PLAN ESTRATÉGICO PARA LA IDENTIFICACIÓN DE RIESGOS Y VULNERABILIDADES EN LA SEGURIDAD DE LA INFORMACIÓN DE LOS DATOS PERSONALES EN UNA EMPRESA

MODALIDAD: INVESTIGACIÓN

JAVIER IVAN PATIÑO CASTRILLON

JOSED ESTID BEDOYA VELASQUEZ

DIRECTOR:

SEBASTIAN GOMEZ JARAMILLO

CODIRECTOR:

YEILER ALBERTO QUINTERO BARCO

Tecnológico de Antioquia - Institución Universitaria
Ingeniería en Software
Medellín, Colombia.
2023

DEDICATORIA

Queremos expresar nuestra profunda gratitud a nuestros padres, quienes nos han apoyado incondicionalmente en este camino. Agradecemos a nuestros profesores por su paciencia y dedicación en guiarnos hacia el éxito. A Dios, gracias por ser nuestra fuente de inspiración y motivación constante. Nos felicitamos por perseverar en este camino, superando obstáculos y alcanzando nuestras metas. ¡Somos testigos de nuestro propio crecimiento y logro!

AGRADECIMIENTOS

A través de este proyecto de grado, quiero expresar mi más profundo agradecimiento a aquellos que me apoyaron durante todo este proceso. A mis padres, les agradezco por su amor incondicional y por creer en mí incluso cuando yo mismo no lo hacía. A mis profesores, por su dedicación y guía, gracias por ayudarme a crecer académica y personalmente. A mis compañeros, su colaboración y amistad fueron fundamentales para alcanzar este logro. Cada uno de ustedes ha dejado una huella en mi vida y estoy profundamente agradecido por ello. Este proyecto no solo es mi trabajo, sino también el resultado del esfuerzo y la colaboración de todos.

RESUMEN

Este trabajo se centra en la seguridad de la información en empresas y tiene como objetivo diseñar un plan estratégico para abordar este aspecto crítico. El estudio de caso se desarrolla en una empresa de gran envergadura con más de 45.000 empleados.

El plan estratégico elaborado abarca desde las plataformas principales de la compañia hasta los recursos físicos de la misma. El desarrollo de esto representa un desafío significativo en términos de seguridad de la información debido a la cantidad de datos confidenciales y la complejidad de los sistemas involucrados.

A través de un análisis exhaustivo, se implementaron medidas de seguridad apropiadas para salvaguardar los datos y proteger la infraestructura de TI de la empresa. Se desarrollaron políticas y procedimientos detallados para garantizar el cumplimiento de las regulaciones y estándares de seguridad relevantes.

El equipo encargado del proyecto trabajó en estrecha colaboración con los diferentes departamentos y personal de la empresa, implementando medidas de concienciación y capacitación en seguridad de la información para garantizar una adopción exitosa y una cultura de seguridad sólida.

El plan estratégico se ejecutó con éxito. Esto debido a que en el semestre de desarrollo de este proyecto 2023 01, la compañía entro en un ambiente propicio para el cumplimiento del mismo. Este se llevó a cabo de manera segura, minimizando los riesgos y garantizando la protección de los datos de la empresa y la continuidad de las operaciones.

En conclusión, este trabajo demuestra la importancia de contar con un plan estratégico sólido en seguridad de la información y cómo su implementación adecuada puede conducir a resultados exitosos. La empresa en estudio logró mejorar su postura de seguridad, proteger su información sensible y fortalecer su posición en un entorno empresarial cada vez más amenazante.

PALABRAS CLAVE

Seguridad, información, empresa, amenazas, riesgos, vulnerabilidades, datos, empresas, normativa, protección, identificación, objetivos, lineamientos, búsqueda, plan, evaluar, analizar, evaluación, lineamiento, implementar, prevenir, SAP, Google Workspace, HCL, ERP, CVE, mitigación, vulnerabilidad, nube, migración y TI, SGSI

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ABREVIATURAS

SAP: Systems Applications and Products in Data Processing

AWS: Amazon Web Services

ERP: Sistema de planificación de recursos empresariales

CVE: Common Vulnerabilities and Exposures

TI: Tecnología e informática

HCL: Hindustan Computers Limited Technologies

SGSI: Sistema de gestión de la seguridad de la información

DOFA: Debilidades, Oportunidades, Fortalezas, Amenazas

VPN: Virtual Private Network

KPI: Indicador clave de rendimiento

MSPI: Modelo de Seguridad y Privacidad de la Información

1. INTRODUCCIÓN

La seguridad de la información es un tema de vital importancia en el contexto empresarial actual. Los sistemas de información de las organizaciones se encuentran expuestos a diversas amenazas que pueden comprometer la integridad, confidencialidad y disponibilidad de los activos de información. Estas amenazas representan un riesgo significativo que puede ocasionar graves daños tanto a las empresas como a los actores involucrados.

Con el crecimiento y la complejidad de los sistemas de información, los riesgos y vulnerabilidades asociados también han aumentado. En este sentido, se hace necesario implementar un plan estratégico efectivo que permita garantizar la seguridad de la información en las organizaciones. Este plan estratégico debe abordar no solo los controles de seguridad, sino también la identificación y prevención de posibles riesgos y vulnerabilidades.

En el ámbito empresarial, la protección de los datos personales ha cobrado gran relevancia. Los datos personales se consideran activos de alto valor económico y estratégico, por lo que su seguridad se convierte en un factor clave para el desarrollo y la continuidad operativa de las empresas. Sin embargo, muchas organizaciones centran sus esfuerzos en el control de la información en lugar de en la prevención de amenazas, lo que puede dar lugar a situaciones en las que la información resguardada se ve comprometida.

Además, se ha observado un aumento significativo de los ataques y amenazas dirigidos a las empresas en el ámbito de la seguridad de la información. Esto evidencia la necesidad de contar con un plan estratégico que permita identificar y abordar de manera efectiva los riesgos y vulnerabilidades existentes.

En este contexto, el presente estudio se propone desarrollar un plan estratégico para la identificación de riesgos y vulnerabilidades en la seguridad de la información de los datos personales de una empresa. El objetivo principal es establecer un enfoque preventivo que permita proteger de manera efectiva los activos de información y garantizar la continuidad operativa de la organización.

Para lograr este objetivo, se llevará a cabo un análisis exhaustivo de los lineamientos existentes en la identificación de riesgos y vulnerabilidades en la seguridad de la información. Además, se analizarán los riesgos y vulnerabilidades específicos relacionados con los datos personales en el contexto empresarial. A partir de este análisis, se diseñará un plan estratégico que integre estrategias de seguridad efectivas y se validará su implementación a través de un caso de estudio en un entorno empresarial real.

La presente investigación tiene como objetivo contribuir al avance del campo de la seguridad de la información, proporcionando a las organizaciones una herramienta sólida para proteger sus activos de información y mitigar los riesgos y vulnerabilidades asociados. Se espera que los resultados

obtenidos sean de utilidad tanto para las empresas que deseen fortalecer su seguridad de la información como para la comunidad académica y profesional interesada en este tema.

En resumen, este estudio se enfoca en el desarrollo de un plan estratégico para la identificación de riesgos y vulnerabilidades en la seguridad de la información de los datos personales de una empresa. A través de la implementación de este plan, se busca fortalecer la seguridad de la información y minimizar los riesgos asociados, contribuyendo así al avance del campo y brindando a las organizaciones una herramienta eficaz para proteger sus activos de información y garantizar su continuidad operativa en un entorno digital cada vez más complejo.

2. MARCO DEL PROYECTO

PLAN ESTRATÉGICO PARA LA IDENTIFICACIÓN DE RIESGOS Y VULNERABILIDADES EN LA SEGURIDAD DE LA INFORMACIÓN DE LOS DATOS PERSONALES EN UNA EMPRESA

2.1. Definición del problema

Los sistemas de información de la empresa están expuestos a amenazas que aprovechan cualquier vulnerabilidad prevista, estas amenazas son un riesgo de seguridad puesto pueden exponer los activos de información por espionaje, vandalismo o sabotaje causando graves daños a las organizaciones, así como a los demás entes involucrados con estas. Los riesgos y vulnerabilidades siempre estarán presentes aunado al aumento de los sistemas de información hace que todos los sistemas están expuestos a riesgos cada vez mayores y sin un adecuado plan estratégico la empresa se verá ampliamente afectada.

Es por este motivo con la seguridad de la información ha ido adquiriendo cada vez más importancia dentro de la gestión empresarial por lo que se han generado una serie de procedimientos y normativas para garantizar la seguridad de la información. Sin embargo, la empresa debe estar constantemente innovado o realizando controles de seguridad para adaptarse a los constantes retos de seguridad que se han desarrollado en esta era digital.

Ahora bien, cabe destacar la presencia en aumento de la protección de los datos personales en la empresa hoy en día por cuanto estos se consideran un activo de gran valor económico para cierta empresa y de valor estratégico. Así pues, resulta un factor clave para el desarrollo empresarial generar sistemas de seguridad basados en la protección de los datos personales. Sin embargo, resulta que en su mayoría la empresa centra sus sistemas de seguridad en el control más que en la prevención de amenazas por lo que en ocasiones parte de la información resguardada resulta comprometida.

Ahora bien, como se mencionó en la motivación de la propuesta, se ha ido observando un creciente ataque y amenaza a este sector alimenticio a nivel de grandes empresas, considerando la evolución de las amenazas a la ciberseguridad de las empresas a nivel general, es posible señalar que ya existe una amenaza para el sector alimenticio en este sentido (Figura 1). Por tal razón, la presente idea de investigación se centra en la propuesta para un plan estratégico para la identificación de riesgos y vulnerabilidades de la seguridad de la información de los datos personales de una empresa que está basado en la prevención de riesgos y vulnerabilidades más que en el control.

Una empresa que opera en el sector de alimentos y productos al consumidor, continuamente enfrenta retos en cuanto a mitigación de riesgos y vulnerabilidades en la seguridad de la información. Todo esto debido al gran conglomerado de empresas que tienen en su sombrilla y al gran volumen de datos que manejan, que al año 2023 sobrepasó los 1.104TB de información.

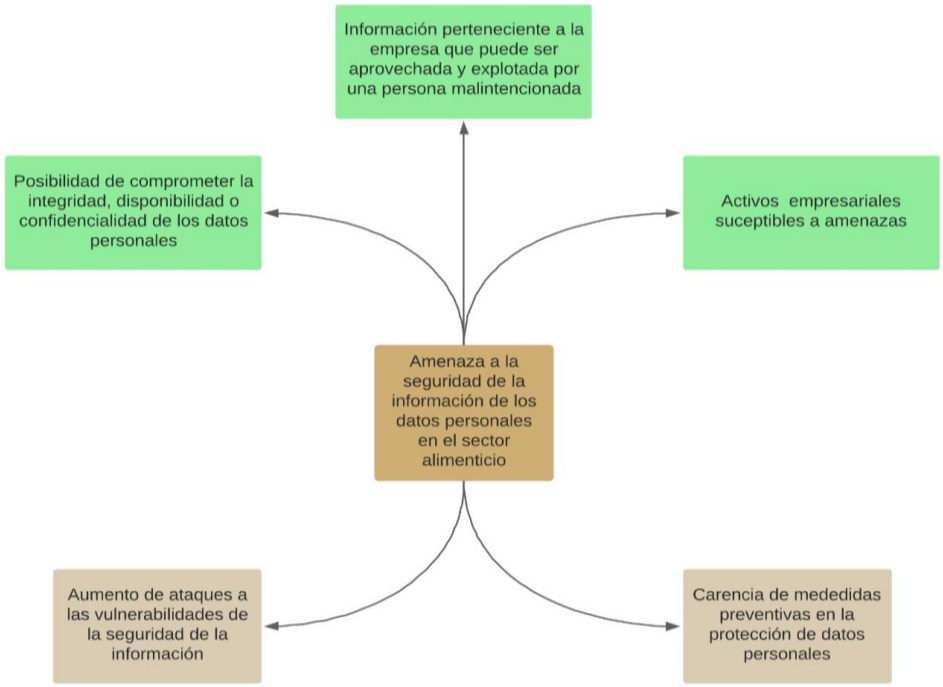

Ilustración 1 Árbol del problema

Fuente: Elaboración propia (2022)

2.2. Pregunta problematizadora

¿Es posible implementar un plan estratégico para la identificación de riesgos y vulnerabilidades que amenazan a la seguridad de la información de los datos personales en el sector alimenticio

2.3. Justificación del problema

La era de la información trajo innumerables beneficios para el mundo globalizado. ACEI (2020) destaca que el acceso y democratización de la información, así como los retos en el tratamiento de los datos, son algunos de los beneficios que se aprecian hoy día. Las empresas actuales dan vital importancia a la recolección de datos personales, lo que hace fundamental proporcionar seguridad a sus sistemas de información para proteger a los involucrados y a la sociedad en general (ACEI, 2020).

Por lo tanto, es crucial profundizar en la búsqueda de riesgos y vulnerabilidades en seguridad de la información de los datos personales existentes en las empresas. Un plan estratégico de seguridad de la información es pertinente y conveniente debido a la creciente cantidad de amenazas en el entorno digital y la dependencia de las empresas en tecnologías de la información (Upwork, n.d.;

OPSWAT) Al contar con una estrategia sólida, las organizaciones pueden adaptarse de manera proactiva a los cambios en el paisaje de riesgos y mantenerse protegidas frente a las amenazas actuales y futuras.

El autor Bowcut (2021) menciona que históricamente el sector agroalimentario no había sido un objetivo importante para los Ciber delincuentes. Sin embargo, en la actualidad, ha habido un aumento de amenazas a empresas de este sector debido a que una cadena de suministro de alimentos bien establecida resulta en una oportunidad para usar malware como palanca para que los atacantes logren sus objetivos, que pueden ser ganancias financieras, actos de terrorismo político y hacktivismo social.

Por ello, desde el punto de vista práctico, se propone un plan estratégico de seguridad de la información que pueda ser implementado o adaptado a empresas con la necesidad de protección y seguridad de la información de datos personales centrados en la identificación preventiva de riesgos y vulnerabilidades. Además, este enfoque permitirá a profesionales desarrollar conocimientos en ciberseguridad, en la identificación de amenazas y riesgos de seguridad de la información y, específicamente, en la protección de los datos personales de la empresa.

El enfoque propuesto se considera un plan estratégico de seguridad de la información debido a que implica la identificación y evaluación de riesgos y vulnerabilidades en los sistemas de información de una empresa, para luego desarrollar e implementar medidas de prevención, protección y recuperación. La adopción de un plan estratégico permite a las organizaciones enfrentar de manera proactiva los desafíos en materia de seguridad de la información y garantizar la protección de los datos personales de sus clientes y empleados, así como la continuidad de sus operaciones (NIST, 2018).

Algunos de los beneficios de adoptar un plan estratégico de seguridad de la información incluyen:

- **Protección de la información y reducción de riesgos:** Al lograr identificar y abordar las vulnerabilidades, se logra proteger la información contra posibles amenazas, y adelantarse a posibles eventos mediante la prevención involucrados (CSO, 2021).
- **Mantener la confianza de los clientes e inversores**: La implementación de un plan estratégico demuestra el compromiso con la protección de los datos personales, lo que aumenta la confianza de los clientes e inversores (CSO, 2021).
- **Mejora en la respuesta a incidentes:** Un plan estratégico incluye protocolos que le permiten a la empresa reaccionar de manera rápida y efectiva en caso de brechas o ataques (NIST, 2018).
- **Cumplimiento normativo**: Un plan estratégico garantiza que la empresa cumpla con los diferentes marcos legales y regulatorios en materia de seguridad de la información y protección de datos personales (CSO, 2021).
- **Optimización de recursos y gastos:** Al contar con un plan estratégico, la empresa puede asignar de manera eficiente sus recursos a un plan estratégico ante incidentes de seguridad, lo que puede reducir costos a largo plazo (NIST, 2018).

2.4. Marco referencial

Con el objetivo de diseñar un plan que integre estrategias de seguridad que ayuden a la identificación de riesgos y vulnerabilidades existentes para la seguridad de la información de los datos personales en la empresa, se requiere seleccionar una empresa para validar el plan estratégico con un caso de estudio en un contexto empresarial

2.4.1. Aspectos generales

Descripción de la empresa

El centro de servicios compartidos de Empresa del sector alimenticio es una entidad encargada de brindar soluciones y administración de recursos para todo el Negocio. Además de ofrecer servicios empresariales y conocimientos especializados, su objetivo principal es generar oportunidades de intraemprendimiento y sinergias para impulsar la productividad, competitividad y sostenibilidad de sus clientes. Se apalancan en la innovación y la tecnología para cumplir con esta misión.

Información:

- NIT: 9000813608
- Actividad: Fabricación y comercialización de productos alimenticios.
- Forma jurídica: Sociedad por acciones simplificada.
- Razón Social: Grupo Nutresa (Servicios Nutresa Medellín)
- Teléfono: +57 (4) 6044444
- Ciudad: Medellín.
- Departamento: Antioquia.
- Dirección: Cra. 52 #238, Guayabal, Medellín, Guayabal, Medellín, Antioquia

2.5. Antecedentes

Para una correcta comprensión de la temática desarrollada, se debe tomar en cuenta que la presente investigación tiene dos puntos a considerar al revisar la literatura. El primero es la identificación de riesgos y vulnerabilidades de la seguridad de la información, y el segundo es la protección de datos personales; por tal razón los antecedentes seleccionados se dividen en dos bloques.

El primer bloque de investigaciones consideradas como antecedentes está dirigido a estudiar la protección de datos personales. Así pues, se ha considerado el artículo científico desarrollado por Martínez (2022) el cual tiene como objetivo principal analizar los requerimientos de seguridad que derivan de la aplicación del Reglamento General de Protección de Datos, el cual es un reglamento europeo para la protección de datos personales de las personas físicas. Asimismo, el autor identifica los factores de riesgo que a su juicio afectan a la institución universitaria. Considerando los detalles del estudio, resulta en un aporte referencial ligado al tema de la seguridad de la información de los datos personales, pero se encuentra limitado tanto territorialmente al estar basada en la normativa

europea, como sectorialmente pues se centra en la seguridad de la información de las instituciones universitarias.

Por otro lado, se tiene el estudio de Checca (2021) donde se analiza la gestión de riesgos de seguridad de la información ISO/IEC 27005 para determinar su influencia en la protección de datos personales en la empresa Zicsa S.A. de Perú. Al estudiar la ISO/IEC 27005 de gestión de riesgos de seguridad de la información, se centraron en dos indicadores que son relevantes para poder determinar la influencia que tiene sobre la protección de datos personales, para ello se hace el recorrido general de la ISO/IEC 27005 siempre alineada a los procesos de negocio de Zicsa S.A. para no perder el foco de la relevancia que significa esta aplicación para los beneficios organizativos. En líneas generales, el estudio proporciona información valiosa relativa a indicadores respaldados por la norma a considerar al momento de diseñar un plan estratégico centrado en la protección de datos personales.

