prácticas necesarias para la creación, uso y gestión de contraseñas por parte de los usuarios. Esta política incluiría requerimientos como la complejidad de las contraseñas, la frecuencia de cambio, la prohibición de compartir contraseñas, y la implementación de controles de acceso para prevenir el uso de contraseñas inseguras.

Objetivos de la política de gestión de contraseñas:

- Establecer requisitos de complejidad para las contraseñas, como longitud mínima, uso de caracteres especiales, letras mayúsculas y minúsculas, y números.
- Definir la frecuencia de cambio de contraseñas, por ejemplo, cada 90 días.
- Prohibir el uso de contraseñas previamente utilizadas en un número determinado de ciclos de cambio de contraseñas.
- Implementar la autenticación multifactor (MFA) para cuentas con acceso a información sensible.
- Realizar capacitación regular a los usuarios sobre las mejores prácticas para crear y gestionar contraseñas seguras.
- Establecer sanciones para el incumplimiento de las políticas de contraseñas.

Estrategias

- Implementar una herramienta de gestión de contraseñas que permita generar contraseñas seguras automáticamente y almacenarlas de forma cifrada.
- Realizar campañas de concientización y capacitación periódicas para educar a los usuarios sobre la importancia de las contraseñas seguras y las mejores prácticas para crear y

gestionar contraseñas.

- Establecer una política de bloqueo de cuentas temporales después de un número determinado de intentos fallidos de inicio de sesión.
- Utilizar la autenticación multifactor (MFA) para agregar una capa adicional de seguridad a las cuentas con acceso a información sensible.
- Implementar un proceso de revisión regular de las contraseñas de los usuarios y asegurarse de que cumplan con los requisitos de complejidad y frecuencia de cambio establecidos.
- Realizar auditorías de seguridad periódicas para identificar posibles debilidades en la gestión de contraseñas y tomar medidas correctivas.

Procesos.

- Proceso de creación y gestión de contraseñas: Incluye la definición de los requisitos de complejidad de contraseñas, la asignación y cambio periódico de contraseñas, la prohibición de compartir contraseñas, y la implementación de controles de acceso para prevenir el uso de contraseñas inseguras.
- Proceso de capacitación y concientización en seguridad de contraseñas: Incluye la capacitación regular de los usuarios sobre las mejores prácticas para crear y gestionar contraseñas seguras, así como la concientización sobre los riesgos asociados con el uso de contraseñas débiles o compartidas.
- Proceso de monitoreo y detección de contraseñas no seguras: Incluye la implementación de herramientas y sistemas de monitoreo para detectar contraseñas no seguras o en violación de las políticas establecidas, así como la aplicación de medidas correctivas en caso de identificar contraseñas comprometidas.

Procedimientos.

- Creación de contraseñas seguras: Este procedimiento puede incluir la definición de requisitos de complejidad para las contraseñas, como longitud mínima, uso de caracteres especiales, combinación de letras y números, etc.
- Cambio periódico de contraseñas: Este procedimiento puede establecer la frecuencia con la

que los usuarios deben cambiar sus contraseñas, por ejemplo, cada 90 días.

- Restricción de compartir contraseñas: Este procedimiento puede establecer la prohibición de compartir contraseñas con otros usuarios o divulgarlas de alguna manera.
- Implementación de controles de acceso: Este procedimiento puede incluir la configuración de controles técnicos para prevenir el uso de contraseñas inseguras, como bloqueo de cuentas después de varios intentos fallidos, uso de autenticación multifactor, entre otros.
- **Política de gestión de accesos:** Esta política define los procedimientos para otorgar, modificar y revocar los permisos de acceso a los recursos de información. La política de gestión de accesos incluiría la definición de roles y permisos, la implementación de controles de acceso basados en el principio de necesidad, la revisión periódica de los permisos de acceso, y la implementación de controles de monitoreo y seguimiento para detectar y prevenir el acceso no autorizado.

Objetivos de la política de gestión de accesos.

- Definir roles y permisos claros y actualizados para cada usuario, basados en el principio de necesidad y minimizando los privilegios innecesarios.
- Establecer procedimientos formales y documentados para otorgar, modificar y revocar los permisos de acceso, con una revisión y aprobación adecuada.
- Implementar controles de monitoreo y seguimiento para detectar y alertar sobre actividades sospechosas o no autorizadas.
- Realizar revisiones periódicas de los permisos de acceso para garantizar que estén alineados con los roles y responsabilidades actuales de los usuarios.
- Establecer un proceso de gestión de cambios controlado para la asignación de permisos de acceso a recursos de información sensibles.
- Mantener un registro de auditoría de los cambios realizados en los permisos de acceso para fines de seguimiento y cumplimiento.

