UNIVERSIDAD TÉCNICA DE BABAHOYO

Facultad de Administración, Finanzas e Informática

Escuela de Tecnologías de la Información y la Comunicación

Carrera de Ingeniería en Sistemas

TEMA

NORMATIVA ISO27001 COMO BASE EN LA GESTIÒN DE SEGURIDAD DE LA INFORMACIÒN DE LA CAMARONERA SANTA PRISCILA DE LA CIUDAD DE GUAYAQUIL.

ALUMNO

GARCÍA GÒMEZ JHON BRYAN

DOCENTE

ING. FREDDY MAXIMILIANO JORDÁN CORDONES

PERIODO ACADÉMICO

ABRIL 2024 – SEPTIEMBRE 2024

RESUMEN

Esta investigación se ha realizado en la camaronera Santa Priscila, de Guayaquil, una de las empresas más importantes del Ecuador y del mundo por ser una de las mejores en relación al camarón, esta se encuentra en el desafío de fortalecer su seguridad de la información como problemática, así como la protección de sus datos sensibles y estar preparada ante posibles interrupciones operativas, por lo que surge la necesidad de tener un enfoque adaptado a sus necesidades, es por ello que con la implementación de la ISO 27001 se conlleva a cultivar una cultura de tratamiento seguro de los datos.

Los objetivos de esta investigación han sido implementar un sistema de gestión de la información basado en normativa ISO27001 que permita una mejora en la seguridad de la información en la camaronera Santa Priscila de la ciudad de Guayaquil, los cuales se han logrado tras realizar aportes técnicos acompañados de políticas informáticas que se han elaborado apegados a normativas 27001 y con soporte además de la 27002 para estimar la eficiencia de sus controles.

Se ha elaborado en el capítulo V, una propuesta técnica de aplicación a partir de análisis anteriores y estudios donde se han evidenciado ciertos ajustes por realizar en cuanto a políticas para cuidado de la información, así como también se elaboraron nuevas políticas y se las ha socializado para mejorar el contexto de la seguridad de la información.

Se han evidenciado cambios importantes luego de aplicar políticas propuestas que fueron desarrolladas en el capítulo V, por lo que se reconoce que en una institución es esencial que se pueda contar con Sistemas de Gestión de la Seguridad de la información, y este sea implementado de acorde con la norma internacional ISO 27001, lo que permite un análisis completo del estado de la gestión de seguridad y permite evolucionar en el tratamiento de los riesgos de seguridad de los activos de información.

ABSTRACT

This research has been carried out in the Santa Priscila shrimp farm, in Guayaquil, one of the most important companies in Ecuador and the world for being one of the best in relation to shrimp, it is facing the challenge of strengthening its information security as problematic, as well as the protection of your sensitive data and being prepared for

possible operational interruptions, which is why the need arises to have an approach adapted to your needs, which is why the implementation of ISO 27001 leads to cultivating a culture secure data processing.

The objectives of this research have been to implement an information management system based on ISO27001 regulations that allows an improvement in information security in the Santa Priscila shrimp farm in the city of Guayaquil, which have been achieved after making accompanied technical contributions. of IT policies that have been developed in accordance with 27001 regulations and with support in addition to 27002 to estimate the efficiency of their controls.

In Chapter V, a technical application proposal has been prepared based on previous analyzes and studies where certain adjustments have been made to be made in terms of policies for the care of information, as well as new policies have been developed and have been socialized. to improve the context of information security.

Important changes have been evident after applying proposed policies that were developed in chapter V, which is why it is recognized that in an institution it is essential that it can have Information Security Management Systems, and this be implemented accordingly. with the international standard ISO 27001, which allows a complete analysis of the state of security management and allows evolution in the treatment of security risks of information assets.

PALABRAS CLAVE

NORMA ISO27001, ISO27002, Políticas informáticas, Seguridad de la información.

KEYWORDS

STANDARD ISO27001, ISO27002, IT policies, Information security.

INTRODUCCIÓN

En un panorama de los actuales momentos, marcados tecnologías y la interconexión apuntando a lo global, la seguridad de la información surge como una preocupación grande, tanto a nivel local como internacional, la creciente de ciberataques y la necesidad de proteger los datos sensibles hacen que este tema sea de vanguardia de en cualquier agenda empresarial y hasta gubernamental en todo el mundo, en tal sentido, la normativa ISO 27001 surge como una herramienta crucial en la defensa contra amenazas cibernéticas, ayudando con el establecimiento de estándares reconocidos internacionalmente para la gestión de la seguridad de la información.

La camaronera Santa Priscila, de Guayaquil, se encuentra sumergida en el desafío de su seguridad de la información como problemática, a medida que enfrenta esta problemática en cuanto a la gestión de la seguridad de la información, así como la protección de sus datos sensibles y una preparación ante posibles interrupciones operativas, surge la necesidad de tener un enfoque adaptado a sus necesidades.

Con la implementación de la ISO 27001 en esta empresa, no solo conlleva a cumplir con requisitos formales, sino que además permite cultivar una cultura de seguridad que proteja a todos los niveles de la organización en cuanto a datos e información.

En el sentido del cuidado de la información, la normativa ISO 27001 ha surgido como un estándar reconocido internacionalmente y ampliamente adoptado para poder establecer, implementar, mantener y hasta mejorar un Sistema de Gestión de Seguridad de la Información SGSI, su aplicación no solo que proporciona un marco sólido para proteger la información, sino que, también permite a las organizaciones cumplir con requisitos regulatorios y a fortalecerla ante posibles amenazas.

En la industria camaronera, donde es muy necesaria la información relacionada con la producción, logística y las relaciones comerciales, es vital y muy importante mantener una gestión efectiva de seguridad informática, por lo que adquiere una relevancia aún mayor; los desafíos específicos en cuanto proteger datos sensibles y la preparación ante posibles interrupciones operativas, la lleva a adoptar un enfoque integral y dinámico en su gestión de seguridad informática.

Esta investigación tiene como objetivo principal Implementar un SGSI basado en la ISO 27001, para mejorar la seguridad de la información en la camaronera Santa Priscila de la ciudad de Guayaquil, centrándose principalmente en la identificación de desafíos que enfrenta la empresa en el contexto de una evaluación del nivel de cumplimiento actual de la normativa mencionada y la proposición sus recomendaciones prácticas para fortalecerse frente a posibles amenazas y eventos negativos.

Para lograr este objetivo, con esta investigación, se hará un análisis exhaustivo de la situación actual de la empresa, basándose en datos anteriores del 2023 en cuanto a la gestión de seguridad de la información, así como un estudio nuevo detallado de los requisitos y principios que se establecen en la normativa ISO 27001 y a partir de esto, lograr identificar mejoras por lo que se propondrán soluciones prácticas que permitan a la camaronera Santa Priscila alcanzar un nivel óptimo de seguridad de la información, garantizando de esta manera su continuidad operativa y proteger sus activos más valiosos como lo es la información.

CAPITULO I.

1. PROBLEMA 1

1.1 Marco Contextual

1.1.2 Contexto Internacional

Contextualizar la seguridad informática, que es una inquietud mundial ante el aumento de número de ciberataques y la necesidad importante de resguardar datos sensibles, en un mundo interconectado cada vez más, la protección de la información y los datos se ha vuelto fundamental para garantizar una integridad y disponibilidad de los datos.

Las múltiples amenazas cibernéticas han destacado que es importante implementar medidas de seguridad sólidas en todas las empresas, tanto a nivel empresarial como personal y de gobierno, para mitigar los riesgos y salvaguardar la confidencialidad de la información, este escenario subraya la necesidad urgente de generar políticas y tecnologías eficaces para hacerle frente a estos desafíos de seguridad en una era tecnológica.

- La seguridad de la información se ha convertido en preocupación global por razones del aumento de ciberataques y la relevancia que tiene proteger datos sensibles.
- La normativa ISO 27001 es un estándar internacional, que ha sido reconocido para establecer sistemas de gestión de seguridad de la información SGSI.
- Organizaciones de todo el mundo están buscando implementar la ISO 27001 para proteger sus activos informáticos y cumplir requisitos regulatorios.

1.1.3 Contexto Nacional.

En el Ecuador, la seguridad informática se ve influenciada por la Ley Orgánica de Protección de Datos Personales, la que establece requisitos para salvaguardar la información de los ciudadanos y el aseguramiento de su privacidad, esta norma se hizo para regular el tratamiento de datos personales de parte de entidades públicas y privadas,

estableciendo obligaciones como obtener consentimientos para el manejar de datos y garantizar la confidencialidad.

En tal sentido, la implementación de normas tipo ISO 27001 se vuelve crucial, ya que proporciona un marco de trabajo reconocido a nivel mundial para establecer, implementar, mantener y mejorar sistemas gestión de seguridad de la información, adoptar estas normativas permiten a las organizaciones ecuatorianas a fortalecer sus mecanismos de seguridad y lograr cumplir con regulaciones vigentes y mantener protegida la información sensible de manera efectiva.

Sin embargo, existe una falta de concienciación acerca de la importancia de estas normativas acompañadas de inversión insuficiente en infraestructura y capacitación de personal, pueden ser una barrera ante su implementación efectiva en el país, por lo que es sumamente necesario promover una cultura de seguridad de la información con apoyo gubernamental y empresarial para abordar estos desafíos garantizado así la protección adecuada de los datos en el país.

1.1.4 Contexto Regional.

La región a la que pertenece Guayaquil, es reconocida por su gran actividad comercial e industrial, donde, además, la producción camaronera se destaca como uno de los principales sectores de exportación del país y de aporte al PIB, esta región es de constante aprovechamiento de los ríos que la rodean, así como con Santa Elena y las Islas Galápagos, lo que crea un entorno adecuado para su crecimiento; sin embargo, además, esto la vuelve un poco desafiante en términos de seguridad de la información.

Desde el punto de vista de la región, las normas ISO 27001 representan en las empresas camaroneras de la región un escudo que puede garantizar la protección adecuada de sus datos sensibles relacionados con la producción, logística y relaciones comerciales; sin embargo, es una tarea que posee obstáculos debido a la complejidad logística y una necesidad de adaptación de medidas de seguridad a condiciones específicas de la región y sus industrias.

La gestión efectiva de la seguridad de la información en la zona de Guayaquil requiere un enfoque integral ya que es un centro comercial e industrial del país e por sus características geográficas y ambientales que la hacen blanco de ciber ataques.

1.1.5 Contexto Local y/o Institucional

La empresa camaronera Santa Priscila, ubicada en Guayaquil, enfrenta desafíos específicos relacionados con la gestión de la seguridad de la información, por lo que se incluye la necesidad de proteger sus activos de información relacionados con la producción y lo comercial, puesto que los incidentes de seguridad de la información pueden verse con impacto directo en la reputación además de la continuidad del negocio a nivel local.

Con la implementación de normativas ISO 27001 en la camaronera Santa Priscila se aplica un enfoque institucional que involucra todos los niveles organizativos, desde la alta dirección hasta el personal operativo.

Es necesaria una capacitación de personal y asignación de recursos suficientes, así como el establecimiento de procesos y procedimientos claros son fundamentales también para tener éxito en la implementación de la ISO 27001, además del compromiso institucional con la seguridad de la información, no solamente para garantiza el cumplimiento de los requisitos, sino también para promover una cultura de seguridad organizacional.

1.2 Situación problemática

Inicialmente, se puede mencionar que la problemática es la exposición continua a la inseguridad relacionada con la información, al tener la mayor cantidad de procesos soportados sobre tecnologías y sistemas de información, estos se ven expuestos y no se cuenta con políticas ni regulaciones que permitan reducir los riesgos; han existido continuas interrupciones en las operaciones a causa de intrusiones y mala operación de sistemas, así mismo, se ha violentado en varias ocasiones las seguridades de la base de datos principal, siendo una clara muestra de un problema en la empresa.

La empresa camaronera Santa Priscila de Guayaquil se encuentra en una dinámica compleja tras tenido un crecimiento en los últimos 4 años, sin embargo, el haber aumentado su tamaño se relaciona a que ha logrado ser altamente competitiva, sin embargo existen procesos que son vulnerables y no permiten siempre un desempeño con eficiencia porque comúnmente se ven afectadas sus operaciones por la interrupción relacionadas con sus sistemas informáticos, se han detectado intrusiones para hacer caer los sistemas, se ha detectado malos manejos internos de parte de empleados para con sus sistemas y esto ha menguado su capacidad operativa en muchas ocasiones, teniendo claro que la seguridad de la información y los sistemas están siendo violentados.