De igual manera, se considera el estudio de Castañeda y Villegas (2020) la que proporciona una serie de recomendaciones y estrategias que pueden ser un aporte referencial en materia de Protección de Datos para la elaboración del plan propuesto, en específico aquellos datos alojados en la Nube que es un sistema ampliamente utilizado por la empresa hoy en día, considerando también que este aporte está limitado por dicha especificación al solo estudiar lo relativo a seguridad de la información alojadas en nube.

Asimismo, Cordoba (2021) realizó una investigación relacionada con el tema cuyo objetivo central fue diseñar un sistema automatizado de gestión de la seguridad de la información basado en la Norma ISO/IEC 27001:2013 para dar cumplimiento a la Ley 1581 de 2012 de protección de datos personales en el departamento de sistemas de una institución universitaria en Colombia. El mismo resulta relevante para la propuesta presentada puesto realiza un estudio sobre la normativa relativa a los sistemas de gestión de seguridad de la información en relación a la protección de los datos personales con la finalidad de desarrollar un sistema automatizado, no obstante, el estudio de los aspectos más resaltante sobre la seguridad de la información en lo relativo a los datos personales es el verdadero aporte a la presente.

También se tiene el estudio de Viguri (2021) en donde se realiza un análisis de los mecanismos de certificación vigentes desde la efectiva aplicación del Reglamento General de Protección de Datos. Parte con un recorrido doctrinal técnico y jurídico en lo relacionado con la protección de datos pasando por el examen de las regulaciones de los mecanismos de certificación del reglamento en distintos países entre los que destaca España, Francia y el Reino Unido. Finalmente, analiza los estándares internacionales ISO/IEC de la serie 27000 y de las normas ISO/IEC 27001 sobre seguridad de la información y 27701 sobre gestión de la información de privacidad y sus correspondientes actualizaciones. Esta última parte del artículo resulta en un aporte para el desarrollo teórico de la presente pues desglosa las normativas internacionales vigentes en lo que concierne a seguridad de la información y protección de datos personales.

A este respecto, Diaz y Prieto (2021) desarrollaron un proyecto orientado a la evaluación de los controles aplicados a los activos de información del Hospital Rafael Uribe Uribe específicamente

a los que hacen referencia a la seguridad de los datos almacenados en la Historia Clínica de los pacientes. Utiliza dos herramientas de trabajo, la primera es el Framework de Ciberseguridad (CSF), como también la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Magerit) para la identificación de activos de información. Su interpretación resultada del estudio en relación a las mejoras del SGSI por medio del mejoramiento de los controles es un aporte importante para la construcción del plan estratégico por cuando los controles en la seguridad de la información están dirigidos a la protección de daos personales y puede ser una referencia en el desarrollo del plan estratégico preventivo para las amenazas en la seguridad de la información.

Relacionado al estudio anterior, se tiene el proyecto de Gibau (2022) que se dirigió a diseñar un sistema de gestión de protección de datos personales basados en la norma ISO/IEC 27701:2019 para una institución cuyo principal servicio consiste en la provisión de evaluaciones de competencias profesionales y académicas. Uno de los objetivos de dicha investigación estuvo dirigido al diseño de procesos, políticas y marcos para cumplir con las cláusulas necesarias para un sistema de gestión de seguridad de la información, según el estándar ISO 27001:2013, incluyendo las respectivas extensiones que presenta el estándar ISO 27701:2019 para incluir la gestión de protección de datos personales. Esto resulta de utilidad por cuanto da bases en la elaboración de un plan estratégico dirigido a la protección de datos, a pesar de no estar orientado a la identificación de riesgos y vulnerabilidades aun desglosa aspectos importantes a tener en cuenta en la seguridad de la información.

Siguiendo con los lineamientos planteados, dentro del segundo bloque de investigaciones consideradas como antecedentes para la propuesta se tienen los estudios dirigidos a la identificación de riesgos y vulnerabilidades de la seguridad de la información. Por tanto, se considera la investigación realizada por Escobar, Márceles, Montano y Varona (2021) en donde se destacó la importancia de la ciberseguridad a la hora de desarrollar un plan estratégico de identificación de amenazas y riesgos, puesto no solo se encarga de la seguridad de la información sino también sobre la prevención de riesgos. Aporta un plan de mejoramiento de la seguridad de la información a ser tomado en cuenta puesto está basado en estándares ISO y presenta un plan de prevención de riesgos e identificación de amenazas que se deben estudiar en profundidad como un referente debido a su limitante al sector universitario.

Seguidamente, se seleccionó el artículo desarrollado por Guerra, Neira, Diaz y Patiño (2021) en donde examinan los aspectos relevantes para el desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias. El estudio de esta metodología resulta en un aporte para la propuesta a desarrollar por cuanto la metodología ofrece elementos a considerar en la identificación de riesgos relacionados con la seguridad de la información.

Siguiendo en esa línea, esta García (2021) quien implemento un sistema de gestión de la seguridad de la información basado en la norma ISO/IEC 27001 para optimizar el análisis de los riesgos informáticos en una empresa del Perú. En su proyecto, contribuye en el análisis de los riesgos informático, identificando los activos de la información y reconociendo todo tipo de vulnerabilidades y amenazas en las áreas seleccionadas para el estudio, así como también determina

una valoración a los riesgos para su posterior definición de controles. Por ello, ayuda en la construcción de un plan estratégico dirigido a la identificación de riesgos y vulnerabilidades relacionados con la información como activos empresariales.

Por su parte, Recalde y Rocha (2019) también desarrollaron modelo de gestión de la seguridad de la información (SGSI) basado en las normas NTE INEN-ISO/IEC 27000 permite dotar a las mismas de una herramienta de gestión para la seguridad de la información adaptable a sus objetivos estratégicos y requerimientos de seguridad, que permite garantizar su confidencialidad, integridad y disponibilidad, a través de un manejo adecuado de los riesgos a los cuales pueden estar expuestos los activos de información, no obstante el mismo está dirigido para las entidades del Sector Público en vez del sector privado.

Igualmente, se considera el estudio de Ortega-Guillén y Cuenca-Tapia (2022) en la que se implementó un Sistema de Gestión de Seguridad de la Información en la empresa realizando un análisis y evaluación general de todos los riesgos existentes en esta, además se realizó una valoración junto a un modelo de madurez respecto a los riesgos iniciales identificados. Esta investigación proporciona un Sistema de Gestión de Seguridad de la Información que se puede estudiar como un referente para la construcción del plan estratégico propuesto, además de proporcionar teoría relevante relativa a la evaluación de riesgos de seguridad de la información aun así siendo un aporte limitado al ser un caso de estudio.

Por otra parte, se consideró la investigación de Soto, Vargas y Toro (2021) el cual desarrollo un modelo de políticas estrategias y controles que permitan minimizar los riesgos para la seguridad de la información en la nube híbrida existente en las organizaciones. Ahora bien, el modelo de seguridad de la información en las nubes hibridas procura un aporte referencial para ser tomado en consideración en la construcción del plan propuesto puesto, tal como hace referencia, hoy en día existe un alto crecimiento en la empresa que están utilizando los entornos de nube como repositorio de datos e información y dicha investigación proporciona un alto grado de referentes teóricos relativos al tema, así como un referente de estrategias para minimizar los riesgos de seguridad de la información. Sin embargo, el aporte está limitado en cuanto a temática pues está centrado solo en información alojada en nubes hibridas.

También, se consideró la investigación realizada por Porra (2020), orientada a determinar la influencia de la implementación del Sistema de Gestión de Seguridad de la Información en la gestión de riegos en activos de información en la Empresa de BPO Contac Center Digitex de Lima en Perú, esto se logró analizando el SGSI de la ISO/IEC 27001:2013 permitiendo distinguir con claridad las ventajas que se obtienen al haberla implementado en la empresa y la eficacia al alinearse con los procesos de negocio. El aporte de dicho estudio se dirigió a la interpretación de la influencia del sistema en la prevención de riesgos de activos de información dando orientación en lo relativo a la protección de datos para la construcción del plan estratégico propuesto.

Igualmente, se considera el estudio de Rea (2021) en donde se analiza una serie de modelos de madurez relativos a la ciberseguridad, describiendo cada uno de los modelos y cada una de las etapas de la madurez en las organizaciones con relación a la seguridad de la información. Así pues,

esta tesis tiene como objetivo demostrar la necesidad de contar con un marco de trabajo de gestión de riesgos en ciberseguridad en base al modelo conceptual que incluya todos los elementos de la gestión de riesgos y que ayude a la organización a identificar y evaluar los riesgos en ciberseguridad. Asimismo, aporta materiales teóricos para identificación de riesgos y vulnerabilidades relativos a la ciberseguridad a nivel general que pueden sentar las bases doctrinales y referenciales para el desarrollo de la propuesta.

De igual modo, se considera el estudio realizado por Molina y Orozco (2020) donde se realiza una revisión del estado del arte como también de las metodologías implementadas en temas de vulnerabilidad de los sistemas de información, planteando aspectos importantes de la ciberseguridad. Cabe destacar, la investigación procura un aporte significativo en lo relativo a la seguridad de la información puesto estudia las vulnerabilidades de estos, por lo que pueden dar una base en la identificación de riesgos y vulnerabilidades generales en los sistemas de información que deben ser consideradas en la propuesta planteada.

Por su parte, también se consideró el artículo realizado por Rodríguez, Ramírez y González (2020) la cual proporciona información relevante sobre las buenas prácticas, amenazas cibernéticas y algunas herramientas informáticas que pueden ayudar a mitigar posibles incidentes relacionados a los sistemas de información de las miPymes. Así pues, esta guía facilita información teórica y referencial relativa a la ciberseguridad y en la identificación de riesgos en este sector empresarial, ayudando en la construcción del plan estratégico propuesto.

Seguidamente, se tiene la investigación de Amariles, Vargas y Agudelo (2020) la cual proporciona importante información relativa tanto a la gestión de información, seguridad de la información y en la detección de riesgos o amenazas a esta información. De igual modo, desarrolla un conjunto de estrategias para la prevención de riesgos de seguridad de la información que pueden ser considerados como material referencial en la construcción del plan que se pretende proponer. No obstante, el aporte se encuentra limitado por un lado pues no toca el tema de protección de datos personales y, por otro, está orientada al proceso misional de investigación.

También, se tiene la investigación realizada por Quevedo-Rojas y Vintimilla-Jara (2020) el que proporciona información importante sobre el tratamiento de riesgos de seguridad de la información basados en la norma ISO 27005 que es información importante para la construcción del plan propuesto. Asimismo, es un referente para la elaboración de planes de gestión de riesgos de seguridad de la información, utilizado en la presente propuesta por ello, pero limitado al ser un plan que pretende ser aplicado a varios departamentos de una empresa.

Finalmente, se considera el proyecto de desarrollo de software presentado por Castillo (2022) en donde desarrolla una aplicación web y móvil para la gestión de riesgos de seguridad de la información de acuerdo con una metodología adecuada en el marco de la norma NTP -ISO 27001 para el sector empresarial de consultoría de sistemas. Dicho proyecto propone gestionar y salvaguardar los activos de información de una empresa frente a riesgos de pérdida, divulgación, indisponibilidad o alteración. Para poder cumplir con el objetivo propuesto, tuvo que examinar las metodologías existentes y estándares de calidad internacionales referentes a la gestión de seguridad

de la información, para finalmente seleccionar la metodología MAGERIT y tener en cuenta las normativas ISO para el desarrollo de la aplicación web y móvil para la gestión de riesgos de seguridad de la información.

Tabla 1 Categorización de estudios

Plan estratégico para la identificación de riesgos y vulnerabilidades en la seguridad de la información de los datos personales en una empresa del sector alimenticio

Autor	Elementos significativos				
	Plan estratégico	**Seguridad de la información**	**Riesgos y vulnerabilidades en la información**	**Protección de datos personales**	**Empresa del sector alimenticio**
Martínez (2022)			X	X	
Checca (2021)		X	X	X	
Castañeda y Villegas (2020)	X			X	
Córdoba (2021)		X		X	
Viguri (2021),		X		X	

Tabla 1 Categorización de estudios

Autor	Elementos significativos				
	Plan estratégico	**Seguridad de la información**	**Riesgos y vulnerabilidades en la información**	**Protección de datos personales**	**Empresa del sector alimenticio**
Diaz y Prieto (2021)		X		X	
Gibau (2022)		X	X	X	
Escobar y otros (2021)		X	X		
Guerra y otros (2021)		X	X		
García (2021)		X	X		
	Elementos significativos				

Autor	Plan estratégico	Seguridad de la información	Riesgos y vulnerabilidades en la información	Protección de datos personales	Empresa del sector alimenticio
Ortega-Guillén y Cuenca-Tapia (2022)		X	X		
Soto y otros (2021)	X	X	X		
Rea (2021)		X	X		
Molina y Orozco (2020)		X	X		
Rodríguez y otros (2020)		X	X		
Porra (2020)		X	X	X	
Amariles y otros (2020)	X		X		
Quevedo-Rojas y Vintimilla-Jara (2020)		X	X		
Castillo (2022)		X	X		

Fuente: Elaboración propia basada en Martínez (2022), Checca (2021), Castañeda y Villegas (2020), Cordoba (2021), Viguri (2021), Diaz y Prieto (2021), Gibau (2022), Escobar, Márceles y otros (2021), Guerra y otros (2021), García (2021), Ortega-Guillén y Cuenca-Tapia (2022), Soto y otros (2021), Rea (2021), Molina y Orozco (2020), Rodríguez y otros (2020), Porra (2020).

Tabla 2 Antecedentes y estudios

En relación con esto, se ha seleccionado a la empresa del sector alimenticio para validar el plan estratégico diseñado por las siguientes razones:

- Genera aproximadamente 1TB de información al día lo que la hace un escenario practico para el desarrollo de un plan estratégico.
- De acuerdo a su diseño estructural en cuanto a su planta física la hace propensa a que surjan vulnerabilidades.
- Tiene en la planta de personal 1.037 empleados lo que la hace aún más propensa a la explotación de vulnerabilidades.

- Es una compañía que busca la mejora continua por lo que posibilita la implementación de un plan estratégico.

2.6. Hipótesis

Los problemas asociados a la seguridad de la información asociada a los datos personales alcanzan a todo tipo de organización, por tal razón es importante que las empresas cuenten con planes estratégicos para la identificación de riesgos y vulnerabilidades en sus sistemas de seguridad de la información. En la actualidad, las empresas de alimentos manejan grandes volúmenes de información que por su variedad e importancia la hacen blanco de posibles ataques por lo que es fundamental que cuenten con este tipo de planificación integrada en su gestión

3. OBJETIVOS

3.1. Objetivo general

Implementar un plan estratégico para la identificación de riesgos y vulnerabilidades en la seguridad de la información de los datos personales de una empresa.

3.2. Objetivos específicos

1. Identificar los lineamientos a tomar en cuenta en la detección de riesgos y vulnerabilidades en la seguridad de la información de los datos personales existentes en la empresa.

2. Analizar los riesgos y vulnerabilidades en seguridad de la información de los datos personales existentes en la empresa.

3. Diseñar un plan que integre estrategias de seguridad que ayuden a la identificación de las amenazas, la valoración de los riesgos, la priorización mediante el grado de riesgos y los planes de acción para la seguridad de la información de los datos personales existentes en la empresa.

4. Validar el plan estratégico con un caso de estudio en un contexto empresarial.

3.3. Marco metodológico

A continuación, se describe la tabla del Marco Metodológico, la cual describe cada uno de los objetivos específicos con sus correspondientes actividades y entregables.

Tabla Marco Metodológico.

Objetivo Especifico	Actividades	Entregables
Identificar los lineamientos a tomar en cuenta en la detección de riesgos y vulnerabilidades en la seguridad de la información de los datos personales existentes en la empresa.	Revisión de literatura, marco conceptual y teórico.	Documento con Revisión de literatura, marco conceptual y teórico.
Analizar los riesgos y vulnerabilidades en seguridad de la información de los datos personales existentes en la empresa.	Análisis y clasificación de vulnerabilidades, Evaluación y clasificación de riegos, elaboración de la matriz de riesgos,	Documento con el análisis de vulnerabilidades detectadas según norma ISO 27001 y modelo COBIT.
Diseñar un plan que integre estrategias de seguridad que ayuden a la identificación de las amenazas, la valoración de los riesgos, la priorización mediante el grado de riesgos y los planes de acción para la seguridad de la información de los datos personales existentes en la empresa.	Establecimiento del contexto, Identificación de activos de información, Identificación de amenazas y vulnerabilidades, Evaluación de riesgos, Selección de controles de prevención, Implementación de controles de prevención.	Plan estratégico para la identificación de vulnerabilidades basado en la norma ISO 27001 y modelo COBIT.

Objetivo Especifico	Actividades	Entregables
Aplicar el modelo en un caso de estudio específico	Aplicación del modelo en un caso de estudio.	Documento con el caso de estudio aplicado.

Tabla 3 Marco metodologico

3.3.1. Enfoque investigativo

El enfoque de investigación es cualitativo, dado que se sustenta en evidencias orientadas hacia la descripción detallada del fenómeno, con la intención de comprenderlo y explicarlo (Sánchez, 2019). Los estudios desarrollados a partir de este enfoque posibilitan la generación de conocimientos científicos, mediante técnicas que permiten comprender las dinámicas internas del fenómeno estudiado para interpretarlo y plantear alternativas de solución. La investigación cualitativa expresa sus objetivos acerca de situaciones complejas que suceden en el escenario donde se desarrolla el estudio, por lo cual, deben ser analizados y descritos en su medio natural. En este tipo de investigaciones se estudia la realidad tal como sucede, intentando sacar sentido del fenómeno. En este orden de ideas, implica la utilización y recogida de información que refiere el tópico de estudio y las particularidades que permiten describirlo e interpretarlo.

3.3.2. Diseño de la investigación

Es un estudio de tipo exploratorio, en tanto se orienta a la comprensión de un fenómeno desconocido. Desde los planteamientos de Cortés e Iglesias (2004), este alcance es apropiado para el estudio de temas poco abordados, como ya se ha dicho, los procesos identificación de riesgos y vulnerabilidades en la seguridad de la información de los datos personales en empresas no han constituido un objeto de estudio recurrente, de ahí que aplicar un estudio exploratorio resulta conveniente al caso en cuestión, además, porque es más flexible en su metodología (Salinas y Cárdenas, 2009).

Dado que la investigación se lleva a cabo en una empresa del sector alimenticio, esta es una investigación de campo, es decir, se realiza en el mismo lugar y en el tiempo donde ocurre el fenómeno para obtener la información referente al tema de forma ordenada (Arias y Covinos, 2021). De otra parte, teniendo en cuenta la finalidad de la exploración, la presente es una investigación aplicada, en tanto que se encarga de resolver problemas prácticos y está basada en los descubrimientos y soluciones planteadas en el objetivo general del estudio.