Estrategias.

- Implementar una herramienta de gestión de contraseñas que permita generar contraseñas

seguras automáticamente y almacenarlas de forma cifrada.

- Realizar campañas de concientización y capacitación periódicas para educar a los usuarios sobre la importancia de las contraseñas seguras y las mejores prácticas para crear y gestionar contraseñas.
- Establecer una política de bloqueo de cuentas temporales después de un número determinado de intentos fallidos de inicio de sesión.
- Utilizar la autenticación multifactor (MFA) para agregar una capa adicional de seguridad a las cuentas con acceso a información sensible.
- Implementar un proceso de revisión regular de las contraseñas de los usuarios y asegurarse de que cumplan con los requisitos de complejidad y frecuencia de cambio establecidos.
- Realizar Auditorías de seguridad periódicas para identificar posibles debilidades en la gestión de contraseñas y tomar medidas correctivas.

Procesos.

- Proceso de asignación, modificación y revocación de permisos de acceso: Incluye la definición de roles y permisos de acceso basados en el principio de necesidad, la asignación y modificación adecuada de permisos de acceso a los usuarios autorizados, y la revocación o modificación de permisos cuando sea necesario, como parte del ciclo de vida de los usuarios y su relación con los recursos de información.
- Proceso de revisión periódica de los permisos de acceso: Incluye la revisión regular de los permisos de acceso otorgados a los usuarios para asegurarse de que sean apropiados y estén alineados con las necesidades actuales de la organización, así como la identificación y mitigación de posibles riesgos de seguridad.
- Proceso de monitoreo y seguimiento de accesos: Incluye la implementación de controles y herramientas de monitoreo para registrar y analizar los accesos a los recursos de información, identificar actividades inusuales o sospechosas, y tomar acciones adecuadas en caso de detectar accesos no autorizados.

Procedimientos.

- Asignación de roles y permisos: Este procedimiento puede establecer la asignación de roles y permisos a los usuarios según sus funciones y responsabilidades dentro de la organización.
- Modificación y revocación de permisos: Este procedimiento puede establecer los procesos para solicitar cambios en los permisos de acceso, su revisión y aprobación, así como la revocación de permisos cuando un usuario cambie de rol o deje la organización.
- Revisión periódica de permisos: Este procedimiento puede establecer la revisión regular de los permisos de acceso de los usuarios para garantizar que estén alineados con sus funciones y responsabilidades actuales.
- Implementación de controles de monitoreo y seguimiento: Este procedimiento puede incluir la configuración de controles técnicos para monitorear y registrar los eventos de acceso a los recursos de información, con el fin de detectar y prevenir accesos no autorizados.
- **Política de gestión de respaldo y recuperación:** Esta política establece las reglas y prácticas necesarias para la realización de respaldos y la recuperación de la información en caso de incidentes de seguridad. La política de gestión de respaldo y recuperación incluiría la definición de los intervalos de respaldo, la ubicación y protección de los medios de almacenamiento, la definición de procedimientos para la recuperación de información en caso de incidentes, y la realización de pruebas periódicas de los procedimientos de recuperación.

Objetivos de la gestión de respaldo y recuperación:

- Definir y documentar los intervalos de respaldo adecuados para los diferentes tipos de información y sistemas.
- Establecer procedimientos para el almacenamiento seguro y protección de los medios de respaldo, como copias en ubicaciones geográficamente separadas y cifrado de datos sensibles.
- Realizar pruebas periódicas de los procedimientos de respaldo y recuperación para

asegurar su eficacia y eficiencia.

- Definir roles y responsabilidades claros para el personal encargado de realizar y gestionar los respaldos y la recuperación de información en caso de incidentes.
- Establecer un proceso formal para la gestión de incidentes de seguridad, incluyendo la identificación, notificación, manejo y documentación de incidentes de pérdida de información y la recuperación de datos en caso de incidentes.
- Garantizar que los procedimientos de respaldo y recuperación sean revisados y actualizados regularmente para mantener su relevancia y eficacia en el tiempo.

Estrategias.