La inexistencia de estándares de trabajo y la poca adopción en cuanto a políticas reales desarrolladas por expertos son un agujero a las amenazas cibernéticas y la aparición de eventos imprevistos con frecuencia, sumado a desastres naturales en etapas invernales y fallas técnicas por parte de empleados y sistemas. Este problema central, activa algunas situaciones complejas que repercuten en: lo financiero, lo cultural, la complejidad tecnológica, el cumplimiento normativo y la gestión de riesgos.

A pesar de la relevancia indiscutible de normativas como la ISO 9001 o la ISO 27001, la empresa Santa Priscila no posee investigaciones que le permiten evaluar su aplicación y efectividad frente a su ambiente como empresa. Existe una falta de análisis en lo que respecta a planificación y preparación ante interrupciones operativas, lo que pone en riesgo la integridad de la información manejada comprometiendo la continuidad del negocio.

Surge la necesidad urgente de investigar y realizar una comparativa exhaustiva entre lo analizado en el 2023, que dio un resultado no favorable en una auditoria parcial de seguridad informática donde se ha querido aplicar políticas apegadas al marco de la ISO 27001 para la gestión de seguridad de la información de la camaronera Santa Priscila de Guayaquil. Necesario en tal sentido identificar los desafíos específicos a que se enfrenta la empresa, y de esta forma evaluar su nivel de cumplimiento actual

Se puede indicar también, que la empresa camaronera Santa Priscila se encuentra en un punto complicado, donde la falta de un enfoque integral en su gestión de seguridad informática le podría poner en peligro a su estabilidad operativa y con ello la confianza de sus clientes.

1.3 Planteamiento del Problema

Anteriormente se han realizado auditorías a la seguridad de la información en la empresa santa Priscila, en el 2023; por diciembre de ese año, se determinó que tenía muchas vulnerabilidades que ponen en riesgo la operatividad y continuidad de la información, esto se puede observar reflejado en los anexos y se evidencia que se ha tratado de verificar con algunas guías proporcionadas por normativas ISO 27005 y 27002 para levantar y detectar vulnerabilidades, así como de establecer controles que no han servido de mucho, ya que nunca se realizaron políticas que permitan mitigar y evadir problemas con la seguridad.

En un marco creciente de complejidad y sofisticación de amenazas cibernéticas, así como de los posibles eventos negativos a los que conlleva, resulta necesario que la empresa de Santa Priscila adopte enfoques proactivos y eficientes en la gestión de la seguridad de su información, por lo que la normativa ISO 27001 puede ser una ayuda a la construcción de una defensa eficaz.

La gestión de la seguridad de la información es un aspecto fundamental para las organizaciones que buscan garantizar una confidencialidad sana, la integridad además de una disponibilidad de la información sensible, es así que, la empresa Santa Priscila de Guayaquil enfrenta desafíos significativos en cuanto a la planificación y preparación ante

situaciones de interrupciones operativas, lo que pone en riesgo su continuidad operativa y la seguridad de su información.

A pesar de la relevancia que tiene la normativa ISO 27001, hay una carencia en las auditorias que han evaluado su aplicación y efectividad en la empresa Santa Priscila, especialmente en lo relacionado con la planificación y preparación ante interrupciones operativas, ha habido una falta de enfoque integral que se adapte a las necesidades específicas de la empresa, por lo que la han colocado en riesgo por la falta de integridad de la información.

De esta manera, surge la necesidad de analizar de manera detallada cómo la implementación de la normativa ISO 27001 puede servir de base en la gestión de seguridad de la información de la camaronera Santa Priscila, centrándose especialmente en la planificación y preparación ante situaciones que incidan en interrupciones operativas.

1.3.1 Problema General

¿Cómo garantizar la seguridad de la información en la camaronera Santa Priscila de la ciudad de Guayaquil mediante la implementación de un Sistema de Gestión de Seguridad de la Información basado en la normativa ISO27001??

1.3.2 Problemas Derivados

Problema General: “Cómo garantizar la seguridad de la información en la camaronera Santa Priscila de la ciudad de Guayaquil mediante la implementación de un Sistema de Gestión de Seguridad de la Información basado en la normativa ISO27001.”

Por lo que se derivan los sub problemas específicos, donde se requiere un compromiso firme de la alta dirección, asignación adecuada de recursos, capacitación continua del personal y una planificación cuidadosa de la implementación del SGSI para garantizar que se adapte a las necesidades específicas de la camaronera Santa Priscila y cumpla con los estándares de la normativa ISO 27001:

Sub problema 1: No existen recursos suficientes para una inversión significativa en recursos financieros, tecnológicos y humanos para construir políticas apegadas a estándares ISO.

Sub problema 2: En la empresa no existe una cultura de seguridad de la información, por lo que esto exige cambios en las prácticas y comportamientos de los empleados, lo que puede encontrarse con resistencia interna o falta de conciencia sobre la importancia de la seguridad de la información.

Sub Problema 3: Montar sistemas de seguridad de la información es técnicamente compleja, especialmente porque la infraestructura tecnológica de la camaronera Santa Priscila no está actualizada o no es compatible con los requisitos de la normativa ISO 27001.

Sub Problema 4: Inexistencia de capacitación y concienciación del personal sobre los procedimientos y políticas de seguridad de la información, por lo que su proceder es desordenado en cuanto al tratamiento y cuidado de los datos en todos los niveles.

Sub Problema 5: El no apegarse a cumplimientos normativos, le impide lograr penetración comercial a más países; es un requisito fundamental la ISO27001, para construir confianza además de otras regulaciones considerando los cambios en la tecnología y las amenazas de seguridad.

Sub Problema 6: La mitigación del riesgo se ha vuelto un problema de seguridad de la información, se ha vuelto más compleja ya que no existen medios normativos que ayuden a disminuir amenazas; prevenir sería mejor que mitigar.

1.4 Delimitación de la Investigación

Esta investigación se centrará de forma específica en la aplicación de la ISO 27001 como base para la gestión de la seguridad de la información en la camaronera Santa Priscila de la ciudad de Guayaquil.

Este estudio se delimita a analizar cómo la implementación de esta normativa beneficia las prácticas de seguridad de la información en la camaronera, se investigarán datos anteriores para compararlos con los generados por esta investigación y de que forma la ISO 27001 se adapta con la generación de políticas y controles adicionales que deben existir con otras ISO, considerando su tamaño y estructura organizativa.

En términos de Tiempo: Se han estudiado datos del 2023, pero la aplicabilidad de la investigación será durante 2024.

En términos de contenido: Se centrará en gestión de la seguridad de la información en la camaronera Santa Priscila de la ciudad de Guayaquil y se analizará normativa de seguridad de la información ISO27001 para construir políticas que permitan mejorar seguridad y reducir vulnerabilidad.

En términos del Universo: Se realizará con una muestra de 68 empleados de la empresa.

En términos de Espacio: La camaronera Santa Priscila, ubicada en Av. Ejercito y Calle2, Guayaquil Ecuador.

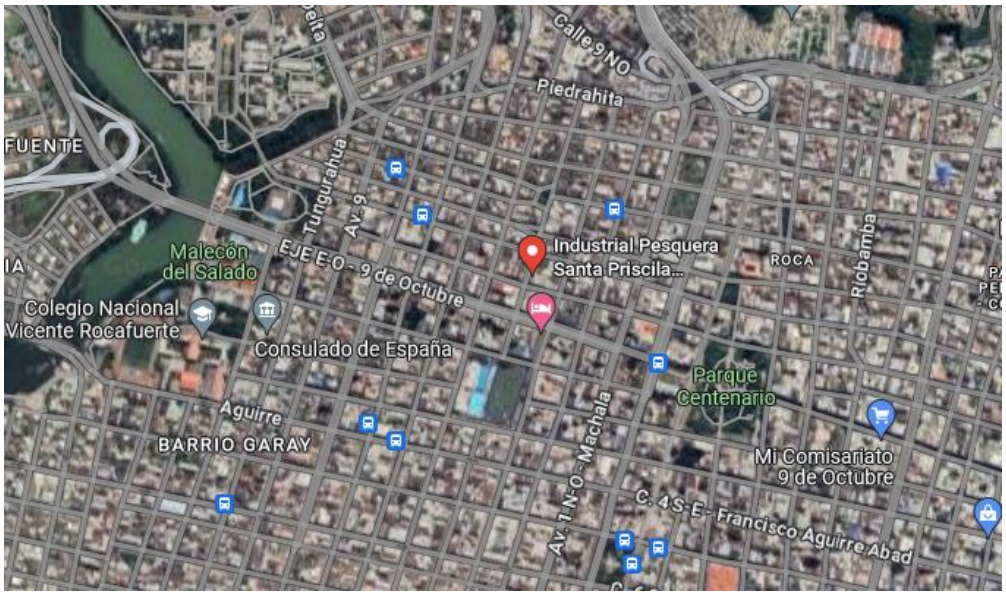


Imagen 1 : Ubicación de Camaronera Santa Priscila de Guayaquil

1.5 Justificación

Elegir la implementación de la normativa ISO 27001 como base en la gestión de seguridad de la información en la empresa Santa Priscila de Guayaquil se fundamenta en diversas razones que destacan la necesidad imperante de fortalecer la seguridad de la información y la resiliencia organizacional en un entorno empresarial cada vez más dinámico y desafiante por las amenazas.

La empresa Santa Priscila, al igual que muchas otras organizaciones, se enfrenta a riesgos y desafíos crecientes relacionados con la seguridad de la información. La proliferación de amenazas cibernéticas, la creciente sofisticación en los ataques y la posibilidad de interrupciones operativas por muchos motivos hacen imperativo que las empresas adopten medidas proactivas para proteger su información y garantizar la continuidad de las operaciones.

La ISO27001 se presenta en este documento como un marco de referencia reconocido internacionalmente que establece los requisitos para un Sistema de Gestión de Seguridad de la Información, la implementación de esta normativa proporciona un enfoque estructurado y sustancial para identificar, gestionar y mitigar riesgos de seguridad de la información, ofreciéndole a la empresa Santa Priscila herramientas integrales para abordar sus desafíos en este ámbito.

Además, esta investigación, no solo busca evaluar el nivel de cumplimiento actual de la empresa con la normativa ISO 27001, sino también proponer mejoras y recomendaciones específicas comparadas con evaluaciones anteriores alineadas con las necesidades y sus características particulares de la empresa, con esto se asegura que la implementación sea factible y adaptada a la realidad operativa y que los recursos además estén disponibles.

Implementar la normativa ISO27001 posicionará también a Santa Priscila como una empresa comprometida apegada a estándares internacionales de seguridad de la información, lo que puede le generar ventajas competitivas y fortalece su reputación de la empresa en el mercado internacional, además, su seguridad mejorada permitirá a la mantenerse con continuidad en sus operaciones inclusive en situaciones de interrupciones operativas, minimizando impactos y acelerando la recuperación.

1.6 Objetivos

1.6.1 Objetivo General

Implementar un sistema de gestión de la información basado en normativa ISO27001 que permita una mejora en la seguridad de la información en la camaronera Santa Priscila de la ciudad de Guayaquil.

1.6.2 Objetivos Específicos

1. Evaluar el nivel de cumplimiento de la camaronera Santa Priscila en relación con los requisitos establecidos por la ISO27001 en materia de seguridad de la información.
2. Consultar bases teóricas relacionadas con las normas ISO27001 que permitan implementar un (SGSI).
3. Estimar la eficiencia de los controles con las normas ISO 27002 en la empresa Santa Cecilia.

CAPITULO II

2. MARCO TEÓRICO

2.1 Marco teórico

Normativa ISO 27001: Fundamentos y Principios - Una Exploración Profunda

La normativa ISO/IEC 27001 surge fundamentalmente como una normativa internacional que permite desarrollar de una manera segura, vigorosa y confiable la gestión procedimental de la información administrada, o dicho de otro modo Sistemas de Gestión de Seguridad de la Información (SGSI). Johnson (2017) resalta en su postura de indagación que no es un mero hallazgo si no que establece de manera universal y globalizada los componentes decisivos de la protección de la información.