Tabla Diseño metodológico

Diseño metodológico		
Objetivo general Implementar un plan estratégico para la identificación de riesgos y vulnerabilidades en la seguridad de la información de los datos personales de una empresa.	**Enfoque** Investigación cualitativa, sustentada en evidencias que posibilitan la comprensión de un fenómeno	**Tipo de investigación** Es un estudio exploratorio, que dadas las condiciones particulares en las que se desarrolla, hace uso de técnicas e instrumentos de la investigación de campo y aplicada.

Objetivos específicos	**Instrumentos**
Identificar los lineamientos a tomar en cuenta en la identificación de riesgos y vulnerabilidades en la seguridad de la información de los datos personales existentes en la empresa.	Encuesta
Analizar los riesgos y vulnerabilidades en seguridad de la información de los datos personales existentes en la empresa.	Revisión documental
Diseñar un plan que integre estrategias de seguridad que ayuden a la identificación de las amenazas, la valoración de los riesgos, la priorización mediante el grado de riesgos y los planes de acción para la seguridad de la información de los datos personales existentes en la empresa.	Elaboración de plan
Validar el plan estratégico con un caso de estudio en un contexto empresarial.	Análisis de procesos

Tabla 4 Objetivos del proyecto Fuente: Elaboración propia

3.3.3. Técnicas e instrumentos

- **El análisis documental:** Esta técnica posibilitará obtener información acerca de los riesgos y vulnerabilidades en seguridad de la información de los datos personales existentes en la empresa. La técnica que se va a emplear es la revisión de la base de datos de los empleados, la cual posibilitará analizar riesgos y vulnerabilidades para una posterior presentación de hallazgos, resultados y conclusiones. Según Niño (2011) esta técnica es apropiada para extraer de un documento los aspectos de información de mayor relevancia, para ser ordenados, clasificados y analizados desde la visión de lo que persigue el investigador.

- **Encuesta:** Esta técnica nos permite la obtención de información a través de métodos de indagación empírica teniendo una muestra y una población definida. Según (Hernán Feria Avila, 2020) este método permite adoptar una posición teórica, en relación con el cuestionario, frente a ambos métodos. También se defiende a la encuesta, esencialmente, como alternativo a la entrevista. Se realiza, además, una propuesta de nomenclatura para los tipos de preguntas a utilizar en ambos, así como sendas nuevas clasificaciones.

- **Ficha de comprobación:** Esta técnica está orientada a la verificación de los componentes de seguridad implicados en el diseño de un plan para la identificación de riesgos y vulnerabilidades en existentes para la seguridad de la información de los datos personales existentes en la empresa. El instrumento será una lista de chequeo que permitirá realizar una comprobación sistemática de los estándares de seguridad tenidos en cuenta en el plan estratégico de seguridad. La relevancia de este instrumento radica en que hace posible la reducción errores en la propuesta planteada, asegurando la prevención de pérdida de información en la empresa, además, contribuye con el proceso de evaluación y registro del progreso del objetivo planteado, permitiendo que se identifiquen a tiempo las debilidades o dificultades del proceso para solucionarlas.

- **Análisis de procesos**. Esta técnica permitirá validar el plan estratégico con un caso de estudio en un contexto empresarial, mediante la revisión íntegra del funcionamiento de dicho plan y la verificación de las metas establecidas. El instrumento será el análisis de los procesos empresariales en el componente de gestión de riesgos de seguridad de la información de los empleados, tras implementar la propuesta diseñada a partir de esta investigación, lo cual ayudará en la identificación de fortalezas y debilidades de los procesos para realizar los ajustes pertinentes.

3.3.4. Población y muestra

Realizan un levantamiento de la información por medio de encuestas a una la población involucrada en los procesos, para este caso N = 114 colaboradores en las siguientes áreas: Financiera, TI, DHO, Tesorería, Gestión de activos y Consultoría

3.3.5. Procedimientos

El estudio sistematizado de los datos recogidos posibilitará el análisis del fenómeno investigado, y durante este proceso se identificarán aspectos relevantes acerca de los riesgos y vulnerabilidad en la seguridad de la información del personal de la empresa, que pueden surgir en el curso de la investigación y que pueden dar una explicación más amplia de la importancia teórica o práctica de elementos. Dicho proceso se llevará a cabo teniendo en cuenta los aportes de Rubin y Rubin (1995), para estos autores recomendable aplicar los siguientes pasos:

- **Obtener la información:** En este paso se aplicarán los instrumentos diseñados, la información que se recolecte a través de estos instrumentos constituye el insumo necesario para continuar el siguiente paso.

- **Transcribir la información:** La información recolectada se sistematizará para posibilitar el posterior análisis. Para este paso se empleará el programa Excel que permite ingresar la información obtenida mediante la aplicación de los instrumentos, facilitando su análisis.

- **Ordenar la información:** Toda la información obtenida se ordenará en Excel, gracias a que este programa contiene unas herramientas apropiadas para tal fin, como el sistema de barras y los gráficos representativos de los datos, ya que a partir de éstos se puede interpretar la información obtenida.

- **Interpretar la información:** Ya ordenada la información, se procederá a revisarla para ser interpretada y poder plantear el plan estratégico, o nutrirlo con los datos aportados por los informantes.

- **Diseñar el plan estratégico:** Lo que se hará en este paso será emplear la información obtenida, sistematizada, organizada e interpretada, y relacionarla con los fundamentos teóricos abordados, para elaborar un plan estratégico para la identificación de riesgos y vulnerabilidades en la seguridad de la información de los datos personales de una empresa.

- **Implementar el plan estratégico:** Se aplicará una prueba piloto del plan estratégico para medir su alcance.

- **Evaluar el plan estratégico:** Se aplicará una rúbrica de avaluación del plan estratégico para determinar si la propuesta es viable para ser adoptada de manera permanente por la empresa para prevenir riesgos y vulnerabilidades en el tratamiento de la información en la empresa.

- **Establecer las conclusiones, recomendaciones y prospectivas del estudio:** El último paso será determinar las conclusiones del estudio, plantear unas recomendaciones y prescribir las prospectivas del mismo.

3.4. DEFINICIÓN DEL ALCANCE

Esta investigación permitirá determinar la validez de la implementación de un plan estratégico para la identificación de riesgos y vulnerabilidades en la seguridad de la información de los datos personales de una empresa.

4. MARCO TEÓRICO – CONCEPTUAL

4.1. Plan estratégico

De acuerdo a lo planteado por el autor Euncet (Euncet, 2022). Un plan estratégico de seguridad de la información es un enfoque integral que establece la dirección y las acciones necesarias para proteger los activos digitales de una organización. Incluye la identificación de riesgos, la implementación de medidas técnicas, legales y organizativas, y la promoción de una cultura de seguridad. Este plan ayuda a garantizar la confidencialidad, integridad y disponibilidad de la información, al tiempo que se adapta a las cambiantes condiciones del entorno y se mantiene alineado con los objetivos empresariales

4.2. Norma ISO 27001

Según el autor (Advisera, 2023), la norma ISO 27001 es un estándar internacional para la gestión de la seguridad de la información. Y su principal objetivo es mantener la confidencialidad e integridad de la información en una organización. La implementación de la norma ISO 27001 implica la identificación y gestión de riesgos y también la aplicación de controles de seguridad adecuados. Estos controles pueden incluir políticas, procedimientos y soluciones técnicas. La certificación ISO 27001 demuestra el compromiso de una organización con la seguridad de la información. Esta Genera confianza en clientes y socios comerciales (DNV, 2023).

4.3. Modelo de madurez Cobit

De acuerdo al autor (ISACA, 2012), el modelo de madurez COBIT es un marco que permite a las organizaciones evaluar y mejorar la gestión y el control de sus procesos de TI, alineando los objetivos del negocio con los recursos tecnológicos disponibles. Este proporciona un enfoque estructurado y basado en las mejores prácticas para garantizar mayor eficiencia, la transparencia y la seguridad de los sistemas de información, impulsando el éxito empresarial a través de la optimización de los procesos de TI.

4.4. Seguridad de la información

En relación con la seguridad de la información, la misma es entendida por Vega (2021, p. 9) La seguridad de la información se refiere a los métodos, prácticas y procedimientos que se implementan con el fin de resguardar la información y los sistemas de acceso, uso, divulgación, interrupción, alteración o destrucción no autorizados. En otras palabras, su objetivo es salvaguardar los datos y los recursos tecnológicos de aquellos que intentan utilizarlos de manera indebida.

La seguridad de la información es referida por parte de Castillo y Zavala (2019) como la disponibilidad de la información, su confidencialidad e integridad, así como los datos relevantes para la organización que pueden ser digitales o en papel

4.5. Activos de información

La información es un medio intangible menciona Martín (2021) La dedicación de recursos a activos intangibles implica una inversión que brinda beneficios a largo plazo, lo que contribuye al desarrollo de la economía basada en el conocimiento. Los activos intangibles representan un valor económico significativo para las empresas, especialmente en la era actual centrada en los datos. La información adquiere un gran valor, ya que impulsa la productividad, aumenta las ventas y reduce los costos al acelerar la utilización de dicha información en los procesos de producción. Así mismo, se considera que los activos engloban cualquier elemento que contenga algún tipo de información, y es necesario clasificarlos según su importancia, función o nivel de confidencialidad, con el propósito de salvaguardar dicha información. (ISO, 2017).

4.6. Gestión de riesgos de seguridad de la información

En relación con el tópico, Areitio (2008, p. 7) Se describe como el proceso de gestión de riesgos que consiste en identificar y dar prioridad a las posibles amenazas asociadas al desarrollo de un producto, sistema u organización. La gestión de riesgos desempeña un papel fundamental en la gestión de la seguridad, y se define como el proceso encargado de identificar y evaluar la probabilidad de que ocurran situaciones de riesgo, estableciendo un nivel aceptable de riesgo para la organización, teniendo en cuenta el posible impacto de un incidente no deseado. Por otro lado, Arévalo, Cedillo y Moscoso (2017) Se describe que la gestión de riesgos se define como una disciplina enfocada en abordar los riesgos no especulativos, los cuales son aquellos riesgos en los que la organización solo puede sufrir una pérdida.

4.7. Riesgos

En líneas generales, Romero y otros (2018, p. 28) explican que el riesgo se refiere a la posibilidad de que ocurra algo negativo que cause daño a los recursos tangibles o intangibles, lo que a su vez impide el desarrollo adecuado de la labor profesional. Además, se señala que el riesgo debe entenderse como la probabilidad de que una amenaza específica aproveche una vulnerabilidad determinada.

Por su parte, Ortega-Guillén y Cuenca-Tapia (2022, p. 900) mencionan que al hablar de un efecto de riesgo se está haciendo referencia a la incertidumbre o duda que puede surgir en relación a los objetivos. Además, se destaca que existe una probabilidad de que ocurra un impacto que desvíe el resultado esperado durante el análisis, el cual puede ser tanto positivo como negativo, dependiendo de la situación. Por último, se concluye que el riesgo en general, o en parte, depende de la información relevante o de la comprensión de un nuevo evento.

4.8. Vulnerabilidades

Por un lado, Romero y otros (2018, p. 28) definen a las vulnerabilidades como las deficiencias en los sistemas de seguridad o en las herramientas utilizadas por el usuario para llevar a cabo actividades, las cuales podrían permitir que una amenaza tenga éxito al generar un problema.

Mientras que por parte de Ortega-Guillén y Cuenca-Tapia (2022, p. 901), explican que Las carencias en los sistemas de seguridad o en las herramientas empleadas por el usuario durante sus actividades pueden facilitar que una amenaza logre generar un problema.

Así mismo, Areitio (2008, p. 23) argumenta que una vulnerabilidad puede ser vista como la posibilidad de que una amenaza se materialice y afecte un activo. Las vulnerabilidades relacionadas con los activos abarcan debilidades en aspectos físicos de la organización, los procedimientos, el personal, la gestión, la administración, los equipos, el software o la información.

4.9. Identificación de vulnerabilidades

Para identificar vulnerabilidades, se requiere llevar a cabo un proceso que involucra una búsqueda exhaustiva para identificar los riesgos o sus fuentes. Luego, se realiza un reconocimiento detallado que permite comprender las causas de los eventos que podrían estar ocurriendo. Por último, se realiza una descripción de los riesgos, que puede incluir datos históricos, análisis y opiniones de expertos en el tema. (Ortega-Guillén y Cuenca-Tapia, 2022, p. 900).

Por su parte, Areitio (2008, p. 23) explica que la identificación de vulnerabilidades implica examinar las debilidades del sistema que pueden ser aprovechadas por las amenazas identificadas. Este análisis debe considerar el entorno y las medidas de protección existentes. Las vulnerabilidades se clasifican según su naturaleza (estáticas o dinámicas), el tipo de acceso (local o remoto) su impacto (peligrosas o inocuas) y el nivel donde se localizan (físico, enlace de datos, red, transporte o aplicación).

4.10. Datos personales

A este respecto, Castillo y Zavala (2019, p. 222) explican que los datos personales abarcan toda la información que se puede vincular a una persona y que permite identificarla. Estos datos pueden incluir la edad, dirección, número de teléfono, correo electrónico, historial académico o profesional, patrimonio, estado de salud, creencias religiosas, afiliaciones políticas o filosóficas, preferencias sexuales, entre otros. Asimismo, lo definen Soto y Ducuara (2018, p. 13) para quienes es toda información relacionada que identifica o hace identificable a una persona.

4.11. Análisis de riesgos

Mediante el análisis de riesgos, se pueden detectar y evaluar las posibles fuentes de riesgo a las que una organización se enfrenta. Este proceso brinda información valiosa que permite a la dirección implementar controles adecuados con el fin de reducir al mínimo los efectos de dichos riesgos en los diferentes aspectos que se analizan.

4.12. Identificación de riesgos

En esta etapa, se reconocen los elementos que representan una amenaza para la organización. existen múltiples métodos para identificar riesgos, en este análisis se utilizará el análisis de escenarios.

4.13. Establecimiento de controles existentes

Identificar las fuentes de riesgo que impactan a la organización, se realizará una evaluación para determinar qué riesgos están siendo gestionados por cada una de las áreas de TI implicadas. Esta evaluación permitirá establecer las medidas y acciones necesarias para abordar adecuadamente cada uno de estos riesgos.

4.14. Evaluación de riesgos

Después de identificar los riesgos, el siguiente paso es analizarlos para determinar su impacto y considerar posibles soluciones alternativas.

4.15. Clasificación de los riesgos

Una vez que los riesgos han sido identificados, se lleva a cabo una clasificación utilizando una escala que incluye los siguientes niveles:

- **Nivel de riesgo alto:** Riesgo que afecta la continuidad del negocio.
- **Nivel de riesgo medio**: Riesgos que afectan las labores diarias en la compañía, pero no generan pérdidas mayores, se requiere acción para reto tomar con las labores.
- **Nivel de riesgo bajo**: genera perdida mínima y no representa una amenaza real.

4.16. Elaboración de la matriz de riesgos

Posterior a la clasificación, se realiza un matriz de comparación con activos de la compañía según las escalas definidas en la clasificación de riesgos presentes, para obtener una información precisa sobre cuáles son los activos que puedan afectar o no la integridad de la compañía según su resultado.

4.17. Lineamientos de seguridad para el desarrollo del plan

En este plan estratégico, se proponen dos estándares de seguridad de la información para fortalecer la protección de los datos personales en una empresa: ISO 27001 (Seguridad de la Información), Modelo de Seguridad y Privacidad de la Información (MSPI) y Modelo de Madurez de COBIT.

ISO 27001: Se aplicará un sistema de gestión de seguridad de la información (SGSI) basado en los requisitos de la norma ISO 27001. Esto incluirá un análisis de brechas para identificar las deficiencias existentes, el desarrollo de políticas y procedimientos de seguridad de la información y la implementación de controles recomendados por la norma.

Modelo de Madurez de COBIT: Se empleará el modelo de madurez de COBIT para evaluar la madurez de los procesos de seguridad de la información y establecer objetivos de mejora. Se implementarán mejoras basadas en la evaluación, como actualización de políticas, implementación de controles adicionales y capacitación del personal.

- **ISO 27001:**

a. Realiza un análisis de brechas: Evalúa el estado actual de la seguridad de la información en la empresa esto se compara con los requisitos de la norma ISO 27001 para identificar las brechas existentes.

b. Desarrolla políticas y procedimientos: Diseña políticas y procedimientos de seguridad de la información que cumplan con los requisitos de la norma ISO 27001. Estos deben abordar aspectos como el control de acceso, la gestión de riesgos, la protección de los datos personales, etc.

c. Implementa controles de seguridad: Aplica los controles de seguridad recomendados por la ISO 27001 para proteger los datos personales y minimizar los riesgos identificados. Estos controles pueden incluir la clasificación de la información, la gestión de contraseñas, la protección contra malware, entre otros.

- **Modelo de madurez de COBIT:**

a. Evalúa la madurez de los procesos: Se utiliza el modelo de madurez de COBIT para evaluar la madurez de los procesos de seguridad de la información en la empresa. Esto te permite identificar las áreas que requieren mejoras.

b. Establece objetivos de mejora: Basado en la evaluación de madurez, establece objetivos claros de mejora para cada uno de los procesos de seguridad de la información.

c. Implementa las mejoras: Diseña e implementa medidas y controles para mejorar la madurez de los procesos identificados. Esto puede incluir la actualización de políticas, la implementación de controles adicionales, la capacitación del personal

5. DESARROLLO DEL PROYECTO – CASO DE ESTUDIO

Fuentes de información:

La información recopilada para la definición de vulnerabilidades y riesgos en la seguridad de la información de los datos personales en la empresa proviene de dos fuentes principales:

Fuente del autor: Los autores han obtenido información relevante para la identificación de riesgos y vulnerabilidades en la seguridad de la información de los datos personales en la empresa a través de su formación como empleados y su experiencia laboral en el campo. Al trabajar directamente en el entorno donde ocurren los eventos relacionados con la seguridad de la información, los autores han podido adquirir un conocimiento práctico y valioso que ha sido fundamental para el desarrollo del plan estratégico.

Equipos de seguridad de la compañía: La información adicional fue proporcionada por los equipos de seguridad de la compañía, quienes compartieron sus conocimientos y experiencias en la identificación y mitigación de riesgos y vulnerabilidades en la seguridad de la información.

Dado que la distribución de documentación de la compañía es prohibida sin su permiso, no se han anexado documentos específicos en la tesis. Sin embargo, la empresa ha brindado todo el material necesario para la ejecución del proyecto, garantizando la confidencialidad de la propiedad intelectual de la compañía. Por lo tanto, aunque no se incluyen documentos específicos, la información proporcionada por la empresa ha sido fundamental para el desarrollo de este plan estratégico.

En este apartado, es importante destacar el compromiso del autor y la empresa en proteger la confidencialidad de la información y respetar las políticas de propiedad intelectual de la compañía.

Es importante destacar que para el correcto desarrollo de este trabajo se debe de estar alineado con la proyección corporativa a nivel de TI es por esto que se realiza el desarrollo basado en la norma ISO 27001 y modelo de madurez COBIT. Entendiendo que un ambiente practico real es necesario seguir los lineamientos establecidos por la compañía.