- Implementar una solución de respaldo automatizada y programada que cumpla con los intervalos de respaldo definidos y asegure la integridad y confidencialidad de los datos respaldados.
- Establecer procedimientos de almacenamiento seguro de los medios de respaldo, como copias en ubicaciones geográficamente separadas y con acceso restringido a personal autorizado.
- Realizar pruebas periódicas de los procedimientos de respaldo y recuperación para asegurar su eficacia y eficiencia, y corregir cualquier problema identificado.
- Documentar y mantener actualizados los procedimientos de recuperación de información en caso de incidentes, incluyendo la identificación, notificación, manejo y documentación de incidentes de pérdida de información.
- Establecer roles y responsabilidades claros para el personal encargado de realizar y gestionar los respaldos y la recuperación de información en caso de incidentes.
- Realizar simulacros de recuperación de información en caso de incidentes para evaluar la efectividad

Procesos.

- Proceso de realización de respaldos: Incluye la definición de los intervalos de respaldo, la identificación y selección de los datos a respaldar, la implementación de las herramientas y

tecnologías de respaldo apropiadas, y la verificación de la integridad de los respaldos realizados.

- Proceso de almacenamiento y protección de los medios de respaldo: Incluye la definición de los procedimientos para almacenar y proteger los medios de respaldo, como el uso de ubicaciones seguras, el cifrado de los respaldos, y la implementación de controles de acceso físico para prevenir accesos no autorizados a los medios de respaldo.
- Proceso de recuperación de información en caso de incidentes: Incluye la definición de procedimientos y planes de acción para la recuperación de la información en caso de incidentes de seguridad, como la restauración de los datos desde los respaldos, la verificación de la integridad de los datos recuperados, y la implementación de medidas correctivas para asegurar su efectividad y realizar ajustes si es necesario.

Procedimientos:

- **Realización de respaldos periódicos:** Este procedimiento puede establecer los intervalos de tiempo en los que se deben realizar los respaldos de la información, así como los métodos y medios de almacenamiento utilizados.
- **Protección de los medios de almacenamiento:** Este procedimiento puede incluir medidas de seguridad física y lógica para proteger los medios de almacenamiento de los respaldos, como almacenamiento en lugares seguros, cifrado de datos, etc.
- **Definición de procedimientos de recuperación:** Este procedimiento puede establecer los pasos y procesos para la recuperación de la información en caso de incidentes de seguridad, incluyendo la identificación de roles y responsabilidades, las herramientas y recursos necesarios, y los plazos de recuperación.
- **Realización de pruebas periódicas de recuperación:** Este procedimiento puede establecer la realización de pruebas periódicas para verificar la efectividad de los procedimientos de recuperación, identificar posibles mejoras y actualizar los planes de recuperación en consecuencia.

Las políticas, estrategias, procesos y procedimientos, son efectivas siempre y cuando se asignen responsables en cada uno de sus procesos. A continuación, se desarrollará dentro del

marco del SGSI los roles y responsabilidades en cada una de las áreas.

2.4.15 Roles y responsabilidades en el SGSI

Según la norma ISO/IEC 27001, toda empresa que implemente un Sistema de Seguridad de la Información, debe incluir en sus cargos los perfiles de los responsables por áreas y comités de control como se muestra en la tabla 28.

Tabla 28

Roles y Responsabilidades en el SGSI

Comité	Función	Responsable	Roles	Descripción
Comité de Gestión	Gestionar y controlar la implementación del SGSI, tomar decisiones de seguridad.	• Coordinador Ingeniería y gestión. • Técnico en sistemas y mantenimiento • Ingeniero de innovación	• Unidad de TIC • Administradores de red • Investigador • Funcionarios	El Comité de Gestión tiene la responsabilidad de supervisar y controlar la implementación del SGSI y tomar decisiones de seguridad. Incluye roles como la Máxima Autoridad, que aprueba políticas, y el Gestor de Seguridad, responsable de la propuesta y difusión de políticas.
Comité de Dirección	Tomar decisiones de	• Gerente General	• Máxima autoridad (Gerente	El Comité de Dirección se encarga

Comité	Función	Responsable	Roles	Descripción
	seguridad relacionadas con aspectos administrativos, legales, recursos humanos y tecnología.	• Gerente de Ingeniería y Gestión • Gerente proyectos TI	General) • Máxima autoridad (Gerente General), • Gestor de Seguridad	de tomar decisiones de seguridad en temas administrativos, legales, recursos humanos y tecnología. Incluye roles clave como la Máxima Autoridad y el CISO.
Comité de Seguridad	Implementar decisiones de seguridad de manera inmediata, mantener confidencialidad, integridad y disponibilidad de activos de información.	• Coordinador NOC • Gerente Talento Humano	• Gestor de Seguridad • Propietarios de Activos de Información	El Comité de Seguridad tiene la responsabilidad de implementar decisiones de seguridad de forma inmediata y garantizar la confidencialidad, integridad y disponibilidad de activos de información. Incluye roles como el CISO y los Propietarios de Activos de Información.