Esta normativa global que permite gestionar de manera segura la información nos provee de una serie de procedimientos que nos concede de una manera segura examinar y autentificar de forma autónoma la información. Esto nos posibilita afianzar con eficacia todos los datos sean estos de carácter económico o reservado de manera que no pueda ser vulnerados, disminuyendo las amenazas por factores externos asociados al manejo de datos.

La normativa ISO/IEC 27001 permite establecer la responsabilidad de cada uno de los usuarios de los datos sean estos de cualquier índole, permitiéndoles laborar con la información de manera preponderante y juiciosa garantizado la veracidad de los datos.

La norma afianza en su totalidad el aseguramiento de los datos de las instituciones y su operatividad confiable. Su trascendencia radica en la competencia al comprometerse al establecer una moldura organizada que permita el accionamiento administrativo de los sistemas de gestión de información corporativa de forma maleable.

La perspectiva general que plantea Smith (2018) de la valoración técnica, esta expresa una postura organizada y sensible, convirtiéndola en un dispositivo resolutivo que es adaptable al medio corporativo. En este sentido la normativa no solo se sitúa como una estructura normalizada, sino como un ente que catapulta la invulnerabilidad en las organizaciones en función de la gestión y operatividad de la información organizada (Culot, 2021)

Actualmente si analizamos detenidamente la norma podemos destacar su relevancia con relación a la vulnerabilidad de la información, es de prioridad establecer su esquema para su aplicación en los contextos organizacionales.

Su organización moldeable se evidencia en el accionamiento con eficiencia de los sistemas de gestión de seguridad de la información sin relacionar la tenacidad del sistema con los enfoques globalizados de vulnerabilidad de datos.

Estableciendo, además una diferencia en función de la responsabilidad y competitividad en el medio digital en transformación. Ante esto las instituciones que se acogen a la normativa ISO/IEC 27001 tienen como ítem importante la seguridad de los datos en ámbitos operativos funcionales. Esta norma es más que un compendio de lineamientos, es más bien un esquema fisionómico seguro de la información, que sirve como estrategia segura para la organización, gestión y utilidad de los datos de manera segura.

Etapas de Implementación de la ISO 27001

Implementar la norma ISO 27001 es un proceso muy minucioso pues este incluye diferentes fases, cada una ellas tienen desafíos específicos, de manera inicial, se puede decir que su alcance como sistema de gestión de seguridad de la información (SGSI) se consideró un componente clave. Según Turner (2019), se enfatiza en la necesidad de un alcance suficientemente amplio para lograr cubrir todos los medios de información relevantes, sin embargo, este alcance debe equilibrarse con los detalles necesarios para promover una gobernanza eficaz. Este proceso inicial no sólo sienta las bases para una implementación exitosa, sino que también da forma a la dirección estratégica de la seguridad de la información dentro de la organización.

La participación activa de las partes interesadas y la concienciación de los empleados son esenciales en esta etapa. La incorporación de opiniones y conocimientos de las partes interesadas garantiza que el alcance refleje con precisión la complejidad de los activos de información y los riesgos asociados. Además, la conciencia de los empleados crea una base sólida para la aceptación e implementación del SGSI en la cultura organizacional. La creación de un marco técnico que sea respaldado y comprendido por todos los niveles de la organización no sólo es fundamental para la

eficacia continua de un SGSI. La atención cuidadosa a estos aspectos en las primeras etapas de implementación sienta las bases para un sistema de seguridad de la información sólido y adaptable. (Giovanna Culot, 2021)

La norma ISO 27001 se implementa en escenarios dinámicos que requieren una gestión cuidadosa en todas las etapas del proceso. Desde el alcance hasta la capacitación del equipo de seguridad, existen desafíos específicos que requieren un enfoque estratégico. Este enfoque estratégico es esencial para superar los obstáculos y garantizar una implementación efectiva.

Además, la norma ISO 27001 reconoce la complejidad de la interacción entre los aspectos técnicos, humanos y organizativos. Este reconocimiento implica la necesidad de un enfoque holístico de la seguridad de la información que incluya todos estos aspectos. La eficacia de la norma ISO 27001 no se limita a la implementación de medidas técnicas de seguridad. De hecho, construir una cultura organizacional que valore y promueva la seguridad de la información es parte integral de su efectividad. Este enfoque integral no solo garantiza el cumplimiento normativo, sino que también mejora la capacidad de una organización para defenderse contra amenazas emergentes en el panorama de la seguridad cibernética.

El papel principal es la participación constante de la alta dirección y auditorías internas periódicas. Estos elementos son esenciales para mantener la eficacia y eficiencia de un sistema de gestión de seguridad de información por sus siglas SGSI, garantizando que una organización sea capaz de adaptarse a los cambios en el entorno de seguridad cibernética

La norma ISO 27001 no sólo proporciona un marco para la implementación de medidas de seguridad, sino que también promueve una cultura de seguridad de la información. Esta cultura está arraigada en todos los niveles de la organización y es fundamental para responder eficazmente a las amenazas de seguridad en evolución.

Controles de Seguridad de la Información según la ISO27001

Con relación al marco de la normativa ISO27001, el control de seguridad juega un papel fundamental para proteger los activos, mitigar riesgos, además de garantizar la confidencialidad, integridad y disponibilidad de datos e información sensibles, la importancia de estos controles puede ir más allá de sus aspectos técnicos y se establece

como base esencial para el funcionamiento confiable de los Sistema de Gestión de Seguridad de la Información SGSI de cualquier empresa.

González (2019) Apoya firmemente esta suposición y enfatizamos la importancia esencial de los controles en la protección de la información. Su investigación muestra que la implementación efectiva de controles específicos no solo ayuda a mitigar el riesgo, sino que también ayuda a construir una infraestructura de seguridad que aumenta la resiliencia de una organización ante las amenazas cibernéticas en evolución.

Este enfoque integral de la norma ISO 27001 considera los controles como elementos de estrategia, no solo como cumplimiento de estándares regulatorios. Estos controles no solo cumplen con las pautas, sino que también protegen de manera proactiva contra desafíos de seguridad de la información dinámicos y complejos. La investigación de González muestra cómo los controles bien implementados no solo protegen la integridad de los datos, sino que también ayudan a construir una cultura organizacional comprometida con la seguridad, donde todos comprenden y aprecian su papel en la protección de la información. Este enfoque holístico, respaldado por la investigación, enfatiza que la efectividad de los controles radica no sólo en su aplicación técnica, sino también en su integración con la naturaleza de la organización.(Normalización, 2022)

Dentro de la norma ISO/IEC 27001, los controles de seguridad son esenciales porque desempeñan funciones clave que protegen los activos, gestionan riesgos y garantizan la integridad, confidencialidad y disponibilidad de la información sensible dentro de una organización. Estos controles no son simplemente medidas técnicas, son las piedras angulares del funcionamiento confiable de un sistema de gestión de seguridad de la información por sus siglas (SGSI).

La investigación de González (2019) Enfatice la importancia crítica de estos controles para proteger la información y enfatice su papel en la construcción de una infraestructura de seguridad sólida. Esta infraestructura se basa no sólo en la tecnología, sino también en la cultura organizacional y la comprensión de la seguridad de la información.

La norma ISO/IEC 27001 define una serie de controles a implementar a través de políticas, procesos y procedimientos. Esta diversidad refleja la necesidad de una estrategia integral que cubra la seguridad de la información tanto digital como física.

Ciclo de Mejora Continua PDCA

El ciclo de mejora continua, conocido como ciclo PDCA que significa (Planificar-Hacer-Verificar-Actuar), este es un método que se ha probado ampliamente y ha sido utilizado para la mejora continua de procesos y productos a nivel organizacional en el mundo, Según Taylor (2018), este enfoque se formula tomando en consideración cuatro fases o etapas principales (planificación, ejecución, prueba y acción).

La esencia de este enfoque es su capacidad para lograr liderar a las organizaciones en la identificación de oportunidades, la implementación de estas mejoras incrementales y la adaptación continua a la dinámica del entorno de la empresa.

La fase de planificación, la organización define metas y objetivos claros, identifica áreas de mejora y desarrolla estrategias para abordar estas cuestiones, esta etapa es muy importante porque determina la dirección y los objetivos de las mejoras a implementar.

La Fase Ejecutar, incluye la implementación de un plan preparado y la implementación de las mejoras recomendadas en la práctica, durante esta etapa, las estrategias y planes se traducen en acciones concretas y comienza el proceso de cambio.

La fase de validación, en esta los resultados obtenidos se evalúan cuidadosamente para garantizar que cumplen con los objetivos planteados, se permite a la organización medir el éxito de las mejoras implementadas y determinar es que se han logrado cumplir las metas recomendadas.

Finalmente, en La fase de acción, se toman medidas en función sus resultados y estos se ajustan los procesos y estrategias según sean necesarios, aquí se permite a la organización aprender de los resultados y realizar los ajustes necesarios para una mejora continua.

Así, este ciclo PDCA se puede convertir en un mecanismo dinámico que impulsa el desarrollo continuo y fomenta una cultura de mejora continua en la organización, la estructura lógica y secuencial de estas fases permite a las organizaciones no solo responder de forma eficaz a los desafíos inmediatos, sino también además anticipar y adaptarse proactivamente a los cambios a largo plazo en el entorno empresarial (Taylor,

2018), esta adaptabilidad le es esencial en un mundo empresarial actual porque el cambio es constante y la capacidad de adaptación de una organización puede ser la clave de su éxito a largo plazo. (Taylor, 2018)

El ciclo de mejora continua, plasmado en el enfoque Planificar-Hacer-Verificar-Actuar (PDCA) es más que un simple proceso estructurado; es una filosofía que impulsa la adaptación organizacional y la mejora continua. La fase inicial de "planificación" enfatiza la importancia de la planificación estratégica como piedra angular del éxito de la mejora continua.

Este paso no sólo identifica oportunidades; también brinda importantes oportunidades para la innovación y la anticipación proactiva de los cambios en el entorno empresarial.

La interrelación entre las fases de "planificación" y "ejecución" revela una dinámica fundamental, una implementación efectiva está indisolublemente ligada a la calidad de la planificación, y el camino hacia una implementación efectiva se determina en la "fase de ejecución".

Roles y Responsabilidades en la Implementación de norma ISO27001

Durante la implementación de ISO 27001, es muy importante la definición de roles y responsabilidades para garantizar un Sistema de Gestión de Seguridad de la Información SGSI eficaz, por lo que se consideran los siguientes:

Auditor Interno de Seguridad, es responsable de evaluar y validar la efectividad de los controles de seguridad implementados, realiza auditorías internas para asegurar el cumplimiento de políticas y procedimientos.

Personal de la empresa, la implementación de un programa de seguridad de la información es una iniciativa de toda la organización, todos los empleados deben comprender su papel en la seguridad y seguir las políticas y procedimientos establecidos. (García et al, 2021)

Líder de Seguridad o Comisario, Consejo de Riesgos de Información y Administrador de Riesgos de Seguridad, este papel es el de un claro líder SGSI, su perfil y funciones pueden variar según el tamaño y la forma de la empresa, en algunas organizaciones pequeñas, la gestión de la seguridad puede compartirse con miembros de otras áreas como TI, ingeniería o jurídico.

Propietario de Control, es el responsable de monitorear y mantener los controles específicos del SGSI, donde cada control tiene un dueño específico.

Gestión de Riesgos y Continuidad del Negocio con normas ISO 27001

La protección de la información y sus elementos se regirán por la norma ISO/IEC 27001:2013, "un estándar global emitido por la Organización Internacional de Normalización (ISO) que detalla cómo administrar la seguridad de la información en una organización". Continuity y sus elementos se fundamentarán en la norma ISO/IEC 22301:2015, que es otro estándar global para administrar la continuidad del negocio; finalmente, se ajustará mediante un análisis de riesgos empresariales apropiado. Estos dos sistemas de gestión están vinculados con el riesgo.