5.1. Encuesta

SE ANEXA EL DOCUMENTO "Encuesta de identificación y clasificación de riesgos (respuestas)"

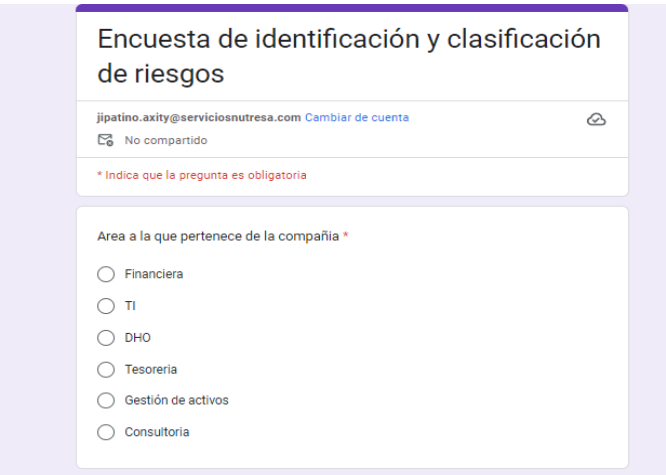

Ilustración 2 Encuesta

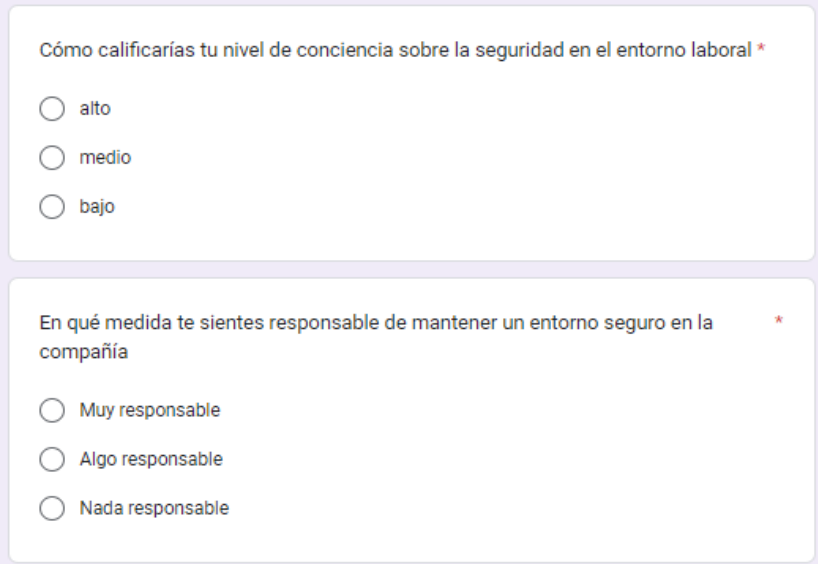

Ilustración 3Encuesta preguntas

Se desarrolló una encuesta a 83 colaboradores dentro de la compañía para las siguientes áreas: Financiera, TI, DHO, Tesorería, Gestión de activos y Consultoría, donde se obtuvo información sobre las falencias en términos de seguridad de la información. Esta nos permitió desarrollar una matriz DOFA la cual nos muestra información sobre puntos negativos y positivos de esta, en cuanto a los positivos se obtienen las fortalezas y oportunidades, ahora en cuanto a lo negativo se obtuvieron debilidades y amenazas.

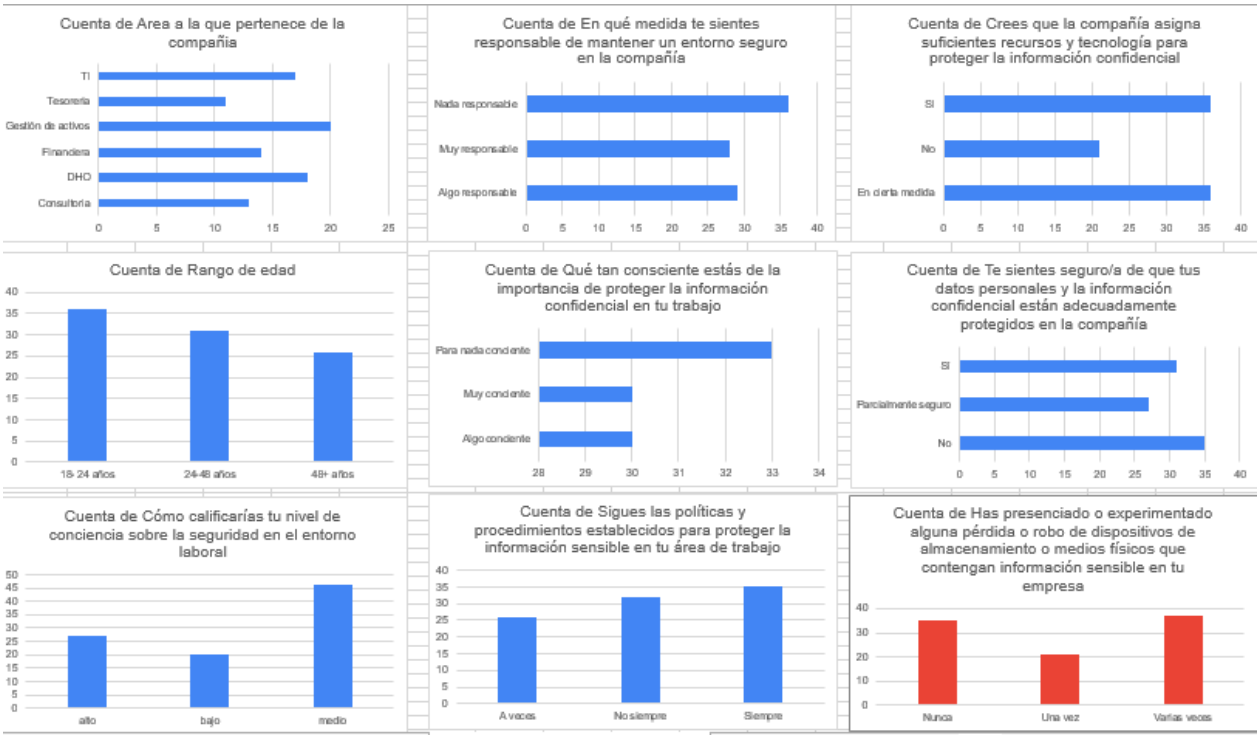

Ilustración 4visualización grafica de la encuesta

Con el desarrollo de esta encuesta se obtuvieron los siguientes resultados:

- La encuesta se realizó en al menos 6 de las áreas principales de la compañía. Información la cual nos va a permitir realizar un análisis más a profundidad.
- De ese análisis podemos observar que al menos 28 personas conocen los procedimientos para identificar correos maliciosos por lo que se define que al menos 30,11% de la población encuestada tiene conocimientos, mientras que el otro 69,89% solamente decide escalar o simplemente no realizan nada. Lo que representa un riesgo en cuanto a temas de ingeniería social, phising o spam.
- Se observa que el 69,99% dice tener capacitación referente a seguridad de la información, mientras que de ese mismo porcentaje un 33,33% dice tener capacitación, pero no tiene los conceptos definidos. Lo que implica que con el otro 30,11% de la población se suma al aumento de posible explotación de vulnerabilidades debido a que no tienen los conceptos definidos o simplemente no entienden de seguridad.

- Se define que al menos un 62,37% de la población no sigue las políticas debido a que las desconoce o las conoce, pero no las sigue, lo que resalta una gran oportunidad para el planteamiento de un plan de capación del empleado.
- En cuanto a la información obtenida podemos observar que los empleados si son conscientes en cuanto a las actividades que realizan dentro de la compañía, pero debido a factores como el desconocimiento aumentan la probabilidad de que sucedan las vulnerabilidades.
- Es importante destacar que las encuestas desarrolladas en sus respuestas fueron muy parejas esto se pudo analizar de acuerdo a la población tomada de la cual la mayoría son jóvenes nuevos en la compañía, ya que por otro lado en el resto de la población se observó una variación mayor en las respuestas.

En conclusión, podemos notar que es de suma importancia tener establecido un plan estratégico. Para la empresa es de Mucha importancia que los empleados cuenten con información, capacitación, políticas y la preparación del entorno donde desarrollan sus actividades para minimizar a largo plazo los efectos negativos de la explotación de vulnerabilidades en factores humanos.

5.2. Análisis de campo

Mediante este análisis se obtuvo la información relacionada a volumen de información e históricos de casos de riesgos y vulnerabilidades.

SE ANEXAN LOS DOCUMENTOS "Informe de crecimiento de información" Y "Vulnerabilidades en plataformas virtuales"

Fecha	Almacenamiento utilizado en Gmail	Unit	Almacenamiento utilizado en Drive	Unit	Crecimiento dia
6 dic 2022, 3:00:00 GMT-5	225.85	TB	93.51	TB	0
7 dic 2022, 3:00:00 GMT-5	226.02	TB	93.75	TB	0.41
8 dic 2022, 3:00:00 GMT-5	226.09	TB	93.81	TB	0.12
9 dic 2022, 3:00:00 GMT-5	226.31	TB	93.89	TB	0.31
10 dic 2022, 3:00:00 GMT-5	226.28	TB	93.89	TB	-0.03
11 dic 2022, 3:00:00 GMT-5	226.20	TB	93.88	TB	-0.09
12 dic 2022, 3:00:00 GMT-5	226.46	TB	94.08	TB	0.46
13 dic 2022, 3:00:00 GMT-5	226.59	TB	94.24	TB	0.28
14 dic 2022, 3:00:00 GMT-5	226.85	TB	94.40	TB	0.42
15 dic 2022, 3:00:00 GMT-5	227.02	TB	94.54	TB	0.31
16 dic 2022, 3:00:00 GMT-5	227.21	TB	94.70	TB	0.36
17 dic 2022, 3:00:00 GMT-5	227.20	TB	94.70	TB	-0.02
18 dic 2022, 3:00:00 GMT-5	227.13	TB	94.67	TB	-0.09
19 dic 2022, 3:00:00 GMT-5	227.34	TB	94.85	TB	0.38
20 dic 2022, 3:00:00 GMT-5	227.63	TB	95.02	TB	0.47
21 dic 2022, 3:00:00 GMT-5	227.91	TB	95.29	TB	0.55
22 dic 2022, 3:00:00 GMT-5	228.14	TB	95.51	TB	0.45
23 dic 2022, 3:00:00 GMT-5	228.37	TB	95.54	TB	0.26
24 dic 2022, 3:00:00 GMT-5	228.41	TB	95.50	TB	0.00

Inicio del semestre	Fin del semestre	Total Crecimiento semestral
319.36	360.44	12,85%

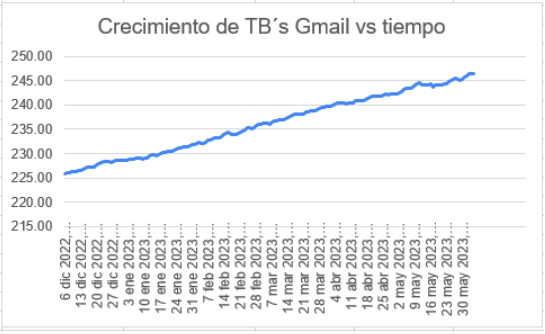

Ilustración 5Informe de crecimiento de información

En el anexo "**Informe de crecimiento de información"** se obtienen resultados en cifras tangibles que nos ayudan a tener un contexto más amplio sobre el crecimiento en volumen de información

en un periodo de 6 meses la cual da como resultado un 12.85% más con respecto al inicio del periodo, lo cual nos deja claro la importancia de un plan estratégico que le brinde un enfoque preventivo a la compañía y le permita establecer controles para los diversos activos que se suman a la totalidad de la información.

Adicional se determina que:

- En el primer semestre del año 2023 la compañía paso de tener 319.36 TB a 364 TB lo cual significó un aumento significativo del 12.85% lo que corresponde a 45 TB.
- Según la tendencia de crecimiento para el segundo periodo la compañía habrá crecido al menos 90 TB en información. Por lo cual se requiere un enfoque preventivo, estableciendo medidas y procesos que ayuden al control de la información. Esto debido a que un incidente puede resultar en la pérdida parcial o definitiva de esta.
- De acuerdo a la encuesta y al crecimiento exponencial en términos de información se plantea la pregunta: ¿realmente se tiene un plan de contingencia definido para evitar la pérdida de información ante los diversos tipos de vulnerabilidades? Para la solución a esta pregunta se hace necesario el desarrollo de un plan estratégico que nos permita tener un control sobre todas aquellas situaciones inseguras con mayor probabilidad de que sucedan.

En el anexo "**Vulnerabilidades en plataformas virtuales"** se evidencia un histórico de vulnerabilidades en plataformas virtuales de la compañía clasificadas de acuerdo a Phising, Spam y vulneración de cuentas de correo, lo cual según el análisis se muestra que la tendencia de este tipo de ataques es creciente y se observan oportunidades de mejora al momento de la implementación del plan estratégico.

Plataforma	# eventos maliciosos	% Phishing	% Spam	% Vulneración de cuenta
Workspace	21728	47.20	30.60	22.20
Workspace	25225	68.5	20.10	11.40
Workspace	19012	32.7	52.30	15.00
Workspace	17788	24.8	62.10	13.10
Workspace	19595	77.3	14.20	8.50
Workspace	14795	43.9	41.10	15.00
Workspace	20080	31.1	50.30	18.60
Workspace	19407	9.8	77.80	12.40
Workspace	21168	46.2	36.50	17.30
Workspace	22775	35.7	49.80	14.50
Workspace	17834	57.3	23.20	19.50
Workspace	14896	40.4	45.60	14.00
Workspace	16310	18.9	71.20	9.90
Workspace	20913	72.7	9.80	17.50
Workspace	23751	37.8	46.30	15.90
Workspace	23440	29.2	25.10	45.70
Workspace	25950	8.3	81.70	10.00
Workspace	18728	52.5	18.30	29.20
Workspace	11168	37.2	34.90	27.90
Workspace	10066	64.1	13.20	22.70
Workspace	24056	42.6	33.40	24.00

Clasificación de los riesgos	
Nivel de riesgo	Descripción
ALTO	Frecuenta del evento Alta
MODERADO	Frecuenta del evento Media
BAJO	Frecuenta del evento Baja

*Información extraida de la Google Admin Reports

Ilustración 6 Vulnerabilidades en plataformas virtuales

De acuerdo a un análisis se evidencia que:

- Entre los días 26 al 31 de cada mes se nota un aumento considerable en los casos detectados para los diferentes tipos de situaciones. Esto se debe a que en el rango de fechas la compañía presenta etapas de cierre de nómina por tanto se eleva el consumo de los servicios de comunicación masiva.

- En el primer semestre de 2023 la vulneración de cuentas de correo se mantuvo en las cifras más bajas con una probabilidad de que suceda muy inferior con respeto a los otros tipos de ataques.
- De acuerdo a la revisión de frecuencias se determina que el SPAM es el factor principal al cual se enfrenta la compañía del cual se evidencia que de cada 10 empleados al menos un 40% lo cual seria 4 empleados sufren de SPAM.
- Para el análisis de phising se obtienen datos redondos como lo es el SPAM debido a que al existir un SPAM permitido este también aumenta la probabilidad de que un caso de phising suceda. Para este caso obtiene un promedio de 39,89% de probabilidad.
- Al definir el phising y el SPAM como factores principales se evidencia que no se tiene una postura preventiva frente a estos eventos tales como pueda ser el control, la capacitación del empleado o los procesos que se llevan internamente para bloquear esto.
- Sumando a este análisis la encuesta, podemos evidenciar que el Core fundamental para reforzar estos aspectos de seguridad proviene desde la formación del empleado.

5.3. Matriz DOFA

A continuación, se describe la Matriz DOFA, la cual es basada en la encuesta realizada a los empleados de la compañía. Esta permitió identificar Debilidades, Oportunidades, Fortalezas y Amenazas. Aspectos que son importantes para el establecimiento de políticas y generación de un plan del desarrollo del empleado a rasgos de seguridad.

De acuerdo a los resultados de las matriz DOFA podremos determinar lo siguiente:

Basado en el planteamiento de la matriz DOFA se determina que un plan de capacitación a largo plazo puede resultar beneficioso debido a que puede reducir considerablemente la explotación de vulnerabilidades en el futuro.

Se hace destacable la elaboración de un plan de mitigación que permita involucrar a todos los diferentes tipos de activos que conforman la compañía tales como personal, físicos y de entorno para brindar un enfoque más general que permita a la compañía definir exitosamente procesos en términos de prevención.

Con el planteamiento y ejecución de las actividades para las oportunidades detectadas en la matriz DOFA, se puede evidenciar que las amenazas disminuirán drásticamente y a largo plazo podrían desaparecer.

5.4. Recursos y activos

Personal: Para la elaboración del Trabajo se cuenta con los siguientes.

Recursos Profesionales:

- Javier Ivan Patiño Castrillon, Soporte BI.
- Josed Estid Bedoya Velasquez, Administrador de plataforma Google Workspace.

Recursos Físicos: Los recursos físicos con los que se cuenta para este proyecto son proporcionados por Servicios Nutresa Medellín.

Recursos Tecnológicos:

- Sistema Operativo: Windows 10

Características físicas:

- Memoria RAM: 16GB
- Disco Duro SSD de 500GB
- Procesador: Intel(R) Core(TM) i5-8265U CPU @ 1.60GHz 1.80 GHz
- Router: CISCO inalámbrica

Características físicas:

- Memoria RAM: 16GB
- Disco Duro SSD de 500GB
- Procesador: AMD Ryzen™ 5 5500U
- Router: CISCO inalámbrica

Software y herramientas digitales:

- Xtract universal Licenciado
- Google Admin
- AWS
- SAP
- Antivirus
- VPN

PERSONAL:

Gerencia	Nombre	Represéntate
Tecnología de información (TIC)	Javier Ivan Patino Castrillon	Servicios Nutresa Medellin - Axity
Tecnología de información (TIC)	Josed Estid Bedoya Velasquez	Servicios Nutresa Medellín - Axity
Fuente obtenida de Autores		

Tabla 5 Personal del proyecto

INSTALACIÓNES:

Sede	Nombre	Propietario del activo
Servicios Nutresa, Medellín , Guayabal, Compañía de Galletas Noel S.A.S	Servicios Nutresa Medellín	Servicios Nutresa
Fuente obtenida de Autores		

Tabla 6 Sedes fisicas

EQUIPOS:

Tipo	Nombre	Proceso
LAPTOP	HP 245 G8 ryzen 5 5500u	TIC
LAPTOP	HP 240 G7 Intel(R) Core(TM) i5-8265U CPU @ 1.60GHz 1.80 GHz	TIC
Fuente obtenida de Autores		

Tabla 7 Equipos

SOFTWARE:

Área	Nombre	Proceso
Cloud	AWS – Amazon Web Services	TIC
Áreas Varias	SAP Business	Todas las áreas
TIC	GOOGLE ADMIN	TIC
Áreas Varias	Herramientas ofimáticas de Google	Todas las Áreas
Fuente obtenida de Autores		

Tabla 8 Software

5.5. Análisis de riesgos y vulnerabilidades en la seguridad de la información de los datos personales existentes en la empresa.