2.4.16 Plan de socialización y capacitación en el SGSI

Objetivo del plan

El objetivo del plan de socialización y capacitación en el SGSI es asegurar que todos los empleados de SP Sistemas Palacios Ltda adquieran los conocimientos, habilidades y conciencia necesarios para comprender y cumplir con los requisitos de seguridad de la información establecidos en el SGSI, contribuyendo así a la protección efectiva de la información de la organización.

Justificación del plan

La socialización y capacitación son fundamentales para garantizar el éxito de un SGSI. Al proporcionar a los empleados el conocimiento y las habilidades necesarias, se promueve una cultura de seguridad de la información en la organización. Esto ayuda a mitigar los riesgos asociados con el manejo de la información y a proteger los activos de la empresa, fortaleciendo su imagen interna y externa.

Estrategias de socialización y capacitación

Realización de talleres interactivos para fomentar la comprensión de los conceptos clave de seguridad de la información.

Organización de foros o sesiones informativas donde se aborden temas relevantes relacionados con la protección de la información.

Utilización de medios audiovisuales, como videos y presentaciones, para presentar de manera visual los principios y buenas prácticas de seguridad de la información.

Acciones específicas

Realización de un seminario introductorio sobre el SGSI y sus principales componentes. Impartición de talleres prácticos donde los empleados puedan aplicar los conocimientos adquiridos en escenarios simulados.

Elaboración de materiales de capacitación, como manuales y guías, para facilitar el aprendizaje y la consulta posterior.

Evaluación del proceso de socialización y capacitación

Se llevará a cabo una evaluación periódica para medir el impacto y la efectividad del plan de socialización y capacitación. Esto permitirá identificar áreas de mejora y ajustar las estrategias y acciones en consecuencia.

Cronograma

Semana 1: Realización del seminario introductorio sobre el SGSI.
Semanas 2-3: Talleres prácticos en grupos reducidos.
Semana 4: Evaluación del proceso de socialización y capacitación.

Para que las políticas de seguridad que se han creado en el punto anterior seaneficientes, todo el personal de la empresa SP Sistemas Palacios LTDA deben ser capacitados sobre la importancia de la seguridad dela información y los procedimientos que se deben emplear pada dar un correctouso de esta información.

Para las capacitaciones debe existir un responsable por áreas los cuales ayuden a socializar estos temas:

Personal de seguridad: Sera el personal experto en seguridad el cualse encargará de capacitar al personal sobre la seguridad y las buenas prácticas.

Personal de sistemas: Serán los encargados de capacitar al personal en el manejo de los equipos y correcto control en la información interna.

Usuarios finales: Serán los que reciban la capacitación y deberán poner total interés en la capacitación para obtener los nuevos conocimientos.

Programación de las capacitaciones

Sesiones: las capacitaciones deben ser distribuida en varias sesiones lo cual no interrumpa el funcionamiento de la empresa.

Tiempo: para que la capacitación tenga un correcto desarrollo se deben hacer sesiones de una hora.

Material: todo el material para las capacitaciones debe ser interactivo y contener información relevante del tema a ser tratado. Como un método de repaso el personal recibirá en su correo la materia que se empleó en la capacitación.

Evaluación: una vez finalizada la capacitación la empresa debe programar actividades de evaluación las cuales ayuden a verificar el grado de aprendizaje que se ha obtenido en las capacitaciones. En caso de que las evaluaciones que se han tomado al personal no cumplan con una nota satisfactoria se debe implementar retroalimentaciones periódicas con el fin de crear la persona con conciencia sobre la seguridad de la información y su correcto uso.

Verificación y Análisis del diseño del SGSI.

Una vez organizada la información para diseñar el SGSI, se procede a realizar una verificación de los requisitos necesarios para el cumplimiento de los lineamientos que se plantean al inicio de la implementación, con el fin de obtener un sistema de seguridad con calidad.