El sistema de gestión que se basa en la norma ISO 31000:2018 es otro estándar global que proporciona directrices sobre cómo manejar los riesgos de acuerdo a sus principios, marcos de referencia y procesos, también se destacará la conexión entre ellos y la voluntad; este análisis se llevó a cabo con un enfoque multidisciplinario; en resumen, la integración puede realizarse a través de una estructura de alto nivel (Apéndice SL) que permite estandarizar la integración. Gracias a esta integración, lograremos un sistema de gestión unificado capaz de desempeñar funciones de salvaguarda de la información y mantener la continuidad de sus procesos en caso de interrupciones.

El propósito es establecer un sistema de gestión integrado multiestándar, que vincule la ISO 27001 centrada en la seguridad de la información, la ISO 22301 basada en la continuidad del negocio y la ISO 31000 enfocada en la gestión de riesgos. Esta coherencia de normas se aplicará en la empresa Paris & Asociados S.A.C.

La Organización Internacional de Normalización (ISO) declaró que: Para salvaguardar la información, es necesario implementar, mantener y mejorar las medidas de seguridad,

con el objetivo de asegurar que cualquier tipo de organización alcance sus metas y además garantice el cumplimiento de la legislación, mejorando la reputación y la imagen de la organización. (ISO,2017) La norma ISO 27001 es un estándar internacional emitido por la ISO, que propone un enfoque para gestionar la seguridad de la información en una organización.

De la misma manera, contiene los requisitos del SGSI. Forma parte de la familia de la ISO/IEC 27000. La ISO/IEC 27000 describe la visión general y el vocabulario de los sistemas de gestión de seguridad de la información, así como define los términos y definiciones asociados. Este estándar puede ser aplicado a cualquier tipo de empresa sin distinción de sector o tamaño. (GALLO, 2021)

La administración de la seguridad de la información se refuerza con las buenas prácticas que propone, y la norma ISO27002; para llevar a cabo el estudio, se plantean además el problema, los objetivos, la justificación y el alcance. Se toca la conceptualización, así como la descripción de la normativa de seguridad de la información en Ecuador. Se exponen las metodologías de análisis de riesgos más relevantes. El diseño del sistema de gestión comienza definiendo el alcance, la metodología de análisis de riesgos, el inventario de activos, la identificación de amenazas y vulnerabilidades, la evaluación de los riesgos, la implementación de los controles y la declaración de aplicabilidad.

Estos sistemas de gestión diseñados se convierten de esta forma en un instrumento para mejora específicamente y subir el nivel de madurez en seguridad de la información de una organización, asistiéndola en la reducción de los riesgos a los que está expuesta, y debe ser un pilar para establecer métodos orientados a la protección de activos informáticos.

La implementación y mantenimiento de un SGSI no sólo es responsabilidad del departamento de tecnología, sino de todos los empleados de la organización. Además, no existe ninguna limitación para el uso de los recursos de información, según una evaluación realizada que se basó en la norma ISO/IEC27001:2013, se ha determinado que existe un incumplimiento del 66%, con respecto a los 12 dominios.

- En (Imbaquingo Esparza & Pusdá Chulde, 2021), se indica que la implementación de la norma ISO 27001 es esencial para determinar el cumplimiento de los controles que garantizan la seguridad de la información

en cualquier tipo de organización. Las organizaciones no saben cómo gestionar la seguridad de la información.

- Según (Solarte Solarte, Enriquez Rosero 2020), el SGSI tiene como objetivo el establecer mecanismos de gestión para la confidencialidad, integridad y disponibilidad de la información esta adentrado en conjunto para poder calificar los niveles de seguridad. Su objetivo destacado principalmente es pode reconocer los activos y personas que están de acuerdo con el proceso de gestión de riesgos de sistemas de información que se emplean en procesos.

Identificación y evaluación de riesgos operativos

En un entorno empresarial verdadero, en constantes cambios y además competitivo, la gestión eficiente de riesgos es una herramienta de uso obligado que va a generar el éxito a largo plazo, su relevancia de la gestión de riesgos reside en su habilidad para lograr asistir a una empresa a prever y prepararse ante retos inesperados, y de esta forma minimizar pérdidas financieras y facilitar una toma de decisiones más profesional.

La identificación y evaluación de riesgos son etapas cruciales en cualquier enfoque, ya sea estratégico, operativo o de seguridad de la información. Es crucial planificar la respuesta al riesgo, que puede incluir la reducción, aceptación, transferencia o eliminación del riesgo. La comunicación y consulta con las partes interesadas, tanto internas como externas, es fundamental. Finalmente, estas tecnologías ayudan a disminuir la incertidumbre y permiten tomar decisiones basadas en información en una variedad de situaciones, garantizando la continuidad del negocio.

Conectar y optimizar el capital de gestión de activos de la empresa y las oportunidades de apalancamiento.

Los analistas de riesgos deben identificar y comprender la incertidumbre y cuantificar los diversos aspectos del riesgo. Las empresas de todo el mundo pueden agregar valor a sus servicios y mantener la sostenibilidad identificando la incertidumbre en sus procesos. La evaluación de riesgos de una empresa cubre áreas regulatorias, administrativas, de archivos, técnicas y organizativas.

Una gestión de riesgos deficiente o la ausencia de ella pueden provocar los siguientes problemas: definición poco clara del alcance del proyecto, planificación inadecuada de actividades y tareas, carencia de habilidades de gestión, visión empresarial restringida, incertidumbre en las inversiones, interrupciones imprevistas en el trabajo, resultados empresariales insatisfactorios, estabilidad limitada, optimización insuficiente de los procesos organizacionales, nivel de integración bajo, uso restringido de sistemas de información, planificación estratégica insuficiente y formación del personal inadecuada.

Se destaca esta investigación con la necesidad de administrar operaciones con riesgos ya que utiliza una metodología genérica para comprender e identificar las necesidades y expectativas de las partes interesadas. Por medio de una secuencia de etapas se propone abordar los riesgos y oportunidades en una organización, se inicia con la identificación de las fuentes, causas y consecuencias que puede ocasionar la materialización de un riesgo inherente, seguido de la valoración a través de un análisis cualitativo, cuantitativo, semicuantitativo o una combinación de estos, dependiendo de la herramienta que se prefiera utilizar.

Utilizando múltiples pruebas, se utiliza estrategias para poder gestionar o administrar los riesgos que puede cometer el sistema y así priorizarlos. Finalmente, se prosigue con el proceso de tratamiento del riesgo donde se modifican o implementan acciones frente al mismo para poder controlar la materialización de los riesgos o disminuir el impacto que podría causar en caso de que se materialice. (Tomás, 23 de agosto de 2019)

2.1.1 Marco conceptual

Importancia de la seguridad de la información. - La información es el activo más valioso de una empresa, es importante asegurarla, ya que su pérdida o alteración pueden causar inconvenientes operativos en las empresas.

Políticas informáticas de Seguridad de la información. – Son un conjunto de reglas y procedimientos bien estructurados que permiten mantener una forma y disciplina de trabajo enfocado en el buen cuidado de la información y los datos.

Norma ISO 27002.- Es un estándar internacional que proporciona guías de buenas prácticas para la gestión de la seguridad de la información

Área de tecnologías de la información TI : Es el área encargada de proteger los sistemas informáticos mediante prácticas y políticas específicas, utilizando herramientas como antivirus y firewalls.

Norma ISO/IEC 27001-2022: Establece requisitos para implementar un SGSI, usando el ciclo PVHA. La norma se divide en dos secciones: requisitos generales y un anexo con buenas prácticas.

Seguridad de la Información: Aplica medidas preventivas para garantizar la disponibilidad, confidencialidad e integridad de la información.

Implementación SGSI: Preserva la confidencialidad, integridad y disponibilidad de datos y sistemas según la norma ISO 27001.

Paso para Implementar un SGSI: Utiliza el ciclo PHVA, con fases de Planificación, Implementación, Revisión y Mantenimiento/Mejora.

Tabla 1. Fases de Implementación de un SGSI:

Fase	**Descripción**
Fase Diagnóstico	Comprender el estado actual de la empresa en seguridad de la información, identificando activos, procesos y riesgos asociados.
Fase Planificación	Determinar grupos de trabajo, plan de trabajo y asignación de responsabilidades para la implementación del SGSI.
Fase Implementación	Cumplir los objetivos establecidos durante la planificación, comparando los resultados obtenidos con lo planificado.
Fase de Evaluación y Monitoreo	Evaluar resultados que se han obtenidos durante la implementación del SGSI y diseñar un programa que permita el seguimiento para monitoreo de mejoras.
Fase de Identificación de Vulnerabilidades	Utilizar herramientas y Listas de Chequeo para identificar potenciales amenazas para el sistema, incluyendo vulnerabilidades físicas, de infraestructuras y conectividad.
Determinación de las Amenazas	Establecer la probabilidad de eventos que puedan dañar el sistema, clasificando las amenazas en diferentes categorías según su origen.

Fuente: El Autor, (2024)

Esta tabla proporciona una visión organizada y clara de las fases necesarias para implementar un SGSI, desde el diagnóstico hasta la determinación de amenazas, facilitando la comprensión y ejecución del proceso.

2.1.2 Antecedentes investigativos

Después de revisar las bases teóricas de varias bibliotecas universitarias, este documento puede ser considerado como una referencia a esta investigación, aunque no hay un trabajo previo sobre el tema: una propuesta de diseño para un SGSI que cumple con la norma ISO/IEC 27001.

Caso de investigación Marco Vinicio Guacanés Castro y Jonathan Alexander Vilatuña Morales son estudiantes de la escuela politécnica nacional, facultad de ingeniería de sistemas, y su trabajo de titulación es la creación de un modelo de un sistema de gestión de seguridad de la información por sus siglas (SGSI) basado en la norma ISO/IEC para la toma de decisiones en una empresa llamada Ultralink, las cuales se adaptan a las normas y estándares internacionales actuales para prevenir o reducir los riesgos de seguridad mediante procedimientos de tratamiento de riesgos y para lograr una gestión adecuada de los activos de información, se implementaron nuevas tecnologías que mejoran los procesos de la organización y la atención a los usuarios.

De esta manera, se ha encontrado una publicación titulada: Propuesta de Implementación de un Sistema de Gestión de Seguridad de la Información Basado en la Norma ISO 27001 para una Empresa de Telecomunicaciones, 2021, del autor Falcon Fernandez Junior Alejandro de la Universidad Nacional José Faustino Sánchez Carrión, en la Escuela Académica Profesional de Ingeniería de Sistemas. Su conclusión fue: La implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 para una empresa de telecomunicaciones.

Con base en datos estadísticos para el valor de prueba menos que el error, la implementación de un sistema de gestión de seguridad de la información basado en las normas ISO 2700 tiene un impacto en el número de incidentes de seguridad en la empresa de telecomunicaciones en 2021. En tercer lugar, el cumplimiento de los nuevos estándares establecidos para las empresas de telecomunicaciones 2021 se ve afectado por la implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 2700. Esto confirma el proceso de Spearman, que utiliza la prueba de Spearman para evaluar las similitudes entre los dos grupos.

Así mismo, se tiene como antecedente y material de consulta a la tesis de maestría del Ing. José Mejía Viteri, docente de la UTB, con el tema: Plan de seguridad informática del departamento de tecnologías de la información y comunicación de la universidad técnica de Babahoyo para mejorar la gestión en la confidencialidad e integridad de la información y disponibilidad de los servicios, donde su objetivo fue, Desarrollar un plan de Seguridad Informática del departamento de tecnologías de la información y comunicación de la Universidad Técnica de Babahoyo para mejorar la gestión en la confidencialidad e integridad de la información y disponibilidad de los servicios. (Mejía, 2015)

2.2 Hipótesis

2.2.1 Hipótesis general

Con un sistema de Gestión de Seguridad de la Información (SGSI) basado en la normativa ISO 27001 se logrará mejorar la seguridad de la información en la camaronera Santa Priscila de la ciudad de Guayaquil

2.2.2 Hipótesis específicas

1. Si se establecen controles adecuados y estrictos detallados como políticas de gestión de contraseñas conforme a los estándares de la normativa ISO 27001, se reducirán los riesgos de acceso no autorizados a los sistemas de información de la empresa Santa Priscila.
2. Si se realizan auditorías de seguridad periódicas y con procedimientos de monitoreo continuo relacionados con sistemas de información, siguiendo lineamientos ISO 27001, entonces se identificarán posibles vulnerabilidades y amenazas en la infraestructura tecnológica de la empresa.
3. Si se establece un programa de concientización para el personal sobre buenas prácticas de seguridad informática alineados a normativa ISO 27001, se fortalecerá la cultura de seguridad y se reducirán los riesgos asociados con errores humanos en la camaronera Santa Priscila.