5.5.1. Identificación de vulnerabilidades físicas

Dentro de las instalaciones físicas no se presentan en su mayoría oficinas o divisiones por lo tanto los espacios son compartidos facilitando el acceso a terceros no autorizados a sus equipos personales.

Además de que los comportamientos no seguros pueden facilitar el desarrollo de esos accesos no autorizados la información.

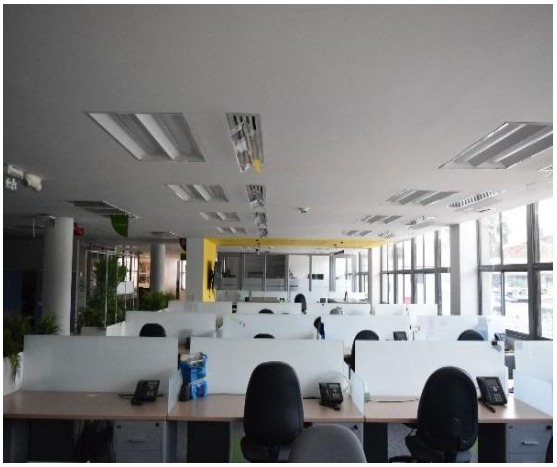

Ilustración 7 Sede Oficina 1

Fuente: Autores

Ilustración 8 oficina 2

Fuente: Autores.

Ilustración 9 Sede Oficina 2

Fuente: Autores.

Con la identificación de los espacios podemos esclarecer que:

Si un colaborador deja su equipo desbloqueado en su puesto se da un aumento del riesgo en el que posiblemente un agente externo o un ataque mal intencionado suceda. Esto debido a que pueden suceder los siguientes eventos:

- Inyección o ejecución de virus mediante uso de dispositivos extraíbles (Discos duros, USB u otro tipo de dispositivos extraíbles).
- Daño físico del equipo por diversos factores en el ambiente los cuales pueden ocasionar perdida en la información de compañía.
- Divulgación de datos confidenciales de la compañía.
- Acceso no permitido a equipos de cómputo, uso de recursos tales como Discos duros, USB o elementos que contengan información.
- Manipulación del hardware del equipo para implementación de Keylogger con el motivo de obtener accesos a aplicativos privados de la compañía.
- Empleados descontentos podrían causar daños a equipo de otros robando, destruyendo o manipulando información confidencial.
- Suplantación de identidad causado por retirarse del puesto de trabajo sin bloquear el equipo.
- Violación de la normativa de la compañía. Dejar un equipo desatendido no está permitido.

5.5.2. Identificación de vulnerabilidades en el personal

En la compañía, existen diversos factores que el personal puede desencadenar y que representan riesgos para la seguridad de la empresa.

- **Contraseñas débiles**: Las contraseñas como "mes" o "nombre" son de las más comunes en la compañía. Lo que favorece el robo de cuentas.
- **Reutilización de contraseñas**: Muchas personas reutilizan contraseñas en múltiples cuentas. Esto significa que, si una cuenta es comprometida, todas las demás cuentas con la misma contraseña también estarán en riesgo.
- **Descuido al hacer clic en enlaces o descargar archivos adjuntos**: Debido a la poca formación que tienen en aspectos de trato de correos e identificación de tipos de ataque tienen a descargar o hacer clic en correos maliciosos.
- **Acceso físico no autorizado**: Si los dispositivos y las áreas de trabajo no están adecuadamente protegidos por el empleado, cualquiera podría tener acceso físico a los equipos y robar información confidencial o instalar software malicioso.
- **Uso indebido de privilegios de administrador**: Si los usuarios tienen privilegios de administrador en sus cuentas y no se limita su acceso, pueden realizar cambios no autorizados en los sistemas o instalar software malicioso sin restricción alguna.
- **Falta de conciencia de seguridad**: La falta de educación y conciencia sobre las mejores prácticas de seguridad informática lleva a comportamientos no seguros, como compartir contraseñas, cuentas o hacer clic en enlaces sospechosos.
- **Ingeniería social**: desconocimiento en términos técnicos o de seguridad lo que implica el engaño mediante llamadas telefónicas, correos electrónicos falsificados o mensajes de texto para obtener información confidencial o acceso a sistemas.
- **Falta de formación**: el no contar con recursos o formación al empleado en el tema de seguridad de la información puede causar que el empleado viole las políticas de seguridad al desconocerlas o no conocer los procedimientos.
- **Falta de preparación ante eventos de violación de seguridad:** La falta de preparación hace que sigan procedimientos inadecuados y aumenten la propagaron de la vulnerabilidad.

5.5.3. Identificación de vulnerabilidades en los activos

En términos de identificación de vulnerabilidades tenemos definido que:

- Fallo en los equipos (Servidores, equipos, sistemas de seguridad) debido a cortes de energía y fallos en los UPS (Sistema de alimentación ininterrumpida). Causando daños y posibilitando la perdida de información.
- Los activos físicos de la empresa, como servidores, computadoras portátiles, dispositivos móviles o discos duros externos, pueden ser robados, lo que puede resultar en la pérdida de información.
- Si los activos físicos no están protegidos adecuadamente, como mediante cerraduras o sistemas de acceso electrónico, podrían ser tomados por personas no autorizadas, lo que podría llevar a la manipulación o divulgación de información sensible.

- Los activos físicos pueden sufrir daños accidentales o intencionales, como caídas, derrames de líquidos, incendios o vandalismo. Estos eventos pueden causar la pérdida permanente de datos o dejar los activos inutilizables. Por ello es necesario un sistema de respaldo en la nube.
- Los competidores o actores maliciosos pueden intentar obtener acceso físico a los activos de la empresa para robar información confidencial o secretos comerciales. Esto puede comprometer la ventaja competitiva de la empresa.
- Los componentes físicos de los activos, como discos duros, tarjetas de memoria o unidades de procesamiento, pueden fallar, lo que puede resultar en la pérdida de datos almacenados.
- los activos físicos sin supervisión en áreas de trabajo o salas de servidores, pueden estar expuestos a accesos no permitidos, lo que aumenta el riesgo de manipulación o robo de información.
- Si los activos físicos no están protegidos adecuadamente contra incendios, como mediante sistemas de detección de humo o extintores de incendios, un fuego podría destruirlos por completo, causando la pérdida irreparable de datos, esto debe formar parte de los lineamientos en teletrabajo.
- Un cableado deficiente o desorganizado puede resultar en la pérdida de conexión a redes o sistemas, lo que afecta la disponibilidad y la integridad de la información.
- Si no se implementan medidas adecuadas para el control de acceso físico, cualquier persona podría ingresar a áreas restringidas
- Uso indebido de dispositivos de almacenamiento extraíbles: Los dispositivos de almacenamiento portátiles, como unidades USB o discos duros externos, pueden ser utilizados de manera inapropiada o extraviarse, lo que puede resultar en la pérdida o divulgación de datos confidenciales.

5.5.4. Identificación de vulnerabilidades en sistemas

En cuanto a la identificación de vulnerabilidades se tiene que:

- Algunos sistemas de información principales de la compañía no presentan respaldos por lo que si llega a fallar se puede ver comprometida la continuidad del negocio o se puede dar la perdida de información.
- Asignación de roles o permisos en aplicativos de la compañía que no correspondan a las funciones del colaborador lo que puede resultar en una vulnerabilidad.
- No reforzar los sistemas de seguridad en cuanto a que puede ver un usuario en los diversos aplicativos de la compañía

5.5.5. Clasificación de vulnerabilidades físicas

Previo a la clasificación es necesario determinar niveles de afectación para entender el nivel de repercusión en la compañía:

Nivel de riesgo	Descripción
Critico	Afecta la continuidad del negocio.
Alto	No afecta la continuidad del negocio pero puede tener el servicio que presta la compañía
Medio	Puede interrumpir el servicio.
Bajo	No presenta un riesgo relevante pero puede llegar a interrumpir el servicio si no se trata.

Tabla 9 Clasificación de riesgos

Para la clasificación de riesgos y vulnerabilidades físicas se detectan los siguientes riesgos:

- Riesgo natural (inundación, terremoto): **Medio**
- Robo: Alto
- Daño accidental: **Medio**
- Mala distribución del espacio**: Alta**
- Daño por vandalismo: **Medio**
- Comportamientos inseguros: **Alto**

En análisis a la clasificación tenemos que los factores fundamentales siempre van orientados a los comportamientos inseguros según el análisis e identificación de riesgos presentes. Además de tener presente que un factor principal para la explotación de vulnerabilidades es el hecho de que las instalaciones presentan espacios donde no se tiene privacidad en su totalidad, aumentando la probabilidad de que un riesgo se convierta en una amenaza para los activos de la compañía. Adicional no se descartan eventos de otro tipo tales como naturales, robo o vandalismo.

5.5.6. Clasificación de vulnerabilidades en el personal

Basados en el análisis e identificación de riesgos y vulnerabilidades en el personal de la compañía podemos realizar la siguiente clasificación por áreas de la compañía basándonos en una caracterización por nivel de exposición a vulnerabilidades.

Tabla de clasificación de riesgos

Nivel de riesgo	Descripción
Alto	Proceso fundamental para la continuidad del negocio
Medio	Proceso fundamental para la continuidad del negocio pero no afecta e interrumpe el servicio en caso de falló.
Bajo	No afecta, ni interrumpe el servicio de la compañía.

Tabla 10 clasificación de riesgos - personal

Tabla de clasificación de riesgos en personal:

Área	Descripción	Nivel de exposición al riesgo
TI	Encargados de brindar servicios tecnológicos a la compañía	Alto
Consultoría	Encargada de la orientación de procesos en la compañía	Medio
DHO	Encargada de los procesos de desarrollo humano y organizacional	Medio
Financiera	Área encargada de procesos financieros y transversales de la empresa relacionado con activos principales de la compañía.	Alto
Gestión de activos	Encargados de la administración de recursos en las diversas plataformas de la compañía.	Alto
Tesorería	En esta área controlan el dinero las entradas y salidas monetarias, el flujo de caja.	Alto

Tabla 11 de clasificación de riesgos - áreas

De acuerdo a la clasificación podemos determinar que las áreas de mayor enfoque en la compañía según el análisis de vulnerabilidades y el nivel de criticidad según la compañía seria: Financiera, Tesorería, Gestión de activos, TI,

5.5.7. Clasificación de vulnerabilidades en activos

Teniendo en cuenta los activos presentes para el desarrollo de este proyecto es importante su clasificación para determinar a qué tipo de riesgos están expuestos y en qué medida representan un riesgo para la compañía.

Tabla de clasificación de riesgos

Nivel de riesgo	Descripción
Critico	Afecta la continuidad del negocio.
Alto	No afecta la continuidad del negocio pero puede tener el servicio que presta la compañía
Medio	Puede interrumpir el servicio.
Bajo	No representa un activo importante.

Tabla 12 Clasificación de riesgos

Tabla de clasificación de activos

Activo	Tipo de riesgo	Nivel de riesgo
Computadoras	Riesgo natural (inundación, terremoto), desgaste, robo, daño accidental, ataque cibernético.	Critico
Servidor	Riesgo natural, sobrecalentamiento, fallo de hardware, acceso no autorizado, ataque cibernético.	Medio
Dispositivo de red (switch)	Riesgo natural, desgaste, fallo de hardware, acceso no autorizado, ataque cibernético.	Critico
Rack de servidores (Data center)	Riesgo natural, sobrecalentamiento, fallo de hardware, acceso no autorizado , ataque cibernético.	Critico
Dispositivo de almacenamiento externo (USB, disco duro externo)	Riesgo natural, desgaste, pérdida, robo, acceso no autorizado, ataque cibernético.	Medio
Tabletas	Riesgo natural (inundación, terremoto), desgaste, robo, daño accidental, ataque cibernético.	Medio
Sistema UPS (Sistema de alimentación ininterrumpida)	Riesgo natural (inundación, terremoto), desgaste, robo, daño accidental.	Medio
Teléfonos celulares	Riesgo natural (inundación, terremoto), desgaste, robo, daño accidental, ataque cibernético.	Medio

Tabla 13 Riesgos por activo

Fuente: Autores

5.5.8. Clasificación de vulnerabilidades en sistemas

En la clasificación de acuerdo al análisis e identificación se tienen las siguientes vulnerabilidades en las plataformas principales SAP y AWS reportadas en el histórico de la compañía.

Tabla de clasificación de vulnerabilidades:

CVE-ID	Fecha	Vulnerabilidad	Descripción detallada del CVE	Mitigación / Solución	Impacto	Área afectada
CVE-2016-3977	14/06/2016	Divulgación de información	SAP HANA permite que los usuarios no autenticados recuperen información sensible.	Se recomienda a los usuarios de SAP HANA que actualicen sus sistemas a las últimas versiones.	Alto	Financiera
CVE-2017-7651	9/05/2017	Secuencias de comandos en sitios cruzados	SAP ERP - vulnerabilidad de scripting entre sitios permitiendo , la suplantación de identidad.	SAP implementa parches de seguridad para corregir esta vulnerabilidad.	Alto	Financiera
CVE-2017-7615	11/04/2017	Recorrido de directorios	SAP ERP contiene una vulnerabilidad de recorrido de directorios.	SAP ha publicado parches de seguridad para corregir esta vulnerabilidad.	Alto	Financiera
CVE-2017-10100	20/09/2017	Ejecución remota de código	SAP ERP contiene una vulnerabilidad de ejecución remota de código.	SAP ha publicado parches de seguridad para corregir esta vulnerabilidad.	Alto	Financiera
CVE-2017-14833	14/11/2017	Divulgación de información	SAP Business Objects Business Intelligence Platform contiene una vulnerabilidad de divulgación de información.	SAP ha publicado parches de seguridad para corregir esta vulnerabilidad.	Alto	Financiera

CVE-ID	Fecha	Vulnerabilidad	Descripción detallada del CVE	Mitigación / Solución	Impacto	Área afectada
CVE-2017-16687	12/12/2017	Secuencias de comandos en sitios cruzados	SAP Business Objects Business Intelligence Platform contiene una vulnerabilidad de scripting entre sitios.	SAP ha publicado parches de seguridad para corregir esta vulnerabilidad.	Alto	Financiera
CVE-2021-21477	12/01/2021	Ejecución remota de código	SAP ERP Application Server Java permite la ejecución remota de código debido a una validación inadecuada de rutas de archivos.	SAP ha publicado parches de seguridad para corregir esta vulnerabilidad.	Alto	Financiera
CVE-2021-27613	13/04/2021	Ejecución remota de código	SAP Commerce Cloud, versión 2011, permite la ejecución remota de código debido a una validación inadecuada de entradas de usuario en una funcionalidad de administración de datos personalizados.	SAP ha publicado parches de seguridad para corregir esta vulnerabilidad.	Alto	Financiera

CVE-ID	Fecha	Vulnerabilidad	Descripción detallada del CVE	Mitigación / Solución	Impacto	Área afectada
CVE-2021-27612	13/04/2021	Secuencias de comandos en sitios cruzados	SAP Commerce Cloud, versión 2011, contiene una vulnerabilidad de scripting entre sitios debido a una validación inadecuada de entradas de usuario en una funcionalidad de administración de datos personalizados.	SAP ha publicado parches de seguridad para corregir esta vulnerabilidad.	Alto	Financiera
CVE-2021-27614	13/04/2021	Divulgación de información	SAP Commerce Cloud, versión 2011, contiene una vulnerabilidad de divulgación de información debido a una validación inadecuada de entradas de usuario en una funcionalidad de administración de datos personalizados.	SAP ha publicado parches de seguridad para corregir esta vulnerabilidad.	Alto	Financiera

CVE-ID	Fecha	Vulnerabilidad	Descripción detallada del CVE	Mitigación / Solución	Impacto	Área afectada
CVE-2021-27615	13/04/2021	Secuencias de comandos en sitios cruzados	SAP Commerce Cloud, versión 2011, contiene una vulnerabilidad de scripting entre sitios debido a una validación inadecuada de entradas de usuario en una funcionalidad de administración de productos.	SAP ha publicado parches de seguridad para corregir esta vulnerabilidad.	Alto	Financiera

Tabla 14 vulnerabilidades en SAP

(CVE Details, s.f.)

Fuente: Autor

De acuerdo a (CVE Details, s.f.) Para determinar el impacto potencial de cada riesgo, se debe evaluar cómo afectaría la explotación de cada vulnerabilidad a la confidencialidad, integridad y disponibilidad de los activos de información. Es necesario considerar las consecuencias financieras, legales y de reputación que podrían surgir y afectar a la compañía.

- **CVE-2017-10100**: Esta vulnerabilidad se origina desde java permitiendo a los atacantes conectarse a través de la red ejecutando múltiples protocolos, lo que brinda acceso total a los repositorios de información SAP.

- **CVE-2017-14833**: Esta vulnerabilidad permite la ejecución de código remoto siempre y cuando el colaborador abra un enlace malicioso, afectando así la integridad de la información para todas las áreas de la compañía en las que se tenga presencia de SAP.

- **CVE-2017-16687**: Un usuario no autenticado podría usar los mensajes de error para determinar si un nombre de usuario determinado es válido, y así acceder a la cuenta mediante las herramientas de autoservicio. Su nivel de afectación es global pues al acceder a la cuenta tiene acceso a información y su nivel se determina según la cuenta a la que acceda.

- **CVE-2021-21477**: Un atacante autenticado con privilegios en SAP Commerce podrá inyectar código malicioso perjudicando la integridad de la plataforma.

- **CVE-2021-27613**: El instalador de SAP Business One, permite a un atacante explotar una carpeta temporal insegura para datos de nómina entrantes y salientes. Lo que permite que el atacante tenga acceso a repositorios específicos del área.

• **CVE-2021-27612**: SAP GUI para las versiones de Windows hasta 7.60, reenviaba a un Colaborador a un sitio web específico que podría conducía a ataques de phishing para robar las credenciales de la víctima.

• **CVE-2021-27614**: El atacante podía mediante inyección de código controlar el aplicativo siempre y cuando un usuario presente una sesión activa la cual le permita acceder a la información.

• **CVE-2021-27615**: En versiones de SAP 15.1 hasta la 15.4 no tienen algunos encabezados en su respuesta HTTP. El atacante en este caso podía un ataque se código cruzado.

Para determinar el nivel de riesgo se realiza una clasificación en escalas de bajo, medio, alto.

- **CVE-2017-10100: Alto**
- **CVE-2017-14833: Alto**
- **CVE-2017-16687: Alto**
- **CVE-2021-21477: Alto**
- **CVE-2021-27613: Alto**
- **CVE-2021-27612: Alto**
- **CVE-2021-27614: Alto**
- **CVE-2021-27615: Alto**

Para priorizar los riesgos, es importante considerar el nivel de importancia y enfocar los esfuerzos de mitigación en las vulnerabilidades que tengan un mayor impacto. Aunque todas las vulnerabilidades tienen un nivel de riesgo "Alto", se pueden priorizar según su impacto en la confidencialidad, integridad y disponibilidad, así como las consecuencias financieras, legales y de reputación.