3. Conclusiones

En este estudio, se logró una comprensión del proceso de gestión de información en el entorno organizacional de SP Sistemas Palacios Ltda. A través del análisis de las diferentes áreas funcionales, se identificaron los flujos de información, las prácticas existentes y las áreas. Se reconoció la importancia de una gestión eficiente de la información para respaldar la toma de decisiones y la operación de la empresa. Lo que sirvió para la elaboración del inventario de activos.

La metodología empleada ha facilitado una clasificación precisa de los activos, que abarca desde información crítica hasta el personal, lo cual resulta fundamental para una identificación y seguimiento eficaces en la protección de la información. Esta clasificación detallada es crucial en el ámbito de la gestión de riesgos y seguridad de la información, sobre todo en un entorno empresarial cada vez más digitalizado y dependiente de la tecnología. Mediante la asignación de códigos únicos a cada tipo de activo, se ha logrado un control más riguroso y una gestión más eficiente de los recursos fundamentales para la empresa. Esto no solo optimiza la seguridad de la información, sino que también contribuye a mejorar la eficiencia operativa y garantizar la continuidad del negocio.

Además, al adaptar esta clasificación a las necesidades específicas de SP Sistemas Palacios Ltda se resalta la importancia de un enfoque personalizado en la gestión de activos. Este enfoque no solo atiende los requisitos particulares de la empresa, sino que también proporciona un marco para continuar mejorando en cuanto a protección y gestión de sus activos. En última instancia, este estudio ofrece una visión integral que resulta vital para tomar decisiones estratégicas, asegurando así resiliencia y sostenibilidad empresarial en un panorama tecnológico siempre cambiante.

La identificación de amenazas, riesgos y vulnerabilidades a la información de SP Sistemas Palacios Ltda utilizando el estándar MAGERIT reveló una visión integral de las posibles vulnerabilidades en su entorno. Al evaluar amenazas y riesgos específicos para cada área administrativa, se obtuvo una comprensión profunda de los desafíos que enfrenta la empresa en

términos de seguridad de la información. Estos hallazgos proporcionan una base sólida para la implementación de medidas de mitigación y la elaboración de estrategias para proteger la información sensible y crítica de la organización.

El análisis de los riesgos presentados en los resultados resalta la complejidad y diversidad de los desafíos que las organizaciones enfrentan al gestionar la seguridad y el funcionamiento de sus sistemas. Los datos recolectados revelan una variedad de vulnerabilidades que abarcan tanto aspectos físicos como digitales, desde la infraestructura de TI hasta el personal y las políticas operativas. En primer lugar, se identificó que los riesgos más importantes están relacionados con el mantenimiento de equipos y sistemas, lo cual destaca la importancia crucial de contar con un sistema adecuado de prevención contra incendios y refrigeración para evitar daños catastróficos. La negligencia en estas áreas puede tener consecuencias devastadoras, no solo en términos de pérdida de equipos, sino también en la continuidad operativa de la organización. Además, se señalan deficiencias en la configuración de seguridad en sistemas operativos clave como Windows, lo cual plantea riesgos relacionados a posibles vulnerabilidades ante ciberataques.

La gestión de roles y sistemas de control surge como otro aspecto crítico donde su ausencia puede resultar en pérdida de información confidencial. Esto se agrava por falta controles adecuados para el personal interno, incrementando así el riesgo del robo documental importante. Asignar responsabilidades inadecuadas o carecer del personal calificado puede además afectar negativamente la productividad y eficiencia del área correspondiente.

Por otro lado, hay preocupaciones relacionadas con las instalaciones, como la falta de controles de acceso adecuados y la ausencia de medidas de protección digital. Esto destaca la importancia de contar con una sólida seguridad física y digital para evitar accesos no autorizados y pérdidas de equipos. Estos aspectos son esenciales para proteger tanto los activos físicos como la integridad y confidencialidad de la información.

En relación a riesgos adicionales como el robo o extravío de dispositivos móviles, la falta de protección de datos en redes públicas y el posible mal uso por parte del personal técnico. Estos riesgos, considerados altamente impactantes, resaltan la importancia que tienen las políticas y

prácticas eficaces en materia de seguridad para proteger tanto los dispositivos como la información tanto interna como externa.