2.3 Variables

2.3.1 Variables Independientes

Normativa ISO27001

2.3.2 Variables Dependientes

Gestión de seguridad de la información

2.3.3 Operacionalización de las variables

Tabla 2. Operacionalización de Variables

Variable	Definición Conceptual	Dimensiones	Indicadores	Escala de Medición
VI: normativa ISO 27001	Proceso de adoptar e integrar los requisitos y controles de seguridad establecidos por la normativa ISO 27001 en la estructura y operaciones de la camaronera Santa Priscila.	- Cumplimiento de requisitos: Extensión en la que la camaronera cumple con los requisitos específicos de la normativa ISO 27001. - Desarrollo de políticas y procedimientos: La creación y ejecución de políticas y procedimientos que se alinean con los estándares de la ISO 27001. - Capacitación del personal: El grado en que el personal es instruido y comprende los principios de seguridad de la información establecidos por la normativa ISO 27001.	- Porcentaje de requisitos cumplidos según auditorías internas. - Número de políticas y procedimientos implementados basados en la ISO 27001. - Resultados de evaluaciones de conocimiento y comprensión del personal sobre seguridad de la información.	Escala ordinal (porcentaje de cumplimiento, número de políticas implementadas, puntuación en evaluaciones de conocimiento).

VD: Gestión de seguridad de la información	Cambio positivo en las prácticas, procedimientos y resultados relacionados con la seguridad de la información como resultado directo de la implementación de la normativa ISO 27001.	- Reducción de incidentes de seguridad: Disminución en la frecuencia y gravedad de incidentes relacionados con la seguridad de la información. - Eficacia de los controles de seguridad: Mejora en la eficacia de los controles de seguridad implementados para proteger los activos de información de la camaronera. - Confianza del cliente: Incremento en la confianza y satisfacción del cliente respecto a la protección de sus datos personales y la seguridad de la información.	- Número de incidentes de seguridad reportados en un período de tiempo determinado. - tiempo medio de respuesta a incidentes de seguridad. - Puntuación en encuestas de satisfacción del cliente relacionadas con la seguridad de la información.	Escala nominal (número de incidentes), intervalos (horas para respuesta) y ordinal (puntuación en encuestas de satisfacción)

Fuente: El Autor, (2024)

CAPITULO III.

3. METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Método de investigación

Para este proyecto, se empleará principalmente el método inductivo, al que se lo caracteriza por analizar los datos específicos para poder formular teorías generales, este tiene que ver con recopilar una cantidad amplia de datos sobre un fenómeno o problema y luego identificar patrones o tendencias de aquellos, a partir de los cuales se puede elaborar hipótesis que expliquen dicho fenómeno o problemática, este se contrasta con el método deductivo, que parte de leyes o teorías generalizadas de estudios.

En cuanto a la metodología del proyecto, se utilizará un enfoque mixto entre metodologías cualitativas y cuantitativas. Se busca realizar un estudio desde la parte cuantitativa para identificar variables, instrumentación y medición que ayuden a determinar la vulnerabilidad y las fallas. Por otro lado, desde la metodología cualitativa se analizará el funcionamiento de la empresa, se busca con una combinación de ambas metodologías, la creación de un sistema de gestión sólido que refleje la realidad y el funcionamiento de la empresa.

3.2 Modalidad de investigación

En este caso, se utilizará un enfoque investigativo del tipo cuantitativo, debido a que existe la necesidad de recopilar datos numéricos en ciertos casos y de realizar además un análisis estadísticos sobre la población a estudiar, que en este caso son los empleados de la empresa camaronera Santa Priscila, esta investigación se centrará en la recopilación de los datos cuantitativos sobre la aplicación y eficacia que podría tener la normativa ISO27001 en la gestión de la seguridad de la información en esta empresa, motivo de esta investigación.

Así mismo, el estudio utilizará un muestreo aleatorio simple, es decir, se determina una muestra aleatoria de empleados que se seleccionan completamente al azar de una población total de calculada en 175 personas, este método proporcionará una representación aleatoria de la población, lo que puede permitir una generalización de resultados originada de los empleados de la camaronera.

Esta investigación seguirá un enfoque cuantitativo utilizando un simple muestreo aleatorio de recopilación de datos numéricos sobre cómo la empresa Santa Priscila y la implementación de la normativa ISO27001 para la gestión de su seguridad de la información.

3.3 Tipo de Investigación

Investigación de Campo:

- Dado que esta investigación está directamente relacionada con la situación específica de Santa Priscila, realizar una investigación de campo te permitirá recopilar datos de manera directa en el entorno real de la organización. Esto incluirá la interacción directa con el personal y la observación de procesos.

Investigación Documental:

- Esta investigación será además el tipo documental, ya que es una técnica cualitativa que consiste en recopilar y seleccionar información a través de la interpretación y documentos diversos, como libros, revistas, grabaciones, entre otros. Se utiliza en este proyecto para asociarse con la investigación histórica y ofrece beneficios como el análisis, la síntesis y la deducción de documentos.

- Lo más relevante de la investigación documental es la recolección y uso de documentos existentes para poder hacerles un análisis y ofrecer resultados con lógica. Se realiza de forma ordenada, con objetivos específicos, lo que facilita la construcción de nuevos conocimientos a partir de la información recopilada.

3.4 Técnicas e instrumentos de recolección de la Información

3.4.1 Técnicas

Las técnicas de recolección de datos incluirán la observación, que permitirá deducir y comprender los procedimientos reales dentro de la empresa, y la encuesta, que facilitará la comprensión a forma de diagnóstico inicial y así la revisión de la evolución acerca de la aplicabilidad de una propuesta relacionada con mejorar el ambiente de seguridad de la información con estrategias normativas.

Instrumentos de la investigación.

El instrumento que se utilizará es la encuesta, reflejada en el Anexo 1, este instrumento constituye un método de investigación para recopilar información de una muestra de 86 personas y se basa en la formulación de preguntas técnicas relacionadas con la seguridad de sistemas de información.

3.5 Población y Muestra de Investigación

3.5.1 Población

Se refiere al grupo total de individuos que tienen características específicas y que son relevantes para este estudio: 175 personas

3.5.2 Muestra

Muestreo Aleatorio Simple:

Se seleccionará una muestra de empleados de manera completamente aleatoria. Cada empleado tiene la misma probabilidad de ser seleccionado, este método será útil ya que cada miembro de la población tenga una oportunidad igual de ser incluido en la muestra.

Z=	**1,96**
p =	**92%**
q =	**8%**
N =	**175**
e =	**5,0%**

Donde:

Z =	nivel de confianza (correspondiente con tabla de valores de Z)
p =	Porcentaje de la población que tiene el atributo deseado
q =	Porcentaje de la población que no tiene el atributo deseado = 1-p Nota: cuando no hay indicación de la población que posee o nó el atributo, se asume 50% para p y 50% para q
e =	Error de estimación máximo aceptado
n =	Tamaño de la muestra

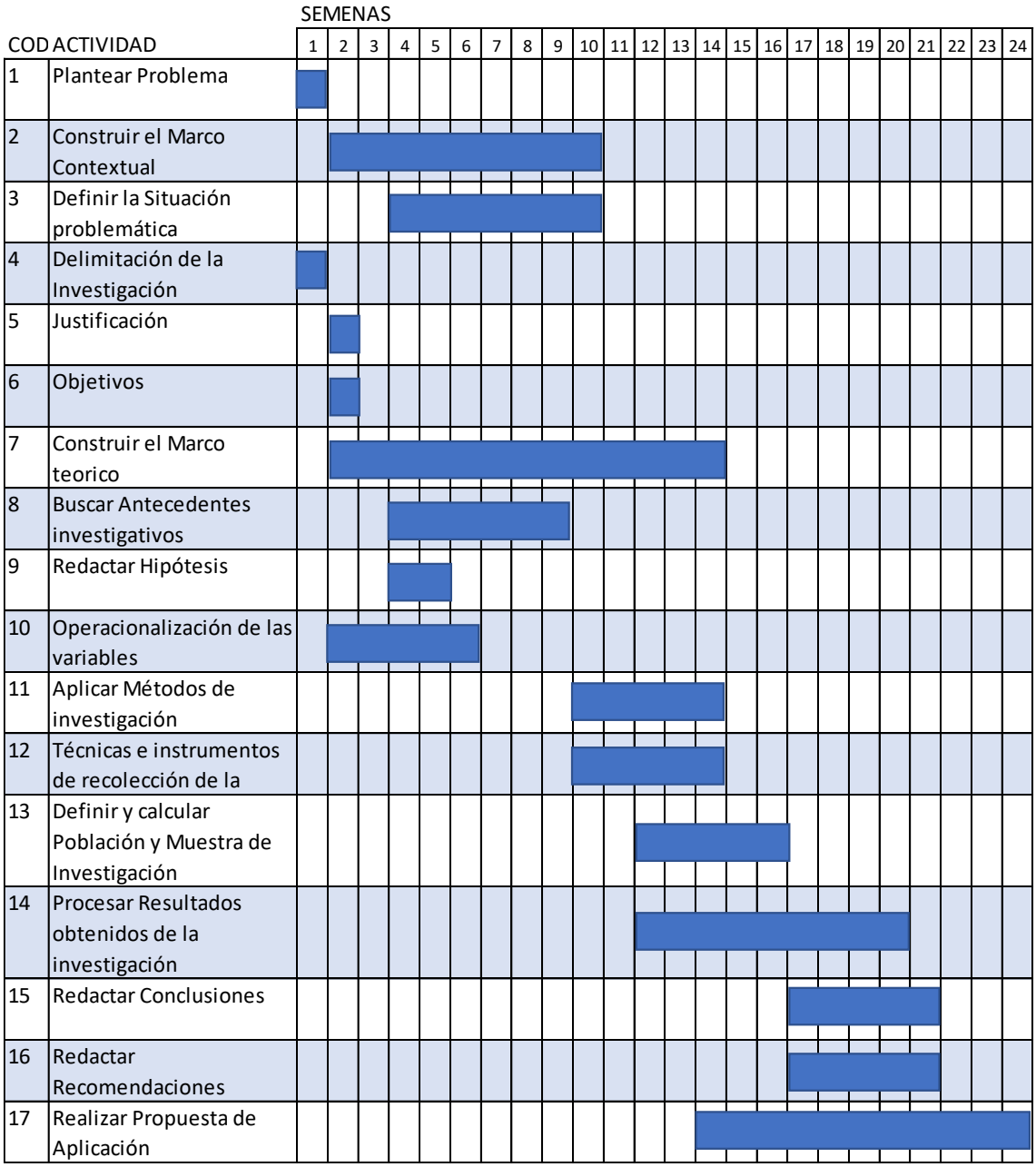
$$\frac{Z^2 * N * p * q}{e^2 * (N-1) + (Z^2 * p * q)}$$

$$\frac{3{,}84 \times 175 \times 92\% \times 8\%}{0{,}003 \times (174) + (3{,}84 \times 92\% \times 8\%)}$$

$$\frac{49{,}48}{0{,}72}$$

Muestra: **68**

3.6 Cronograma del Proyecto



3.7 Recursos

3.7.1 Recursos humanos

Para el presente trabajo, el recurso humano que se dispone es únicamente el autor, que tendrá el rol de investigador, tomar muestras y recopilar información, así como investigar todo lo relacionado con antecedentes de auditoría.