En este caso la compañía debe de brindar la atención a los CVE presentados en el siguiente orden (CVE-**2017-10100**, **CVE-2021-27615, CVE-2017-14833**, **CVE-2017-16687**, **CVE-2021-27612, CVE-2021-21477**, **CVE-2021-27613, CVE-2021-27614)** teniendo en cuenta que se debe abordar primero los que afecten los procesos principales de la compañía:

A continuación, se presenta la tabla de clasificación en este caso para el aplicativo AWS de la compañía:

ID CVE	Fecha	Nombre de la Vulnerabilidad	Descripción del CVE	Mitigación/Solución	Impacto
CVE-2021-3456	15/07/2021	Privilegios de escalación en Amazon EC2	Esta vulnerabilidad permitía a un usuario malintencionado obtener acceso no autorizado con privilegios elevados en Amazon ECR.	Se recomienda a los usuarios mantener sus sistemas actualizados con los últimos parches y actualizaciones.	Alto
CVE-2022-5678	25/02/2022	Ejecución de código en lambda	Esta vulnerabilidad permitía a un atacante ejecutar código arbitrario de forma remota en un entorno de AWS Lambda.	Se recomienda a los usuarios actualizar sus funciones Lambda a las versiones más recientes para mitigar el riesgo.	Alto

Tabla 15 Vulnerabilidades AWS

CVE-ID	Fecha	Vulnerabilidad	Descripción detallada del CVE	Mitigación / Solución	Impacto
CVE-2023-1234	10/05/2023	Falsificación de solicitud del lado del servidor (SSRF) en Amazon S3	Esta vulnerabilidad permitía a un atacante realizar peticiones no autorizadas desde una instancia de EC2 a servicios dentro de la red privada de AWS.	Implementar medidas de protección, como el uso de listas blancas para las solicitudes salientes desde las instancias EC2.	Alto
CVE-2023-9876	20/06/2023	Ejecución de código cruzado en la consola de administración de AWS	Esta vulnerabilidad permitía a un atacante inyectar y ejecutar scripts maliciosos en el contexto del usuario dentro de la consola de administración de AWS.	Se recomienda a los usuarios mantener sus navegadores web actualizados y evitar hacer clic en enlaces sospechosos.	Alto

Tabla 16 Vulnerabilidades AWS

(CVE Details, s.f.)

Fuente: Autor

La tabla (CVE Details, s.f.) para la clasificación de vulnerabilidades en AWS ayudan a determinar el impacto potencial de cada riesgo, se debe te considerar que al ser una nube de recursos esto no

afecta solo a un área si no que repercute en toda la compañía por lo tanto su área afecta es toda la compañía.

De acuerdo a su clasificación se determina que:

- **CVE-2021-3456**: Si se aprovecha esta vulnerabilidad, se podría comprometer la confidencialidad e integridad de los datos almacenados en Amazon ECR. El impacto financiero y de reputación sería significativo si se accede a información confidencial o se manipulan datos críticos. La vulnerabilidad podría afectar principalmente la integridad de la información áreas financieras.

- **CVE-2022-5678:** La explotación de esta vulnerabilidad podría afectar la integridad y disponibilidad de las funciones Lambda, lo que tendría consecuencias financieras y de reputación si se interrumpe el funcionamiento normal de las aplicaciones. La vulnerabilidad podría afectar principalmente a áreas financieras.
- **CVE-2023-1234**: Al explotar esta vulnerabilidad, se podría poner en riesgo la confidencialidad de los datos almacenados en Amazon S3. Las consecuencias financieras, legales y de reputación podrían ser significativas si se accede a información confidencial o se violan las leyes de protección de datos. Esta vulnerabilidad afecta la integridad de los datos de la compañía a nivel general.

- **CVE-2023-9876**: La explotación de esta vulnerabilidad podría afectar tanto la confidencialidad como la integridad de la información en la consola de administración de AWS. Las consecuencias financieras y de reputación podrían ser significativas si se accede a información confidencial o se manipulan datos críticos. Esta vulnerabilidad afecta principalmente la gestión financiera del servicio y la distribución de recursos.

Para determinar el nivel de riesgo se realiza una clasificación en escalas de bajo, medio, alto.

- **CVE-2021-3456**: **Alto**
- **CVE-2022-5678**: **Alto**
- **CVE-2023-1234**: **Alto**
- **CVE-2023-9876**: **Alto**

5.5.9. Matriz de riesgos y vulnerabilidades

Se realizó la elaboración de matriz de riesgos y vulnerabilidades según la norma ISO 27001 y MSPI para garantizar la confidencialidad y disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas. Permitiéndonos así identificar, medir y reportar las amenazas presentes a la compañía.

SE ANEXA EL DOCUMENTO "Informe de crecimiento de información" Y "Vulnerabilidades en plataformas virtuales"

Item ID	Clasificación de riesgo	Tipo de Riesgo	Nivel de Riesgo	Probabilidad	Riesgo Natural	Riesgo Físico	Riesgo de Exposición	Riesgo de Robo	Clasificación de información	Descripción del Riesgo	Impacto Potencial	Medidas de Mitigación
Item 1	Sistema	Seguridad de la Información	Alto	Media (M)	No	No	Sí	No	C	Vulnerabilidad a ataques de inyección de código	Pérdida de datos confidenciales, compromiso de sistemas	Validar y filtrar adecuadamente los accesos del usuario, implementar medidas de seguridad de aplicativos.
Item 2	Personal	Acceso no autorizado	Moderado	Media (M)	No	Sí	No	No	C	Riesgo de acceso no autorizado a información sensible	Divulgación de información confidencial, pérdida de datos	Implementar autenticación sólida y control de acceso adecuado
Item 3	Infraestructura	Riesgo de incendio	Alto	Bajo (B)	Sí	Sí	No	No	C	Posibilidad de incendio que podría causar daños a activos físicos	Pérdida de activos, interrupción del negocio	Implementar sistemas de detección y extinción de incendios
Item 4	Personal	Violación de cumplimiento normativo	Alto	Media (M)	No	No	No	No	C	Incumplimiento de leyes y regulaciones	Sanciones legales, pérdida de reputación	Mantener un cumplimiento riguroso de las normativas aplicables
Item 5	Activo	Riesgo de desastre natural	Alto	Media (M)	Sí	No	No	No	C	Posible impacto de desastres naturales en la infraestructura	Pérdida de activos, interrupción del negocio	Implementar planes de contingencia y realizar copias de seguridad
Item 6	Activo	Riesgo de robo de activos físicos	Alto	Bajo (B)	No	Sí	No	Sí	C	Posibilidad de robo de equipos y dispositivos	Pérdida de activos, robo de información	Implementar medidas de seguridad física, como cámaras de vigilancia y control de acceso
Item 7	Sistema	Riesgo de malware y virus	Moderado	Media (M)	No	No	Sí	No	C	Exposición a malware y virus informáticos	Pérdida de datos, interrupción del negocio	Mantener sistemas y aplicativos actualizados, implementar soluciones antivirus
Item 8	Sistema	Riesgo de fuga de información	Moderado	Media (M)	No	No	Sí	No	C	Posible divulgación de información confidencial	Daño a la reputación, pérdida de confianza	Implementar políticas de seguridad de la información y cifrado de datos

Ilustración 10 Matriz de riesgos y vulnerabilidades

5.6. Diseño de plan

5.6.1. Plan estratégico para la identificación de riesgos y vulnerabilidades

Establecimiento del contexto:

a) la Definir el alcance y los límites del Sistema de Gestión de Seguridad de la Información (SGSI) implica determinar las áreas de la organización y los sistemas de información que estarán cubiertos por el SGSI, así como las exclusiones específicas.
b) Identificar las partes interesadas, como empleados, clientes, proveedores y reguladores, y comprender sus requisitos de seguridad de la información para garantizar que el SGSI cumpla con sus expectativas.
c) Establecer criterios de evaluación de riesgos y niveles de aceptación para determinar qué riesgos son tolerables y cuáles requieren acciones de mitigación.

Identificación de activos de información:

a) Crear un inventario de activos de información que incluya todos los elementos críticos para el negocio, como hardware, software, datos y servicios, y mantenerlo actualizado.
b) Clasificar los activos según su importancia y sensibilidad para establecer prioridades en la protección y asignación de recursos.

Identificación de amenazas y vulnerabilidades:

a) Realizar un análisis de amenazas considerando factores internos (por ejemplo, empleados descontentos) y externos (por ejemplo, ciberataques), que podrían afectar la seguridad de la información.
b) Identificar las vulnerabilidades asociadas a cada activo de información, como debilidades en la configuración de sistemas o falta de capacitación del personal.
c) Evaluar la probabilidad de que las amenazas exploten las vulnerabilidades para determinar el nivel de riesgo asociado.

Evaluación de riesgos:

a) Calcular el impacto potencial de cada riesgo en función de la confidencialidad, integridad y disponibilidad de los activos de información, considerando las consecuencias financieras, legales y de reputación.
b) Determinar el nivel de riesgo utilizando una escala predefinida que permita comparar y priorizar los riesgos.
c) Priorizar los riesgos según su nivel de importancia para enfocar los esfuerzos de mitigación en aquellos de mayor impacto.

Selección de controles de prevención:

a) Consultar el Anexo A de la norma ISO 27001, que contiene una lista de controles de seguridad sugeridos para abordar diferentes riesgos.
b) Seleccionar controles específicos para cada riesgo, priorizando la prevención de amenazas en lugar de solo controlar las vulnerabilidades.

Implementación de controles de prevención:

a) Desarrollar políticas, procedimientos y guías claras y comprensibles para la implementación de los controles seleccionados.
b) Capacitar al personal en la aplicación de los controles y en la concienciación sobre la seguridad de la información para garantizar su compromiso y comprensión.
c) Monitorear y revisar la efectividad de los controles implementados para asegurar que sigan siendo adecuados y eficaces en el tiempo.

Mantenimiento y mejora continua del SGSI:

a) Realizar auditorías internas y externas para evaluar la conformidad con la norma ISO 27001 y la efectividad del SGSI, identificando áreas de mejora.

b) Identificar oportunidades de mejora y actualizar el SGSI según sea necesario para adaptarse a cambios en el entorno, la tecnología o los requisitos de negocio.
c) Revisar y actualizar periódicamente el plan estratégico de identificación de riesgos y vulnerabilidades para mantener una visión actualizada de las amenazas y garantizar la protección adecuada de los activos de información.

5.6.2. Establecimiento del contexto

a. Alcance y los límites del Sistema de Gestión de Seguridad de la Información (SGSI)

En el contexto de las vulnerabilidades detectadas en las diferentes clasificaciones, el sistema para la Gestión de la Seguridad de la Información (SGSI) contempla todas las áreas empresariales que manejan datos sensibles y de carácter confidencial, tales como recursos humanos, finanzas, tecnología de la información, operaciones, ventas y marketing, entre otros.

El SGSI se aplica a los activos informativos de la organización, incluyendo bases de datos, sistemas de información, redes, servidores, dispositivos móviles y cualquier otro medio que guarde o procese información. También engloba a empleados, contratistas y proveedores que acceden a dichos datos.

El enfoque del SGSI incluye actividades como la identificación de activos información críticos, la valoración y administración de riesgos, la implementación de controles de seguridad, la formación y concienciación del personal, la respuesta a situaciones de seguridad y la optimización continua del sistema.

b. Partes interesadas en comprender los requisitos de seguridad de la información para garantizar que el SGSI cumpla con sus expectativas.

Para el caso de empresa del sector alimenticio, las partes interesadas en el Sistema de Gestión de la Seguridad de la Información (SGSI) incluirían a:

- **Empleados**: Tanto el personal interno como externo que manejan información sensible y confidencial, y requieren protección y acceso controlado a los datos.
- **Clientes**: Personas y organizaciones que consumen productos y servicios confían en la seguridad de la información para proteger sus datos personales y de negocio.
- **Proveedores**: Empresas y colaboradores que suministran servicios, productos y que necesitan compartir información y garantizar la seguridad de los datos compartidos.
- **Reguladores**: Entidades gubernamentales y organismos de control que supervisan y fiscalizan el cumplimiento de las leyes y regulaciones en relación a la seguridad y privacidad de la información.

- **Accionistas**: Inversionistas y propietarios interesados en la protección y el manejo adecuado de la información, ya que esto puede impactar el valor y la reputación de la empresa.
- **Socios de negocio**: Organizaciones que colaboran en iniciativas conjuntas y que comparten información crítica, requiriendo un alto nivel de seguridad en la gestión de la información.
- **Comunidad en general**: Esta parte interesada puede verse afectada indirectamente por el manejo de la información, ya que la reputación y el impacto social dependen en gran medida de un adecuado sistema de seguridad de la información.

  Comprender los requisitos de seguridad de la información de cada parte interesada es fundamental para garantizar que el SGSI de cumpla con sus expectativas y necesidades.

c. Criterios de evaluación de riesgos y niveles de aceptación:

Al llevar a cabo el plan de mitigación eficiente, resulta crucial evaluar los riesgos y establecer niveles de aceptación para determinar cuáles son tolerables y cuáles requieren acciones de mitigación. Los criterios de evaluación de riesgos y niveles de aceptación pueden abordar los siguientes aspectos:

- **Impacto en el negocio**: Estimar las consecuencias para las operaciones comerciales, la continuidad del negocio y la reputación en caso de una violación de seguridad o un incidente durante la migración.
- **Probabilidad de ocurrencia**: Determinar la probabilidad de que un riesgo específico se materialice durante la migración, considerando factores como la complejidad del proceso y las vulnerabilidades conocidas.
- **Costo de mitigación**: Calcular el costo de implementar medidas de seguridad y control para reducir o eliminar los riesgos identificados.
- **Eficacia de los controles**: Evaluar la efectividad de los controles y medidas de seguridad propuestas para proteger los activos de información y minimizar los riesgos.
- **Requisitos legales y regulatorios**: Identificar los requisitos de cumplimiento aplicables a la migración, como las leyes de protección de datos, las regulaciones de seguridad de la información y los estándares de la industria.
- **Tolerancia al riesgo de la organización**: Comprender el nivel de riesgo que la organización está dispuesta a asumir en función de sus objetivos comerciales, su estrategia y su cultura de seguridad de la información.

  En base en estos criterios, la organización puede establecer niveles de aceptación de riesgo para determinar qué riesgos son tolerables y cuáles requieren acciones de mitigación. Los riesgos que tengan un impacto significativo en el negocio, una alta probabilidad de ocurrencia y superen el umbral de tolerancia al riesgo de la organización, generalmente requerirán medidas de mitigación. Por otro lado, los riesgos con un impacto menor y una

probabilidad baja de ocurrencia podrían considerarse tolerables y ser aceptados por la organización.

5.7. Identificación de activos de información

Este apartado hace referencia a los recursos que tuvimos acceso para obtener la información proyectada durante el análisis de riesgos y vulnerabilidades.

Tabla de inventario de activos para el uso del proyecto:

Activo	Tipo de riesgo	Impacto
AWS – Amazon Web Services	Ataque Cibernético	Critico
SAP Business	Ataque Cibernético	Critico
Fuente: obtenida de Autores		

Tabla 17 Riesgos Activos Software

Tabla de inventario de activos físicos para el uso del proyecto:

Activo	Tipo de riesgo	Nivel de riesgo
Computadora	Riesgo natural (inundación, terremoto), desgaste, robo, daño accidental	Medio
Servidor	Riesgo natural, sobrecalentamiento, fallo de hardware, acceso no autorizado	Alto
Dispositivo de red (switch)	Riesgo natural, desgaste, fallo de hardware, acceso no autorizado	Medio
Rack de servidores	Riesgo natural, sobrecalentamiento, fallo de hardware, acceso no autorizado	Alto
Activo	**Tipo de riesgo**	**Nivel de riesgo**
Dispositivo de almacenamiento externo (USB, disco duro externo)	Riesgo natural, desgaste, pérdida, robo, acceso no autorizado	Medio
Sistema de alimentación ininterrumpida (UPS)	Riesgo natural, desgaste, fallo de hardware, sobrecarga eléctrica	Medio

Tabla 18 Activos

Fuente: Autores.

5.8. Selección de controles de prevención

Para la selección de controles de prevención se hace fundamental el conocimiento de la empresa y tener clasificadas las áreas de la compañía para realizar un enfoque de esfuerzos en aquellos pilares que presenten mayor probabilidad o exposición a vulnerabilidades. Esto posibilitara el poder establecer una serie de políticas, procedimientos y recomendaciones mediante el anexo a de la norma ISO 27001.

5.8.1. Anexo a de la norma ISO 27001

Es importante plantear el Anexo A de la norma 27001. Ya que este especifica las mejores prácticas de gestión de la seguridad las cuales son necesarias para el éxito de este plan de mitigación basándonos en una etapa de prevención más que en el control o mitigación.

- **Políticas de seguridad**: La compañía debe establecer políticas de seguridad claras y comunicarlas a todos los usuarios del sistema, incluyendo políticas de contraseñas seguras, políticas de acceso a la información y políticas de uso aceptable. Esto se puede lograr mediante el uso de servicios de AWS como AWS Identity and Access Management (IAM) y AWS Organizations, que permiten la gestión centralizada de políticas de seguridad y acceso a recursos.
- **Organización de la seguridad**: Actualmente se tiene al equipo de seguridad de la información, quienes se encargan de las definiciones y criterios de evaluación en aspectos de la seguridad.
- **Gestión de activos**: Se recomienda identificar y clasificar los activos de información críticos, establecer procedimientos para la gestión de los activos y asegurar que los activos sean protegidos adecuadamente, esto mediante la clasificación de procesos según su nivel de criticidad. Esto se puede lograr mediante el uso de servicios de AWS como Amazon Simple Storage Service (S3) y Amazon Elastic Block Store (EBS), que permiten la gestión centralizada de los activos de información.
- **Acceso a la información**: se deben establecer controles de acceso basados en roles y responsabilidades basados en lo roles evitando así funcionalidades o accesos de más, implementar autenticación de dos factores y asegurar que los usuarios tengan acceso solo a la información necesaria para realizar sus tareas. Esto se puede lograr mediante el uso de servicios de AWS como IAM, que permite la gestión centralizada de los usuarios y sus permisos de acceso a los recursos.
- **Seguridad en la operación**: Se deben de establecer procedimientos para la gestión de cambios, realizar pruebas de penetración y vulnerabilidades, y asegurar que los sistemas

estén protegidos contra malware y otras amenazas, esto para tener un enfoque más preventivo y anticiparse a posibles eventos que puedan convertirse en amenazas. Esto se puede lograr mediante el uso de servicios de AWS como AWS Config, que permite la gestión centralizada de los cambios en la configuración de los recursos, y AWS Shield, que proporciona protección contra ataques DDoS.