La falta de medidas adecuadas en el control dentro de las instalaciones del cliente, así como en los sistemas corporativos y el acceso a datos es otro factor crítico que requiere atención. La carencia tanto en políticas claras como en personal encargado del mantenimiento documental, junto con una falta de controles adecuados en vehículos y protecciones digitales en dispositivos móviles amplía aún más el rango amplio e importante riesgos a considerar.

La estructuración de la propuesta del Sistema de Gestión de la Seguridad de la Información (SGSI) basado en el estándar ISO/IEC 27001 es un hito significativo en este estudio. Al desarrollar esta propuesta, se definieron objetivos claros, se estableció el alcance del SGSI y se identificaron los controles de seguridad necesarios. Además, se delinearon roles y responsabilidades, se propuso un plan de socialización y capacitación, y se presentó un enfoque en la mejora continua. Esta propuesta proporciona un camino claro para que SP Sistemas Palacios Ltda fortalezca su seguridad de la información y busque la certificación ISO/IEC 27001, lo que es fundamental para garantizar la protección de sus activos de información en un entorno cada vez más digital y amenazante.

4. Recomendaciones

Dado el análisis detallado de amenazas y vulnerabilidades, en consecuencia, se recomienda utilizar este trabajo como referencia para el análisis de amenazas y vulnerabilidades en la empresa en cuestión.

Considerando la importancia de una gestión eficiente de la información, por lo tanto, se sugiere diseñar en primera instancia políticas de seguridad enfocadas en los objetivos de negocio de SP Sistemas Palacios Ltda.

De acuerdo con la propuesta del Sistema de Gestión de Seguridad de la Información (SGSI), asimismo, se propone considerar los estándares de la ISO/IEC 27001 para implementar y controlar el sistema de seguridad de la información.

Dada la necesidad de crear conciencia en seguridad de la información, por consiguiente, se recomienda realizar sesiones de concientización en seguridad de la información con los empleados de la compañía.

Con el objetivo de prevenir posibles brechas de seguridad y fugas de información, en este sentido, se sugiere implementar un monitoreo y seguimiento constante, así como la aplicación de actualizaciones en sistemas operativos, aplicaciones y software.

En el mismo contexto de prevención de amenazas, por ende, se recomienda programar y llevar a cabo actualizaciones periódicas de las firmas de antivirus, antispyware y otras aplicaciones.

Considerando la necesidad de fortalecer la seguridad de la información, por lo tanto, se sugiere iniciar la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en los estándares de la ISO/IEC 27001, teniendo en cuenta los puntos anteriores.

Referencias bibliográficas

Acosta, N. y León, T. (2017). *Diseño del Sistema de Gestión de Seguridad de la Información (SGSI) para el centro de datos de la personería de Bogotá DC bajo las normas NTC-ISO-IEC 27001: 2013 y GTC-ISO-IEC 27002: 2013*.

Aguirre, R. y Zambrano, A. (2015). *Estudio para la implementación del sistema de gestión de seguridad de la información para la secretaria de educación departamental de Nariño basado en la norma ISO/IEC 27001*

Amutio, M. y Candau, J (2012). *Portal de Administración Electrónica MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Libro 1. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

Ariasca Suma, F. L. y Quispe Borda, S. K. (2017). *Desarrollo de una propuesta de implementación de la ntp iso/iec 27001: 2014, sistema de gestión de seguridad de la información, para la oficina funcional de informática del gobierno regional* Cusco.

Blandón Jaramillo, C. y Benavides Sepúlveda, A. (2018). *Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico*. *Scientia Et Technica, 23* (1), 85-92. https://www.redalyc.org/journal/849/84956661012/84956661012.pdf

Buitrago, J., Bonilla, D. y Murillo, C. (2012). *Diseño de una metodología para la implementación del sistema de gestión de seguridad de la información - SGSI basado en ISO 27001*. http://repository.ean.edu.co/bitstream/handle/108.

De la Cruz, V. (2016, 19 de enero). *Metodología Cualitativa.* http://elmundodelametodologia19.blogspot.com/2016/01/tipos-de-investigacion.html

Decreto 2578 de 2012. (2012, 13 de diciembre). Ministerio de Cultura. Diario Oficial No. 48.643. https://www.icbf.gov.co/cargues/avance/docs/decreto_2578_2012.htm

Departamento Nacional de Planeación [DNP]. (2016) *Lineamientos para la administración de riesgos en los procesos del DNP*. https://colaboracion.dnp.gov.co/CDT/DNP/ARL02%20Lineamientos%20Administracion%20Riesgos.Pu.pdf.