3.7.2 Recursos económicos

Tabla 3. Cuadro de Gastos

Recurso / Gasto	Descripción	Monto Aprox
Material de Oficina	Papelería, cartuchos de tinta, material de escritura, etc.	300
Equipamiento tecnológico	Adquisición de computadora, software de ofimática, impresora.	2400
Acceso a Bibliotecas	Suscripción a bases de datos académicas y herramientas de investigación en línea.	300
Viajes para investigación	Costos de transporte, alojamiento y manutención para visitas a Babahoyo y Traslado a Guayaquil donde resido	250
Impresiones	Impresión de documentos, y copias	200
Como un indirecto, Honorarios de Asesores	Honorarios a asesores o tutores académicos por su tiempo y orientación durante la investigación	1200
Extras	Otros gastos relacionados con la investigación	400
	Total	**5050**

3.8 Plan de tabulación y análisis

Tabla 4. Plan de tabulación de datos

Pregunta # 1, Formulación de pregunta		
Alternativa	*Frecuencia*	*Porcentaje*
dato	*dato*	*dato*
Total	*Valor Entero*	*Porcentaje*

La forma de recopilar será con el instrumento encuesta, estas se tabularán y organizarán será de acuerdo a la Tabla 4.

Así mismo, otra representación que se realizará en esta investigación y que será de gran ayuda es el grafico de barras donde cada barra refleja el porcentaje encontrado de cada pregunta recopilada con la encuesta.

3.8.1 Base de datos

La organización que se tendrá a partir de los datos recopilados en la encuesta, formará una base de datos que permitirá realizar el análisis, esta se forjará utilizando la aplicación Excel que permite realizar búsquedas y organizar los datos para luego ser trasladada a otras aplicaciones de análisis.

Es decir, luego de encuestar se guardará en la base de datos que se realizará en Excel para mantener organizados y preparados los datos para un posterior análisis y que estos se puedan convertir en información útil para la investigación.

3.8.2 Procesamiento y análisis de los datos

Para procesar y analizar datos, se utilizará la base de datos conformada en Excel, y se realizarán análisis con tablas dinámicas, de la misma forma se apoyará con la utilización de SPSS 26.0, un reconocido paquete estadístico que permite determinar y gestionar datos para producir información estadística relevante y eficiente en el mejor tiempo posible.

Los datos a obtenerse en su totalidad con la encuesta son numéricos, por lo que es necesario utilizar aplicaciones como Excel y SPSS 26.0 para mejorar la interpretación y generar una mejor comprensión.

CAPITULO IV

4 RESULTADOS DE LA INVESTIGACIÓN

4.1 Resultados obtenidos de la investigación

En relación a la investigación plasmada con un instrumento encuesta, se han obtenido los resultados siguientes:

Fecha de toma de datos: **14 de diciembre del 2023**

Tabla 3. **Resultado de: Tiempo laborando en la empresa**

	FRECUENCIA	PORCENTAJE
Menos de un año	4	6%
1 año	12	18%
Mas de 1 año	52	76%
	68	**100%**

Gráfica 1. **Resultado de: Tiempo laborando en la empresa**

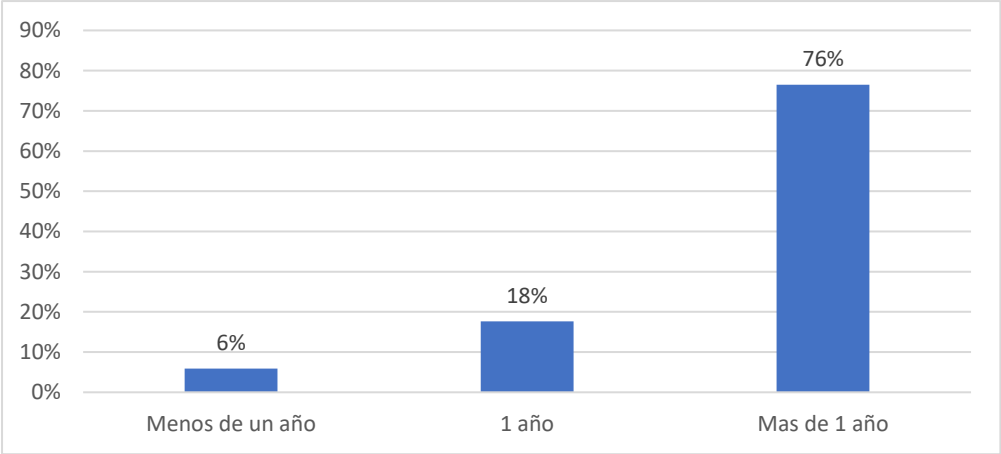


Tabla 4. En relación al cuidado de los datos en la empresa

	FRECUENCIA	PORCENTAJE
No he recibido	22	32%
Una vez al año	16	24%
Dos veces al año	30	44%
Mas de dos veces al año	0	0%
	68	**100%**

Gráfica 2. **En relación al cuidado de los datos en la empresa**

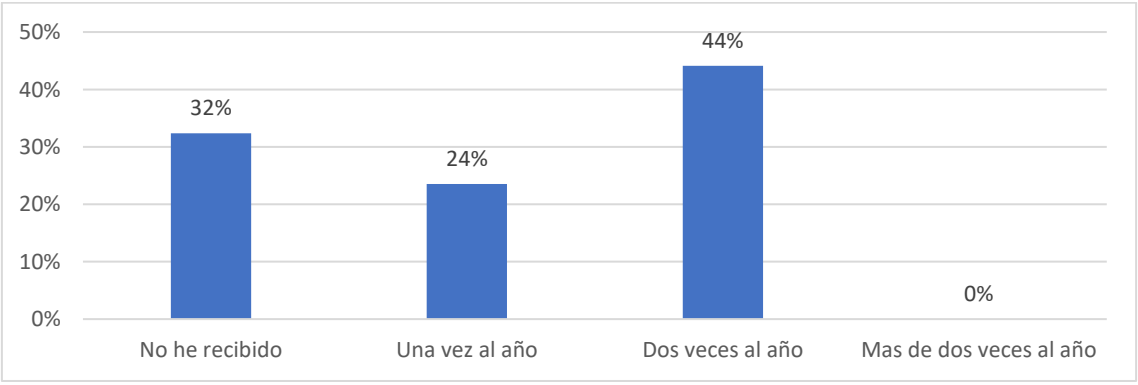


Tabla 5. En relación al conocimiento de políticas y procedimientos que permitan cuidar datos en la empresa

	FRECUENCIA	PORCENTAJE
Si	2	3%
No	66	97%
	68	100%

Gráfica 3. En relación al conocimiento de políticas y procedimientos que permitan cuidar datos en la empresa

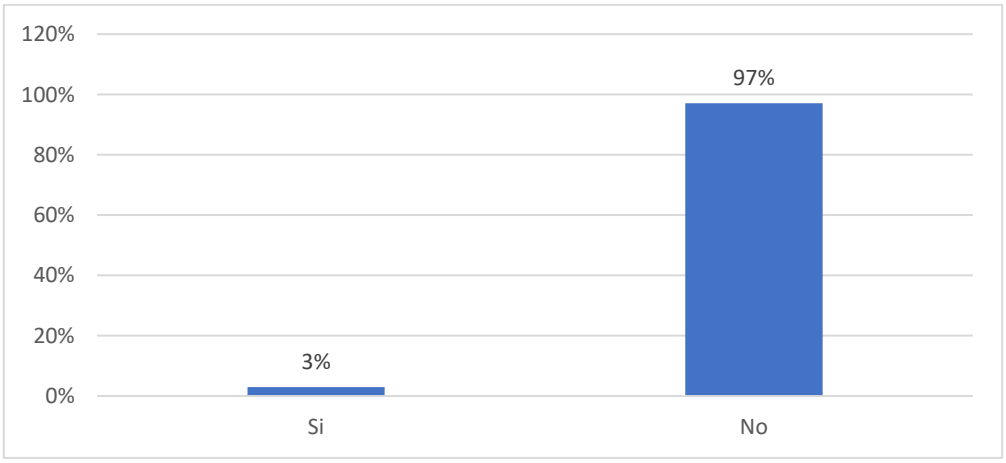


Tabla 6. En relación a que si utiliza sistemas informáticos para alguna actividad en la empresa

	FRECUENCIA	PORCENTAJE
Si	45	66%
No	23	34%
	68	100%

Gráfica 4. En relación a que si utiliza sistemas informáticos para alguna actividad en la empresa

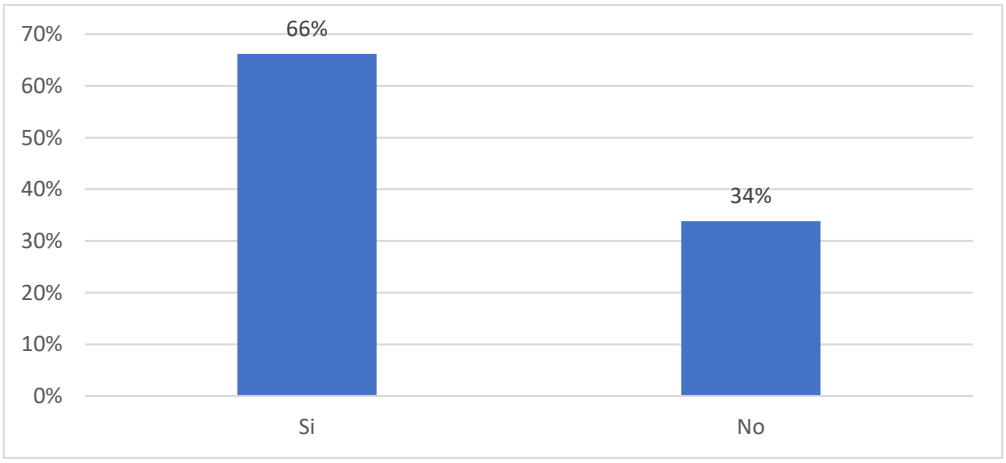


Tabla 7. En relación al tiempo de cambio de contraseñas de acceso a los sistemas de la empresa

	FRECUENCIA	PORCENTAJE
No la ha cambiado	34	50%
Cada mes	0	0%
Cada tres meses	0	0%
Cada año	3	4%
No recuerda	31	46%
	68	**100%**

Gráfica 5. En relación al tiempo de cambio de contraseñas de acceso a los sistemas de la empresa

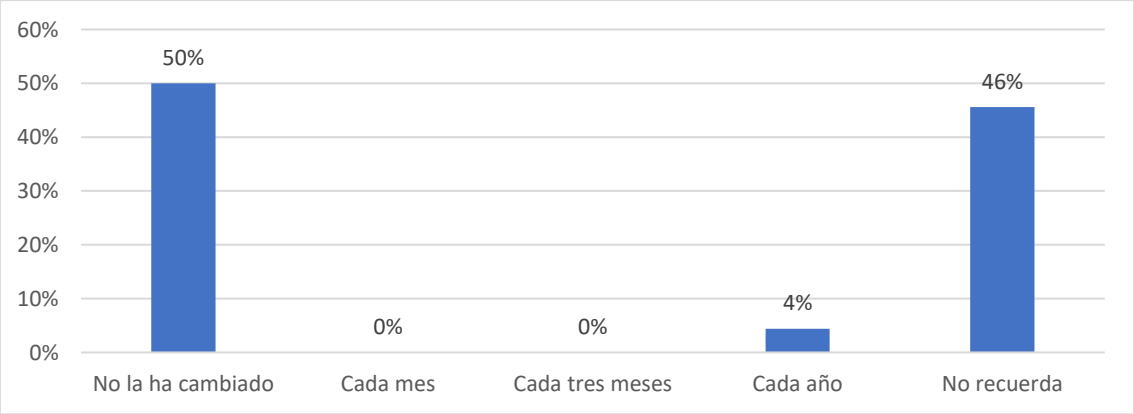


Tabla 8. En relación a compartir contraseñas con algún compañero del trabajo

	FRECUENCIA	PORCENTAJE
Si	43	63%
No	25	37%
	68	100%

Gráfica 6. En relación a compartir contraseñas con algún compañero del trabajo

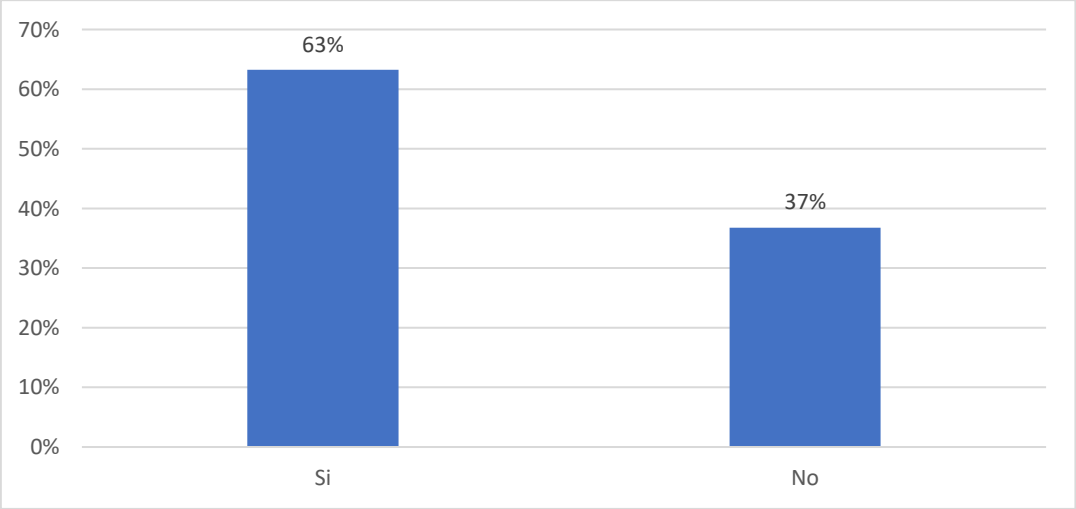


Tabla 9. En relación a que se proporciona recursos tecnológicos donde con estos se puedan proteger información confidencial