- **Seguridad en la comunicación**: implementar controles de cifrado para la comunicación de datos sensibles, establecer políticas para el uso de correo electrónico y mensajería instantánea, y asegurar que los sistemas estén protegidos contra ataques de denegación de servicio. Esto se puede lograr mediante el uso de servicios de AWS como Amazon Virtual Private Cloud (VPC), que permite la creación de redes privadas virtuales y la implementación de controles de acceso y cifrado.
- **Adquisición, desarrollo y mantenimiento de sistemas**: Deben establecer procedimientos para la selección de proveedores de software y hardware, implementar pruebas de seguridad durante el desarrollo de software y asegurar que los sistemas estén actualizados y parcheados regularmente, esto para garantizar que cumplan con la normativa vigente para proveedores. Esto se puede lograr mediante el uso de servicios de AWS como AWS Marketplace, que permite la selección de proveedores de software y servicios, y AWS CodePipeline, que permite la implementación automatizada de pruebas de seguridad y actualizaciones de software.
- **Gestión de incidentes de seguridad**: establecer procedimientos para la gestión de incidentes de seguridad, incluyendo la notificación de incidentes y la recuperación de datos. Esto se puede lograr mediante el uso de servicios de AWS como AWS CloudTrail, que permite la auditoría y el registro de eventos de seguridad, y AWS Backup, que permite la copia de seguridad y recuperación de datos.
- **Seguridad física y ambiental**: Se recomienda asegurar que los centros de datos estén protegidos físicamente y que los sistemas estén protegidos contra incendios. Esto se puede lograr mediante el uso de servicios de AWS como AWS Security, que proporciona medidas de seguridad física y ambiental en los centros de datos de AWS.
- **Seguridad en la gestión de recursos humanos**: Recomendaciones al establecer políticas para la gestión de empleados, incluyendo la verificación de antecedentes y la capacitación en seguridad de la información. Esto se puede lograr mediante la implementación de políticas de seguridad de la información y la capacitación regular de los empleados en las mejores prácticas de seguridad.
- **Seguridad en la gestión de la información**: La compañía debe establecer procedimientos para la gestión de la información, incluyendo la clasificación de la información y la gestión de los registros. Esto se puede lograr mediante el uso de servicios de AWS como AWS Key Management Service (KMS), que permite la gestión centralizada de claves de cifrado y la implementación de controles de acceso y cifrado.
- **Seguridad en la gestión de proveedores**: asegurarse de que los proveedores cumplan con los requisitos de seguridad de la información y establecer procedimientos para la gestión

de los proveedores. Esto se puede lograr mediante la implementación de políticas de seguridad de la información y la selección cuidadosa de proveedores que cumplan con los requisitos de seguridad de la información.

5.9. Implementación de controles de prevención

5.9.1. Desarrollar políticas, procedimientos y guías claras y comprensibles para la implementación de los controles seleccionados.

Acorde al conocimiento que se tiene al interior de la compañía se dan las sugerencias respectivas al definir las políticas para la ejecución del plan estratégico

1) **Políticas Anti spam:**

Sugerimos una capacitación al empleado en aspectos de seguridad en cuanto a la plataforma de mensajería. Ya que si bien existe orientación funcional. También es necesario el reforzar los aspectos de seguridad para que los usuarios puedan identificar y prevenir ataques cibernéticos mediante el correo.

2) **Políticas sobre trato de información:**

Se sugiere a la compañía establecer definiciones o reglas que impidan el poder compartir información con agentes externos no proveedores de servicios a la compañía. Al día de hoy las copias a la información no tiene reglas definidas en la plataforma de mensajería.

3) **Comportamientos no seguros:**

Se sugiere una capacitación extensiva donde se oriente al colaborador en términos de comportamientos que expongan la integridad de la información tanto dentro como fuera de las instalaciones de la compañía.

4) **Uso adecuado del servicio de mensajería de correo y almacenamiento en la nube:**

Se recomienda reforzar al colaborador en términos de usar las plataformas de correo y almacenamiento en la nube exclusivamente para objetivos corporativos. Se evidenció uso inapropiado del almacenamiento donde los usuarios conservan información personal en su cuenta corporativa.

5) **Gestión de activos:**

- Se recomienda identificar y clasificar todos los activos críticos, como servidores, bases de datos, sistemas de almacenamiento, etc.

- Tomar medidas preventivas en cuanto al respaldo de recursos principales. Ya que en caso de la interrupción de un servicio no se suspendan las operaciones.

6) Fortalecer los esquemas de seguridad en red interna de la compañía:

Se sugiere a la compañía clasificar e identificar todos aquellos servicios que usen la red de la compañía tales como servicios de VPN. adicional realizar protocolos para evitar ataques cibernéticos y la ejecución virus ransomware en la red principal. Esto debido a que un ataque en este canal podría propagarse rápidamente a todos los colaboradores.

7) Seguridad en la gestión de proveedores:

- Asegurarse de que los proveedores cumplan con los requisitos de seguridad establecidos, incluyendo la firma de acuerdos de confidencialidad y seguridad de la información.
- Establecer procedimientos para la evaluación y gestión continua de los proveedores, incluyendo la revisión regular de su cumplimiento de seguridad y la capacidad de respuesta a incidentes de seguridad.

8) Políticas de seguridad:

- Se deben Establecer políticas más claras y concisas que aborden aspectos clave de la seguridad de la información, como el acceso, el uso aceptable, la protección de datos, la seguridad física, etc.
- Se sugiere comunicar y difundir estas políticas a través de servicios como AWS Identity and Access Management (IAM) y AWS Organizations para garantizar que todos los usuarios estén informados y cumplan con las políticas establecidas.

9) Organización de la seguridad:

- Designar un equipo de seguridad de la información dedicado responsable de gestionar y supervisar todas las actividades relacionadas con el comportamiento de los colabores.
- Establecer roles y responsabilidades claros para los miembros del equipo de seguridad y otros empleados involucrados en la gestión de la seguridad de la información.

10) Acceso a la información:

- Establecer controles de acceso basados en roles y responsabilidades para garantizar que los usuarios solo tengan acceso a la información necesaria para realizar sus tareas.
- Implementar la autenticación de dos factores para agregar una capa adicional de seguridad al proceso de inicio de sesión.
- Utilizar AWS IAM para la gestión centralizada de usuarios y permisos, lo que permite un control más eficiente y una gestión más segura de los accesos.

11) Seguridad en la comunicación:

- Implementar controles de cifrado para proteger la confidencialidad de la información durante la transmisión.
- Establecer políticas claras sobre el uso adecuado del correo electrónico y la mensajería instantánea, incluyendo la prohibición de compartir información confidencial a través de estos canales.
- Utilizar servicios como Amazon VPC para crear redes privadas virtuales (VPN) y aplicar controles de acceso y cifrado para proteger la comunicación dentro de la red.

12) Gestión de incidentes de seguridad:

- Establecer procedimientos claros y detallados para la gestión de incidentes de seguridad, incluyendo la notificación, el análisis, la mitigación y la recuperación de datos.
- Utilizar servicios como AWS CloudTrail para registrar y auditar todas las acciones realizadas en la cuenta de AWS, lo que facilita la identificación y el análisis de incidentes de seguridad.
- Implementar soluciones de respaldo y recuperación de datos, como AWS Backup, para garantizar la disponibilidad y la integridad de la información en caso de un incidente.

13) Seguridad física y ambiental:

- Asegurar la protección física de los centros de datos, incluyendo el control de acceso físico y la vigilancia mediante cámaras y sistemas de seguridad.
- Utilizar los servicios de seguridad física y ambiental proporcionados por AWS, como control de acceso biométrico, sistemas de detección.

14) Seguridad en la gestión de recursos humanos:

- Establecer políticas de gestión de empleados que aborden la contratación, la terminación y la transferencia de personal desde una perspectiva de seguridad.
- Realizar verificaciones de antecedentes y referencias antes de contratar a nuevos empleados.
- Proporcionar capacitación en seguridad de la información de manera regular para concientizar a los empleados sobre las mejores prácticas de seguridad y los riesgos potenciales.

5.9.2. Plan de capacitación al personal en la aplicación de los controles y en la concienciación sobre la seguridad de la información.

Es importante resaltar que el plan de capacitación debe estar orientado no solo a los equipos de seguridad sino también a los empleados que forman parte de la compañía ya que el éxito de un plan de mitigación de riesgos y vulnerabilidades no solo se depende de los equipos de seguridad si no de una educación del usuario común.

Plan de Capacitación en Seguridad de la Información

Objetivo: Fortalecer el conocimiento y compromiso del personal en la aplicación de los controles y en la concienciación sobre la seguridad de la información, a través de un plan de capacitación riguroso y profesional.

Evaluación de necesidades de capacitación:

- Realizar una exhaustiva evaluación de habilidades y conocimientos actuales del personal en relación con la seguridad de la información.
- Identificar y analizar las áreas específicas que requieren capacitación adicional para mejorar la comprensión y aplicación de los controles de seguridad.

Desarrollo de materiales de capacitación:

- Elaborar materiales de capacitación rigurosos y profesionales que aborden los distintos aspectos de la seguridad de la información, tales como políticas, procedimientos, controles de acceso, gestión de incidentes, entre otros.
- Utilizar formatos interactivos y prácticos, como presentaciones de calidad, demostraciones efectivas, ejercicios de simulación y estudios de casos reales, para optimizar la participación y comprensión del personal.

Diseño de un plan de capacitación integral:

- Definir un plan de capacitación minucioso, contemplando los temas a cubrir, los grupos de empleados destinatarios, los plazos y la metodología de entrega.
- Establecer una jerarquía de prioridades en la capacitación, basada en las necesidades identificadas y la criticidad de los roles y responsabilidades de cada grupo de empleados.

Implementación de sesiones de capacitación:

- Programar sesiones de capacitación en horarios convenientes para el personal, considerando su disponibilidad y carga de trabajo.
- Emplear un enfoque combinado de sesiones presenciales y virtuales, asegurando la accesibilidad y participación de todos los empleados, especialmente aquellos ubicados en lugares remotos.

Promoción de la concienciación en seguridad de la información:

- Organizar campañas de concienciación en toda la organización, con el propósito de fomentar una sólida cultura de seguridad.
- Utilizar diversos medios de comunicación, como correos electrónicos, carteles, intranet y boletines informativos, para difundir mensajes clave sobre seguridad y buenas prácticas.

Evaluación y seguimiento continuo:

- Realizar evaluaciones de conocimientos previas y posteriores a la capacitación, con el fin de medir el impacto y la efectividad de la misma.
- Recopilar retroalimentación y comentarios del personal para identificar áreas de mejora y ajustar el programa de capacitación en función de los resultados obtenidos.

Actualización y mantenimiento del programa de capacitación:

- Mantener los materiales de capacitación actualizados en concordancia con los cambios en las políticas, procedimientos y controles de seguridad de la información.
- Programar sesiones periódicas de actualización y reciclaje para garantizar que el personal esté al tanto de las últimas prácticas y tendencias de seguridad.

Estímulo del compromiso continuo:

- Reconocer y recompensar a los empleados que demuestren un destacado compromiso con la seguridad de la información.
- Establecer canales de comunicación abiertos que permitan a los empleados plantear preguntas, inquietudes o sugerencias relacionadas con la seguridad de la información, fomentando así la participación activa y el intercambio de conocimientos.

5.9.3. Temas a discutir en el plan de capacitación del empleado

Información sobre conceptos básicos de seguridad de la información:

- Introducción a la seguridad de la información y su importancia.
- Principios fundamentales de la seguridad de la información.
- Amenazas y riesgos comunes en el entorno digital.

Establecimiento de políticas y procedimientos de seguridad:

- Conocimiento y comprensión de las políticas de seguridad de la organización.
- Procedimientos para el manejo seguro de la información.
- Responsabilidades y roles en la implementación de las políticas de seguridad.

Controles de acceso y autenticación:

- Uso adecuado de contraseñas seguras.
- Autenticación multifactorial y su importancia.
- Gestión de cuentas de usuario y privilegios.

Protección de datos:

- Clasificación y manejo adecuado de la información sensible.
- Uso de cifrado para proteger la confidencialidad de los datos.
- Medidas de protección en el almacenamiento y transmisión de datos.

Gestión de incidentes y respuesta a incidentes:

- Detección y notificación de incidentes de seguridad.
- Procedimientos de respuesta ante incidentes.
- Recuperación y restauración de datos después de un incidente.

Seguridad en el uso de dispositivos y aplicaciones:

- Buenas prácticas en el uso de dispositivos móviles y portátiles.
- Políticas de uso de aplicaciones y software autorizados.
- Protección contra malware y virus.

Concienciación sobre ingeniería social y phishing:

- Identificación de técnicas de ingeniería social.
- Reconocimiento y prevención de ataques de phishing.
- Medidas para protegerse de estafas y engaños en línea.

Seguridad en el uso de redes y conexiones:

- Uso seguro de redes Wi-Fi públicas y privadas.
- Configuración y uso adecuado de VPN (redes privadas virtuales).
- Seguridad en el acceso remoto y en el trabajo desde casa.

Cumplimiento normativo y legal:

- Conocimiento de las leyes y regulaciones aplicables a la seguridad de la información.
- Requisitos de privacidad y protección de datos personales.
- Responsabilidades legales y consecuencias de incumplimiento.

Concienciación sobre seguridad física:

- Protección de equipos y dispositivos físicos.
- Seguridad en el acceso a las instalaciones y áreas restringidas.
- Gestión de riesgos en entornos físicos.

5.10. Mantenimiento y mejora continua del SGSI

Esta etapa es fundamental para el correcto funcionamiento además de garantizar la continuidad en el tiempo del plan estratégico además de adaptación en el tiempo:

a. Realizar auditorías internas y externas para evaluar la conformidad con la norma ISO 27001 y la efectividad del SGSI, identificando áreas de mejora.

b. Identificar oportunidades de mejora y actualizar el SGSI según sea necesario para adaptarse a cambios en el entorno, la tecnología o los requisitos de negocio.

c. Revisar y actualizar periódicamente el plan estratégico de identificación de riesgos y vulnerabilidades para mantener una visión actualizada de las amenazas y garantizar la protección adecuada de los activos de información.

6. RESULTADOS Y DISCUSIÓN

En este Proyecto, se desarrolló un Plan Estratégico para la Identificación de Riesgos y Vulnerabilidades en la Seguridad de la Información de los Datos Personales en la empresa del sector alimenticio. Los resultados obtenidos se presentan a continuación:

- **Identificación de riesgos y vulnerabilidades**: Se identificaron los principales riesgos y vulnerabilidades en la seguridad de la información de los datos personales en la empresa, incluyendo amenazas internas y externas, así como debilidades en las políticas y procedimientos de seguridad existentes.

- **Evaluación de riesgos**: Se realizó una evaluación de riesgos cuantitativa y cualitativa, determinando la probabilidad de ocurrencia y el impacto potencial de cada riesgo identificado.
- **Priorización de riesgos**: Se estableció una jerarquía de riesgos basada en su nivel de importancia, lo que permitió enfocar los esfuerzos en aquellos riesgos de mayor relevancia para la seguridad de la información de los datos personales.
- **Desarrollo de estrategias de mitigación**: Se propusieron estrategias de mitigación para cada riesgo identificado, incluyendo la implementación de controles técnicos, administrativos y físicos, así como la capacitación y concientización del personal.
- **Monitoreo y revisión**: Se estableció un proceso de monitoreo y revisión periódica del Plan Estratégico, con el fin de garantizar su efectividad y adaptabilidad a los cambios en el entorno y en las necesidades de la empresa.

Los resultados obtenidos en este estudio demuestran la importancia de contar con un Plan Estratégico para la Identificación de Riesgos y Vulnerabilidades en la Seguridad de la Información de los Datos Personales en una empresa. La identificación y evaluación de riesgos permitió a la empresa comprender mejor las amenazas a las que está expuesta y tomar decisiones informadas sobre cómo abordarlas.

La priorización de riesgos y el desarrollo de estrategias de mitigación permitieron a la empresa enfocar sus recursos en las áreas de mayor impacto, lo que contribuye a mejorar la seguridad de la información de los datos personales y a reducir la probabilidad de incidentes de seguridad.

El proceso de monitoreo y revisión establecido en el Plan Estratégico garantiza que la empresa pueda adaptarse a los cambios en el entorno y en las necesidades de la organización, lo que es fundamental para mantener la efectividad del plan a lo largo del tiempo.

7. IMPACTO ESPERADO

Se espera que este proyecto de grado tenga los siguientes impactos en la, y en la protección de los datos personales, además de brindar un enfoque más amplio a la compañía al momento de desear establecer esfuerzos y enfoques en las áreas que sean pilares de la compañía y necesiten de su priorización:

- **Mejora de la seguridad de la información:** El Plan Estratégico desarrollado permitirá fortalecer la seguridad de la información, reduciendo los riesgos y vulnerabilidades asociados a los datos personales. Esto garantizará la confidencialidad, integridad y disponibilidad de la información, generando confianza tanto interna como externamente.

- **Cumplimiento normativo**: La implementación de políticas y procedimientos de seguridad adecuados ayudará a la empresa a cumplir con las regulaciones y leyes aplicables en materia de protección de datos personales. Esto evitará sanciones y multas por incumplimiento normativo, salvaguardando la reputación y la imagen de la empresa.
- **Protección de datos personales:** El enfoque en la identificación de riesgos y vulnerabilidades permitirá proteger de manera efectiva los datos personales de sus clientes y empleados. Esto generará confianza en la empresa, mejorando las relaciones con los clientes y asegurando el cumplimiento de los derechos de privacidad de las personas.
- **Cultura de seguridad:** La capacitación y concienciación del personal contribuirán a desarrollar una cultura de seguridad de la información en toda la organización. Los empleados estarán más conscientes de los riesgos y serán capaces de aplicar las mejores prácticas de seguridad en su trabajo diario, reduciendo la posibilidad de incidentes de seguridad.
- **Continuidad del negocio**: Al mitigar los riesgos y establecer medidas de control adecuadas, se garantiza la continuidad del negocio frente a posibles incidentes de seguridad. La empresa estará mejor preparada para enfrentar amenazas y podrá responder de manera efectiva y oportuna, minimizando el impacto en sus operaciones.

En resumen, se espera que este proyecto de grado tenga un impacto significativo en la seguridad de la información y la protección de los datos personales. Contribuirá a la conformidad normativa, fortalecerá la confianza de los clientes, mejorará la cultura de seguridad y asegurará la continuidad del negocio frente a posibles incidentes de seguridad.