Gómez, A. (2015*). Enciclopedia de la Seguridad Informática.* https://www.ecoeediciones.com/wp-content/uploads/2015/08/seguridad-informatica-basico.pdf.

Hernández, R. Fernández, C. y Baptista, P. (2014). *Metodología de Investigación.* https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf.

ISO 27001. (2013). *Certificación ISO 27001 y para qué sirve.* https://www.unir.net/ingenieria/revista/iso-27001/#:~:text=La%20ISO%2027001%20es%20una,y%20aplicaciones%20que%20la%20tratan

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

Ley 1273 de 2009. (2009, 5 de enero). El Congreso de Colombia. Diario Oficial No. 47.223. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Ley 1341 de 2009. (2009, 30 de julio). El Congreso de Colombia. Diario Oficial No. 47.426. http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html

Ley 1712 de 2014. (2014, 6 de marzo). El Congreso de Colombia. Diario Oficial No. 49.084. http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html

Ley 527 de 1999. (1999, 18 de agosto). El Congreso de Colombia. Diario Oficial No. 43.673. http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

Ley 599 de 2000. (2000, 24 de julio). El Congreso de Colombia. Diario Oficial No. 44.097. http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

Martínez Orencio, A. (2013). L*a información en la organización, su gestión y Auditoría.* https://www.gestiopolis.com/la-informacion-en-la-organizacion-su-gestion-y-Auditoria

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia [Min TIC]. (s.f.). *Modelo de Seguridad de la Información. Seguridad y Privacidad de la Información.* https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf.

Ministerios Nacional de las Tecnologías de la información y las Comunicaciones [Min TIC]. (2008). *Informe final – modelo de seguridad de la información – sistema sansi - SGSI - modelo de seguridad de la información para la estrategia de gobierno en línea*. http://programa.gobiernoenlinea.gov.co/apc-aa

Pacheco, F. (2010). *La importancia de un SGSI. Welivesecurity.* https://www.welivesecurity.com/laes/2010/09/10/la-importancia-de-un-sg.

Peñuela Vásquez, Y. (2018). *Análisis e identificación del estado actual de la seguridad informática* [Monografía de investigación, Universidad abierta y a Distancia]. Fusagasugá, Colombia.

Pérez, M. y Jurado, M. (2018). *Diseño de un sistema de gestión de seguridad de la información para la ferretería argentina de la ciudad de Pasto*. https://repository.unad.edu.co/bitstream/handle/10596/18306/1087414445.pdf?sequence=1&isAllowed=y

Portal Administración Electrónica [PAE]. (2012) *Dirección General de Modernización Administrativa.* Disponible en: https://administracionelectronica.gob.es/pae_Home/.

Ramos, J. y Morales, J. (2020). *Diseñar el sistema de gestión de seguridad de la información-*

SGSI-para el proceso análisis de laboratorio de físico química de suelos de la corporación colombiana de investigación agropecuaria–Agrosavia

Requena Serra, B. (2022). *Muestreo Intencional.* https://www.universoformulas.com/estadistica/inferencia/muestreo-conveniencia/.

Resolución 500 de 2021. (2021, 10 de marzo 10). Ministerio de Tecnologías de la Información y las Comunicaciones. Diario Oficial No. 51.619. https://www.icbf.gov.co/cargues/avance/docs/resolucion_mintic_0500_2021.htm

Tamayo y Tamayo M. (2003) *Proceso de Investigación Científica*. Editorial Limusa. https://www.gob.mx/cms/uploads/attachment/file/227860/El_proceso__de_la_investigaci_n_c ient_fica_Mario_Tamayo.pdf.

Valencia, F. y Orozco, M. (2017). *Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27001. Revista Ibérica de Sistemas e tecnologías de Informação*, (22), 73.

Vargas, E. y Marchan, A. (2019). *Propuesta de diseño de un Sistema de Gestión de la Seguridad de la Información según la NTP ISO/IEC 27001: 2014* para la Universidad del Pacífico.

Vásquez Guerrero, M. (2022). 3 *pilares de la seguridad informática.* http://www.icorp.com.mx/blog/seguridad-informatica/.

Villamizar, R. (2013). *CISA. CISM. CGEIT. CRISC. Cobit Foundation Certificate e ISO 27001*. Jugando a crear cultura de seguridad.