	FRECUENCIA	PORCENTAJE
Si	56	82%
No	12	18%
	68	100%

Gráfica 7.–En relación a que se proporciona recursos tecnológicos donde con estos se puedan proteger información confidencial

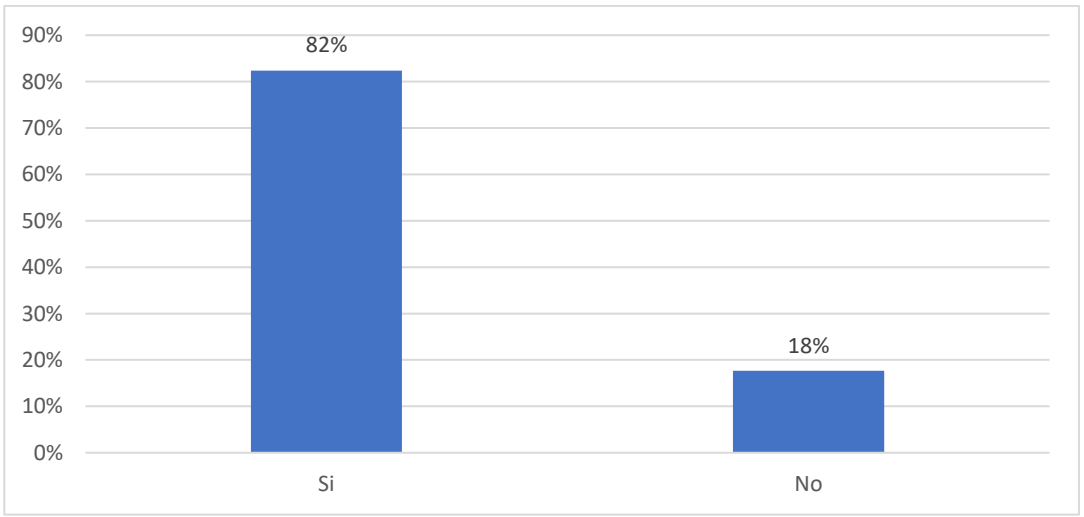


Tabla 10. En relación a correos electrónicos sospechosos en la cuenta de mail empresarial o la personal

	FRECUENCIA	PORCENTAJE
Los recibí, pero no los reporte	34	50%
No los recibí	22	32%
Si recibí y si reporté	12	18%
	68	100%

Gráfica 8. En relación a correos electrónicos sospechosos en la cuenta de mail empresarial o la personal

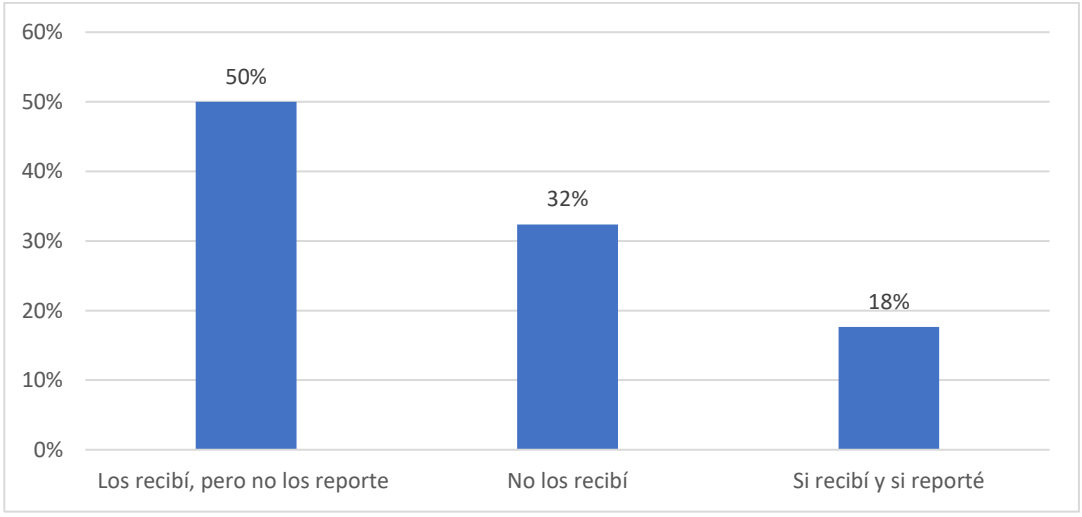


Tabla 11. En relación a reglas o políticas a seguir y los cuidados de la información y datos de la empresa

	FRECUENCIA	PORCENTAJE
Si	17	25%
No	51	75%
	68	100%

Gráfica 9. En relación a reglas o políticas a seguir y los cuidados de la información y datos de la empresa

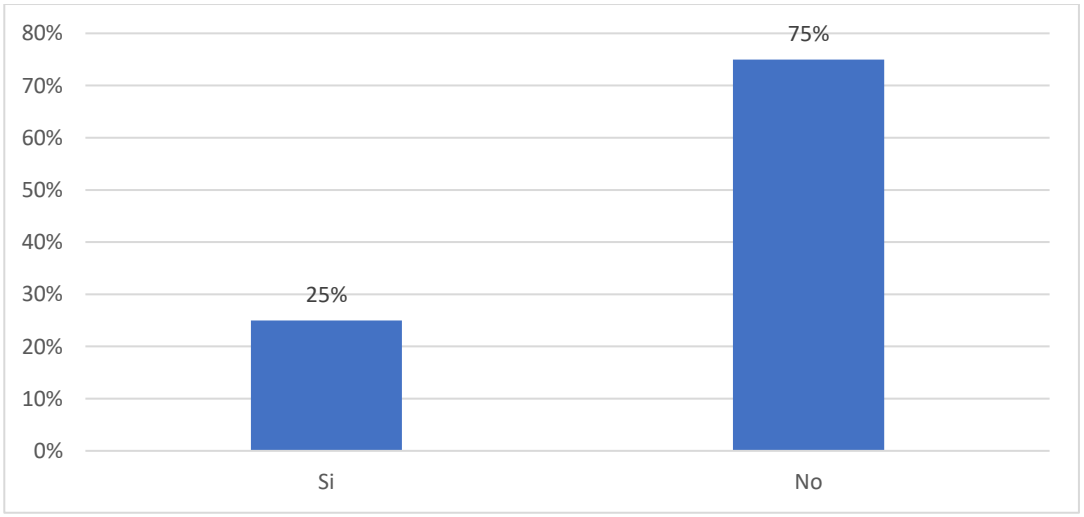
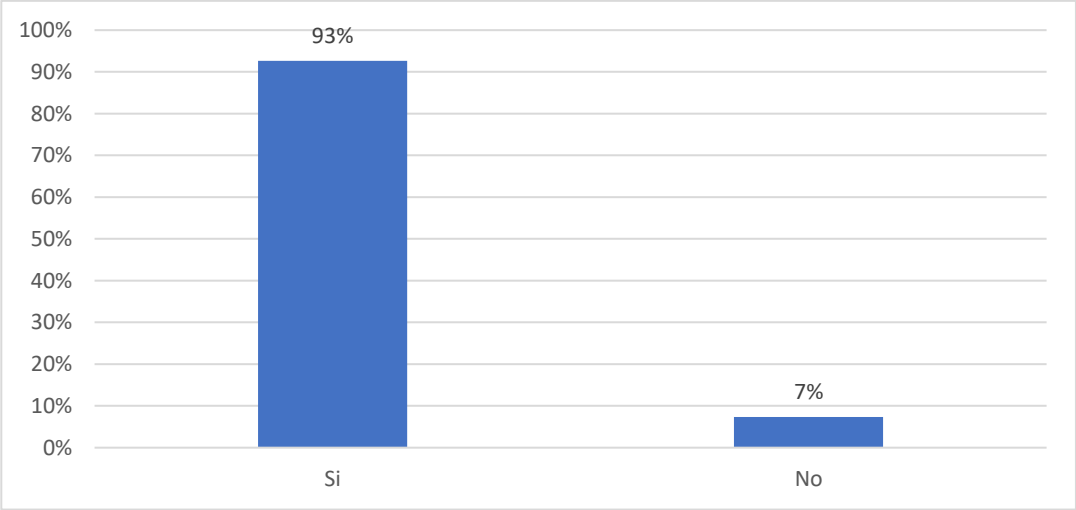


Tabla 12. En relación a si está al tanto de consecuencias graves de no seguir las políticas de seguridad informática de la empresa

	FRECUENCIA	PORCENTAJE
Si	5	7%
No	63	93%
	68	100%

Gráfica 10. En relación a si está al tanto de consecuencias graves de no seguir las políticas de seguridad informática de la empresa



4.2 Análisis e interpretación de datos

En cuanto al análisis de la encuesta, en su primer resultado, se puede notar claramente reflejado en las respuestas que la mayoría tienen un año o más laborando en la empresa, lo que constituye un precedente bueno y confiable para desarrollar la investigación y se apliquen lo resultados de forma eficiente.

Así mismo, cuando se responde a cada cuanto recibe capacitación relacionada con informática y cuidado de los datos en la empresa, han respondido que el 44% la recibe par de veces al año, 24% solo una vez; por lo que se puede reflejar que se está capacitando a un cierto grupo de personas en temas de interés particulares, es decir únicamente el 68% recibe formación específica en temas informáticos y el resto supone no estar inmiscuido en temas inherentes a informática.

En relación a que, si sabes si existen políticas y procedimientos que permitan cuidar datos en la empresa, han contestado en su mayoría que no, y supone han realizado un análisis de auditoría de seguridad de la información el año pasado, donde los productos debieron ser reflejados en una forma más positiva, pues es preocupante que solamente el 3% conozca de aquello y que particularmente sean los del área de tecnologías. Esto refleja que solo existe preocupación por procesos basados en lo comercial y muy poco por lo que se relaciona con la seguridad y la tecnología, representando en si una fuerte vulnerabilidad.

En cuanto se ha preguntado del uso de sistemas informáticos para alguna actividad en la empresa, se ha respondido en su mayoría que sí, esto es un 66%, considerado alto porcentaje de penetración tecnológica, se entiende que para algunas fases de la cadena de producción esto se realiza con tecnología la forma como se realiza y se comunican entre diferentes instancias y procesos de producción, lo que obliga al uso de sistemas informáticos por más mínima que sea la actividad, lo que compromete a que se tomen medidas para fortalecer procedimientos de utilización y así se reduzca la incidencia de inseguridad que pueda existir en cuanto a los datos.