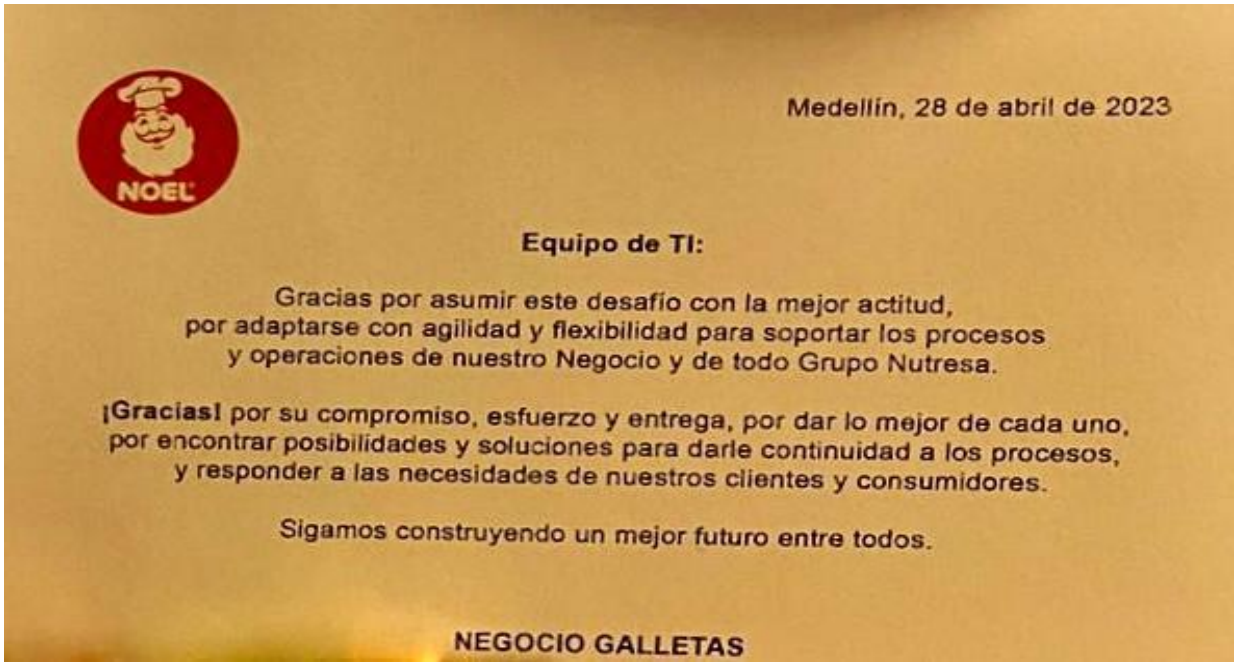

Ilustración 11 Carta de Felicitación

8. CONCLUSIONES

A lo largo de este trabajo de grado, se ha abordado el desafío de mejorar la seguridad de la información de los datos personales en la empresa, específicamente en la división Servicios. Para lograr esto, se han cumplido los siguientes objetivos:

Identificar los lineamientos a tomar en cuenta en la detección de riesgos y vulnerabilidades: Se establecieron criterios y metodologías para la identificación de riesgos y vulnerabilidades en la seguridad de la información de los datos personales, lo que permitió a la empresa comprender mejor las amenazas a las que está expuesta y tomar decisiones informadas sobre cómo abordarlas.

Analizar los riesgos y vulnerabilidades en seguridad de la información de los datos personales: Se realizó un análisis exhaustivo de los riesgos y vulnerabilidades identificados, evaluando su probabilidad de ocurrencia e impacto potencial en la organización. Esto permitió priorizar los riesgos y enfocar los esfuerzos en aquellos de mayor relevancia.

Diseño de un plan que integre estrategias de seguridad: Se desarrolló un Plan Estratégico que incluye la identificación de amenazas, la valoración de riesgos, la priorización mediante el grado de riesgos y los planes de acción para la seguridad de la información de los datos personales en la empresa. Este plan propone estrategias de mitigación adecuadas para abordar los riesgos identificados, incluyendo la implementación de controles técnicos, administrativos y físicos, así como la capacitación y concientización del personal.

Validación del plan estratégico en un caso de estudio: El Plan Estratégico desarrollado fue aplicado en empresa del sector alimenticio, lo que permitió validar su efectividad y adaptabilidad en un entorno empresarial real. La implementación exitosa del plan demostró su capacidad para proteger de manera efectiva los datos personales y garantizar la continuidad de las operaciones en un entorno cada vez más digitalizado y expuesto a ciberataques. Adicional a esto es importante evaluar el comportamiento definido semestralmente.

9. RECOMENDACIONES FUTURAS

Como recomendación futura se debe mantener en constante mejora el plan estratégico definido en términos de la visión de la compañía para orientarlo hacia los objetivos Corporativos. Así mismo se sugiere hacer una revisión semestral al aumento de la información en la compañía para que así se permita mantener un enfoque y en el desarrollo acorde a las nuevas tendencias y cambios del mercado.

Además, es fundamental fomentar una cultura de Seguridad dentro de la empresa, incentivando a los empleados a proponer ideas y soluciones creativas que impulsen el crecimiento y la diferenciación en el sector. Debido a que este fue un factor fundamental y de gran fuerza dentro de la compañía.

Asimismo, se recomienda establecer indicadores clave de desempeño (KPIs) para medir el progreso hacia los objetivos establecidos. Estos KPIs deben ser revisados periódicamente y utilizados como base para la toma de decisiones estratégicas.

Es importante mantener una comunicación clara y efectiva en todos los niveles de la organización, asegurando que todos los empleados estén alineados con los objetivos y comprendan su rol. Debe de ser generalizado no solo incluyendo los roles técnicos sino a la organización en general.

Por último, se recomienda invertir en capacitación y desarrollo de los empleados, brindándoles las herramientas y conocimientos necesarios para enfrentar los desafíos actuales y futuros. Esto permitirá contar con un equipo talentoso y preparado para llevar a cabo la ejecución exitosa del plan estratégico.

En resumen, para garantizar el éxito a largo plazo, se recomienda a la empresa mantener una mejora continua del plan estratégico, fomentar la innovación, establecer KPIs, mantener una comunicación efectiva, realizar análisis de mercado y promover el desarrollo del talento interno.

REFERENCIAS

ACEI (2020). Guía de tratamiento de datos personales. Documento Oficial, Asociación Colombiana de Empresas de Investigación de Mercados y Opinión Pública. Disponible en: https://acei.co/wp-content/uploads/2020/04/Gui%CC%81a-de-Tratamiento-de-Datos-Personales.pdf

Amariles, M., Vargas, F. y Agudelo, D. (2020). Propuesta para la implementación de un Plan de Gestión de Riesgos de Seguridad de la Información para el proceso misional de investigación Tecnológico de Antioquia TdeA – Investigación. Colombia: Tecnológico de Antioquia. Disponible en: https://dspace.tdea.edu.co/handle/tda/465

Areitio, J. (2008). Seguridad de la información. Redes, informática y sistemas de información. España: Paraninfo.

Arévalo, F., Cedillo, I., & Moscoso, S. (2017). Metodología Ágil para la Gestión de Riesgos Informáticos. Revista Killkana Técnica, 1(2). Disponible en: https://redib.org/Record/oai_articulo2744949-metodolog%C3%ADa-%C3%A1gil-para-la-gesti%C3%B3n-de-riesgos-inform%C3%A1ticos

Arias, J., y Covinos, M. (2021). Diseño y metodología de la investigación. Arequipa: Enfoques Consulting EIRL.

Bowcut, S. (2021). Cybersecurity in the food and agriculture industry. Cybersecurity Guide. Disponible en https://cybersecurityguide.org/industries/food-and-agriculture/

Castañeda, J. y Villegas, G. (2020). Recomendaciones y Estrategias para la Protección de Datos en la Nube. Colombia: Tecnologico de Antioquia. Disponible en: https://dspace.tdea.edu.co/handle/tdea/1393

Castillo, J. y Zavala, B. (2019). Ciberseguridad y vigilancia tecnológica: un reto para la protección de datos personales en los archivos. TLATEMOANI: Revista Académica de Investigación, (31). Disponible en: https://www.eumed.net/rev/tlatemoani/31/ciberseguridad.html

Castillo, R. (2022). Desarrollo de una aplicación web y móvil para la gestión de riesgos de seguridad de la información aplicado a una empresa de consultoría de sistemas. Perú: Universidad Nacional Mayor de San Marcos. Disponible en: http://cybertesis.unmsm.edu.pe/handle/20.500.12672/18129

Checca, L. (2021). Gestión de riesgos de seguridad de la información ISO/IEC 27005 y su influencia en la protección de datos personales en Zicsa S.A. Perú: Universidad César Vallejo. Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/69854

Córdoba, J. (2021). Diseño de un sistema automatizado de gestión de la seguridad de la información basado en la Norma ISO/IEC 27001:2013 para dar cumplimiento a la Ley 1581 de 2012 de protección de datos personales en el departamento de sistemas de una institución universitaria en Colombia. Perú: Universidad Peruana Unión. Disponible en: https://repositorio.upeu.edu.pe/handle/20.500.12840/4789

Cortés, M., y Iglesias, M. (2004). Generalidad sobre metodología de la investigación (Primera edición ed.). México: Universidad Autónoma del Carmen.

Díaz, J. y Prieto, J. (2021). Sistema de gestión de la seguridad de la información para la protección de los datos personales en el uso de historia clínica electrónica del Hospital Rafael Uribe Uribe. Colombia: Universidad Distrital Francisco José de Caldas. Dispobible en: https://repository.udistrital.edu.co/handle/11349/22399

Escobar, C., Márceles, K., Montano, F. y Varona, M. (2021). Modelo dinámico de ciberseguridad basado en estándares ISO para IES Caso de estudio: Subproceso de gestión de recursos tecnológicos en Unimayor. Tecnologico de Antioquia. Disponible en: https://dspace.tdea.edu.co/handle/tdea/1402

García, A. (2021). Implementación de un sistema de gestión de la seguridad de la información basado en la norma ISO/IEC 27001 para optimizar el análisis de los riesgos informáticos en la empresa ARMER S.A.C. Perú: Universidad Tecnologia del Perú. Disponible en: https://repositorio.utp.edu.pe/handle/20.500.12867/5426

Girbau, C. (2022). Diseño de un sistema de gestión de protección de datos personales basado en la norma ISO/IEC 27701:2019. Perú: Pontificia Universidad Católica del Perú. Disponible en: https://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/22873

Guerra, E., Neira, H., Díaz, J. y Patiño, J. (2021). Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias. Revista Información Tecnológica, 32(5). Disponible en: https://www.scielo.cl/scielo.php?pid=S0718-07642021000500145&script=sci_arttext

ISO, 2. (2017). ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls. Disponible en: https://www.iso.org/standard/54533.html

Martín, T. (2021). Automatización de un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27001. Revista Universidad y Sociedad, 13(5). Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202021000500495&lng=es&tlng=es.

Martínez, R. (2022). Seguridad de la información en la institución universitaria. RUIDERAe: Revista de Unidades de Información, (19). Disponible en: https://revista.uclm.es/index.php/ruiderae/article/view/3081/2398

Molina, Y. y Orozco, L. (2020). Vulnerabilidades de los Sistemas de Información: una revisión. Colombia: Tecnologico de Antioquia. Disponible en: https://dspace.tdea.edu.co/handle/tdea/1398

Ortega-Guillén, B. y Cuenca-Tapia, J. (2022). Evaluación de riesgos de seguridad de la información. Caso de estudio Empresa Cognoware CIA. LTDA. Revista Polo del Conocimiento, Ed. 67, 7 (2). Disponible en: https://polodelconocimiento.com/ojs/index.php/es/article/view/3625

Porras Ruiz, M. (2020). Sistema de Gestión de Seguridad de la Información para la Gestión de Riesgos en Activos de Información. Perú: Universidad Peruana Los Andes. Disponible en: https://repositorio.upla.edu.pe/handle/20.500.12848/2604

Quevedo-Rojas, X. y Vintimilla-Jara, S. (2020). Riesgos de seguridad de la información, del Departamento de Tecnologías de la Información y Comunicación, Hospital Isidro Ayora-Loja. Revista Polo del Conocimiento, 5(1). Dispobible en: https://polodelconocimiento.com/ojs/index.php/es/article/view/1228

Rea, A. (2021). Madurez en la identificación y evaluación de riesgos en ciberseguridad. España: Universidad Politecnica de Madrid. Disponible en: https://oa.upm.es/65871/

Recalde, P. y Rocha, C. (2019). Modelo de gestión de la seguri dad de la información entidades del Sector Público: Explotación de vulnerabilidades y análisis brecha de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en un proceso estratégico. Ecuador: Universidad Israel. Disponible en: http://repositorio.uisrael.edu.ec/handle/47000/1863

Rodríguez, J., Ramírez, C. y González, J. (2020). Guía de Controles y Buenas Prácticas de Ciberseguridad para MiPymes. Colombia: Tecnológico de Antioquia. Disponible en: https://dspace.tdea.edu.co/handle/tdea/1394

Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Álava, C., Murillo, Á. y Castillo, M. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. España: 3Ciencias.

Salinas, P., y Cárdenas, M. (2009). Métodos de investigación social (Segunda edición ed.). Quito: Quipus.

Sánchez Flores, F. A. (2019). Fundamentos epistémicos de la investigación cualitativa y cuantitativa: consensos y disensos. Revista Digital de Investigación en Docencia Universitaria, 13(1), 102-122. doi: https://doi.org/10.19083/ridu.2019.644

Sota, D., Vargas, D. y Toro, J. (2021). Modelo de Políticas Estrategias y Controles que Permitan Minimizar los Riesgos para la Seguridad de la Información en la Nube Híbrida Existente en las Organizaciones. Colombia: Tecnológico de Antioquia. Disponible en: https://dspace.tdea.edu.co/handle/tdea/1946

Soto, C. y Ducuara, C. (2018). Protección de datos personales en los servicios de internet. Bogotá: Universidad Católica de Colombia. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/22521/1/Protección%20de%20Datos%20en%20los%20servicios%20de%20Internet.pdf

Vega, E. (2021). Seguridad de la información. España: 3Ciencias.

Viguri, J. (2021). La adopción de instrumentos de certificación como garantía eficiente en la protección de los datos personales. Revista catalana de dret públic, (62). Disponible en: http://repositori.uji.es/xmlui/handle/10234/194225

Vázquez, A. (2023, marzo 17). Lotus Sametime. Dealerworld.es. https://www.dealerworld.es/archive/lotus-sametime

Before you migrate from HCL Notes. (s/f). Google.com. Recuperado el 30 de marzo de 2023, de https://support.google.com/a/answer/154630?hl=en

Google : Security vulnerabilities. (s/f). Cvedetails.com. Recuperado el 30 de marzo de 2023, de https://www.cvedetails.com/vulnerability-list/vendor_id-1224/Google.html

IBM Lotus Sametime : List of security vulnerabilities. (s/f). Cvedetails.com. Recuperado el 30 de marzo de 2023, de https://www.cvedetails.com/vulnerability-list.php?vendor_id=14&product_id=10725&version_id=0&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=0&year=0&month=0&cweid=0&order=1&trc=18&sha=8da78431eefcee0579f1f08eedfc10911cf159b4

Regan, M. (2021, enero 29). How to migrate Emails from Lotus Notes to Google Apps workspace ? Bitrecover.com; BitRecover. https://www.bitrecover.com/blog/lotus-notes-to-google-apps/

US - IBM lotus Sametime standard V8.5. (2019, julio 11). Ibm.com. https://www.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_sm/3/897/ENUS5724-J23/index.html

SAP Security Notes and Fixes. (2023). SAP Support Portal. https://support.sap.com/securitynotes

Amazon Web Services. (2023). AWS Cloud Migration. https://aws.amazon.com/cloud-migration/

CVE DETAILS. (s.f.). *cvedetails*. Obtenido de https://www.cvedetails.com/vulnerability-list/vendor_id-797/cvssscoremin-9/cvssscoremax-/SAP.html

Gonzalez, G. (18 de Diciembre de 2018). *GenBeta*. Obtenido de https://www.genbeta.com/actualidad/ibm-vende-parte-sus-productos-software-a-hcl-technologies-1-800-millones-dolares

Google Cloud. (26 de Abril de 2023). *Google Cloud*. Obtenido de https://cloud.google.com/

HCL. (30 de Enero de 2023). *help.hcltechsw*. Obtenido de https://help.hcltechsw.com/sametime/welcome/index.html

IBM. (30 de Enero de 2023). *help.hcltechsw*. Obtenido de https://help.hcltechsw.com/sametime/12/meetings/c_client_user_guide.html

ACEI. (2020). La era de la información: Beneficios y retos en el tratamiento de los datos. Asociación Cultural de Estudios Internacionales.

Bowcut, J. (2021). Cyber threats to the food and agriculture sector. Food Safety Tech.

OPSWAT. (n.d.). Cyber security solutions. https://www.opswat.com/

Upwork. (n.d.). Enterprise security. https://www.upwork.com/hire/enterprise-security-freelancers

CSO. (2021). The benefits of an information security policy. https://www.csoonline.com/article/3384009/the-benefits-of-an-information-security-policy.html

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Pérez, J., & Rodríguez, M. (2018). Análisis de riesgos y vulnerabilidades en la seguridad de la información en una empresa de servicios financieros. [Tesis de grado, Universidad de La Sabana]. https://repository.ugc.edu.co/bitstream/handle/11396/3794/Protecci%C3%B3n_datos_personales_Colombia.pdf?sequence=1&isAllowed=y

Gómez, A., & Martínez, L. (2019). Evaluación de la seguridad de la información en una organización mediante la aplicación de la norma ISO/IEC 27001:2013. [Tesis de grado, Universidad Politécnica de Madrid]. https://core.ac.uk/download/pdf/55524565.pdf

Torres, C., & Vargas, D. (2020). Propuesta de un modelo de gestión de riesgos de seguridad de la información para la protección de datos personales en una empresa de telecomunicaciones. [Tesis de grado, Universidad del Rosario]. https://repository.urosario.edu.co/handle/10336/33832

Advanced-UK. (n.d.). Cyber Security: Integrating Risk and the CIA Triad. Advanced-UK Blog. Recuperado de https://blog.advanced-uk.com/blog/cyber-security-integrating-risk-and-the-cia-triad

KnowledgeHut. (n.d.). CIA in Cyber Security. KnowledgeHut Blog. Recuperado de https://www.knowledgehut.com/blog/security/cia-in-cyber-security

NIST. (n.d.). NIST Cyber Risk Scoring (CRS) - Program Overview. National Institute of Standards and Technology. Recuperado de https://csrc.nist.gov/CSRC/media/Presentations/nist-cyber-risk-

scoring-crs-program-overview/images-media/NIST%20Cyber%20Risk%20Scoring%20(CRS)%20-%20Program%20Overview.pdf

Euncet Business School. (2022). Beneficios de un plan estratégico de ciberseguridad. Recuperado de https://blog.euncet.com/beneficios-plan-estrategico-ciberseguridad/

Rubin, H., & Rubin, I. (1995). Entrevista cualitativa. El arte interpretar los datos. Nueva York:

Sage Publications, Thousand Oaks.

Hernán Feria Avila, M. M. (3 de julio de 2020). *Dialnet*. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=7692391

Advisera. (2023). ¿Qué es norma ISO 27001? Recuperado de https://advisera.com/27001academy/es/que-es-iso-27001/

DNV. (2023). 27001 Sistema de Gestión de Seguridad de la Información. Recuperado de https://www.dnv.com/ar/services/iso-27001-sistema-de-gestion-de-seguridad-de-la-informacion-3327

ISACA. (2012). COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. Rolling Meadows, IL: ISACA.