En el contexto de cambios de las contraseñas de acceso a los sistemas de la empresa, es alarmante que el 50% no la ha cambiado y el 46% no recuerda haberlo hecho,

lo que preocupa porque es una vulnerabilidad grande el no hacerlo y toda norma o política incluye un cambio periódico de contraseñas para mejorar la seguridad, de no hacerlo se corre rasgos hasta del lado del usuario de ser inclusive culpados de algún mal procedimiento o incidir en fuga de datos o mala manipulación.

En relación a que la empresa le proporciona el suficiente recurso tecnológico como computadoras, software, tablets, donde con estos se pueda proteger información confidencial, han respondido el 82% que si, esto representa algo positivo, porque se puede implementar políticas estandarizadas que permitan aprovechar el despliegue tecnológico que existe en la empresa y preparar al personal en el manejo eficiente de los datos y de esa forma se establezcan disciplinas sostenidas.

En el contexto de los correos electrónicos, de si han recibido durante los últimos tres meses correos sospechosos en la cuenta empresarial o personal y si estos ha sido reportados, se tienen resultados de 50% que los han recibido sin reportarlos, por pensar inclusive que es algo normal o puede tratarse de spam común; así mismo no han recibido el 32% y han reportado únicamente el 18% siendo esto un efecto que puede tomarse como riesgoso, aunque también se pudo haber profundizado en cuanto a que si lo abrió y sucedió algo raro luego de apresurarlo; sin embargo no deja de ser una vulnerabilidad un poco elevada este reflejo.

En cuanto a si les han indicado a los empleados de algunas reglas o políticas a seguir en relación a los cuidados de la información y datos de la empresa, estos contestaron el 75% no conocer alguna política relacionada, el 25% si, y en el contexto de seguridad informática como se contaba antes, la política va antes de la tecnología, aquí existe tecnología, pero si no existe la política puede verse comprometida la información y operaciones comerciales importantes

Es preocupante conocer que el 93% no está al tanto de consecuencias graves de no seguir las políticas de seguridad informática de la empresa, lo que puede acarrear consecuencias graves en cuanto al manejo de la información, pues manejan bastantes

dispositivos tecnológicos para cada instancia de la cadena productiva dentro de la organización.

4.3 Conclusiones

El primer diagnóstico relacionado con la capacitación relacionada con informática y cuidado de los datos en la empresa, ha reflejado un cambio, luego de haberse aplicado políticas informáticas pues se ha capacitado casi al 100% del personal, se evidenció un cambio importante, al menos ya se ha sentido que han tenido una capacitación inclusive personal poco relacionado con sistemas de información.

El no conocer o poseer lineamientos puede incidir de forma negativa, por lo que el personal debe conocer que la información, junto con los sistemas informáticos y los procesos, son activos cruciales, y para mantener niveles de conformidad, competitividad e imagen empresarial, es necesario garantizar que la información sea confidencial, disponible e integral.

Es necesario que se establezcan periodos de revisión de políticas y procedimientos que permitan proteger la información; varios procesos siguen políticas ineficientes que dificultan el cumplimiento aceptable, lo que dificulta garantizar la confidencialidad, integridad y disponibilidad de la información.

Se han evidenciado cambios importantes luego de aplicar políticas propuestas que fueron desarrolladas en el capítulo V de esta investigación, por lo que se reconoce que en una institución es esencial que se pueda contar con Sistemas de Gestión de la Seguridad de la información, y este sea implementado de acorde con la norma internacional ISO 27001, lo que permite un análisis completo del estado de la gestión de seguridad y permite evolucionar en el tratamiento de los riesgos de seguridad de los activos de información.

El análisis realizado con datos del año 2023 y 2024 ha permitido identificar la probabilidad e impacto de los riesgos a los que se pueden enfrentar los activos de información, lo que nos ha permitido utilizar los controles necesarios que nos brinda la norma aplicada y así prevenirlos. La encuesta realizada mostró los efectos de no emplear sistemas de SGSI o políticas informáticas que protejan la confidencialidad, disponibilidad e integridad.

Así mismo, se concluye, además, que se ha cumplido el tercer objetivo específico, al estimar la eficiencia que además se ha tenido con el soporte de normas adicionales como la ISO27002, que en conjunto con la 27001, han permitido elaborar unas políticas de seguridad de la información que están propuestas en el capítulo V de esta investigación.

4.4 Recomendaciones

La empresa camaronera Santa Cecilia de Guayaquil debe despertar el interés y el compromiso de la alta dirección para apoyar al departamento de TICS y proporcionar los recursos necesarios para llevar a cabo la puesta en marcha de un Sistema de Gestión de la Seguridad de la Información SGSI de forma integral, o en su totalidad, ya que la seguridad de la información es un pilar muy importante hoy en día para todo tipo de entidades.

Al gerente de la empresa, se le recomienda establecer un comité de seguridad en el departamento de TI y nombrar un responsable que se encargue de administrar la seguridad de la información, así como además supervisar el cumplimiento de las políticas y controles de seguridad y supervisar el manejo efectivo de los activos informáticos.

Además, es importante que cada cierto periodo se revisen las políticas recomendadas en el capitulo V, ya que las tecnologías enfrentan cambios frecuentes y estas deben ser revisadas y perfeccionadas acorde a las variaciones o actualizaciones de la ISO27001 o ISO27002, por lo que se recomienda de ser posible, contratar a un personal en el área de sistemas que tenga el conocimiento y las competencias necesarios para realizar la seguridad de la información y, por lo tanto, evitar la contratación de consultores externos.

Se recomienda también, al departamento de TI, aumentar el alcance con los controles de la norma ISO27001 y 27002 actuales, y hacer un seguimiento a las políticas de seguridad propuestas.

Es recomendable también que se apliquen las propuestas que se han elaborado en el siguiente capitulo V, estas permitirán una mejor gestión de la seguridad de la información y el cuidado de los activos informáticos.

CAPITULO V

5 PROPUESTA TEÓRICA DE APLICACIÓN

5.1 Título de la Propuesta de Aplicación

Política informática con controles complementarios a la norma ISO27001 estimando la eficiencia de los controles con la norma ISO27002 en la empresa Santa Cecilia para fortalecer la seguridad de la información.

5.2 Antecedentes

En la versión actual de la norma internacional ISO 27001, que se mantiene desde el 2013, se reúnen los recursos necesarios para llevar a cabo una política, sin embargo, en enero de 2022 apareció una nueva norma que establece los controles adecuados para las necesidades de la organización.

Para crear confianza a las partes interesadas, se busca proteger todos los activos que se mantienen dentro del alcance de la norma, lo que permitirá la implantación, supervisión, mantenimiento y mejora del sistema con el tiempo, es el conjunto de medidas preventivas o reactivas que protegen la información de las entidades de los ataques cibernéticos, el uso, la divulgación y la alteración no autorizada; esto se hace para garantizar que la información sea segura, confidencial y accesible.

La seguridad de la información abarca la protección de sistemas, recursos, información y activos contra el acceso o uso no autorizado, catástrofes o errores, para reducir el riesgo y las consecuencias de incidentes de seguridad de la información; la nueva versión 2022 de la norma ISO 27002 también ayuda a proteger los activos de información mediante la implementación de políticas de seguridad; esto evita los accesos no autorizados por usuarios o terceras personas y reduce los daños físicos y ambientales, para realizar esto, se realiza un análisis de requerimientos con el apoyo de tecnologías, con el fin de realizar de manera efectiva los controles.

Los procedimientos y técnicas para la gestión de la seguridad de la información serán establecidos, registrados y aplicados en la práctica, esto demostrará el compromiso de la organización con el aseguramiento de la seguridad de la información, lo que también asegurará la asignación adecuada de recursos, la definición de roles y responsabilidades, así como la provisión de la formación adecuada, además de que se mencionará que se implementarán medidas de seguridad para proteger los datos.

5.3 Justificación

La presente propuesta teórica de aplicación contribuye a que la empresa Santa Cecilia pueda tener un esquema de políticas informáticas relacionadas con la norma ISO27001 con controles adicionales de la norma ISO27002, esto será de gran beneficio para la empresa porque podrá organizarse y tener una forma de trabajo disciplinado en relación a sus activos de tecnología.

Se puede, además, identificar necesidades de seguridad de la información, comprendiendo las necesidades específicas de seguridad de la información de la empresa incluyendo la protección de datos confidenciales, prevención de intrusiones y cumplimiento normativo.

Al utilizar la norma ISO27002 se puede proporcionar un conjunto de controles importantes y buenas prácticas para la gestión de la seguridad de la información, estos aportarán a gran medida y permitirán una alineación con los requisitos de seguridad de la información establecidos en la norma ISO27001.

Es importante indicar que, la ISO27001 promueve una mejora continua mediante la identificación y tratamiento proactivo de los riesgos de seguridad de la información, sin embargo, es necesario que se haga una evaluación periódica de la eficiencia de los controles utilizando ISO27002 ya que puede ayudar a la organización a identificar áreas de mejora y fortalecer aún más una postura de seguridad de la información.

5.4 Objetivos

5.4.1 Objetivos generales

Estimar la complementariedad y eficiencia de los controles ISO27002 como aporte complementario para la aplicación de políticas usando la norma ISO27001 en la empresa Santa Cecilia para fortalecer la seguridad de la información.

5.4.2 Objetivos específicos

Revisar documentación de controles ISO27001 y 27002 que permitan adaptarse a la empresa camaronera Santa Cecilia.

Elegir los controles adecuado que permitan garantizar una mejora en la seguridad de la información para la empresa Santa Cecilia.

Redactar un borrador de políticas como base de propuesta, con controles que permitan mejorar la seguridad de la información.

5.5 Aspectos básicos de la Propuesta de Aplicación

Las políticas de seguridad informática consisten en una serie de reglas y pautas que ayudan a minimizar los riesgos que afectan la información y garantizan su confidencialidad, integridad y disponibilidad.

Una política de seguridad se define a alto nivel, incluyendo qué se debe proteger y cómo se deben implementar los controles, esta se compone de una serie de procedimientos e instrucciones técnicas que contienen las medidas organizativas y técnicas que se toman para cumplir con dicha política.

La definición de una política de seguridad debe basarse en una identificación y análisis previos de los riesgos a los que está expuesta la información, esta definición debe incluir todos los procesos, sistemas y personal de la organización, además, debe haber sido aprobado por el consejo de administración de la organización y debe haber sido informado a todo el personal.

Entrando más en detalle, los estándares que regulan la protección de la información de una organización incluyen principalmente las siguientes políticas y procedimientos:

• Mejores prácticas

El documento debe contener buenas prácticas de seguridad de la información, que puede ser un documento específico o cláusulas anexas a los contratos de los empleados, debería incluir, entre otras cosas, las recomendaciones para mantener el puesto de trabajo despejado, el bloqueo de equipos desatendido, la protección de contraseñas y el uso aceptable de los sistemas y la información por parte del personal.

• El procedimiento para controlar los accesos

Recoge las precauciones organizacionales y técnicas necesarias para permitir el acceso tanto a la información de la organización como a la propia, son sistemas y mecanismos utilizados para limitar el acceso de los empleados a las instalaciones de la empresa, como barreras, tornos, cámaras, alarmas, sistemas de apertura de puertas biométricos o por tarjeta, etc.

5.5.1 Estructura general de la propuesta

Tendrá la siguiente estructura, que se compone de la redacción de los lineamientos a seguir para garantizar una seguridad de la información mediante el uso normativo de la ISO 27001 y 27002

- Alcance
- Responsabilidades
- Uso Aceptable de los Recursos Informáticos
- Seguridad de la Información
- Respaldo de Datos y Recuperación ante Desastres
- Cumplimiento Legal y Normativo
- Educación y Concienciación
- Revisiones y Actualizaciones
- Sanciones por Incumplimiento

5.5.2 Componentes

5.5.2.1 Análisis de Riesgos

Este componente es fundamental para que se pueda determinar o estimar la eficiencia de los controles ISO27002 como aporte complementario para la aplicación de políticas usando la norma ISO27001 en la empresa Santa Cecilia para fortalecer la seguridad de la información, este análisis de riesgo es además fortalecido con aspectos de la norma ISO/IEC 27005, pues proporciona directrices y principios para la gestión de riesgos de seguridad de la información, incluyendo el análisis de riesgos para sistemas de información, ayudó a la organizaciones a identificar, evaluar y tratar los riesgos de seguridad de la información de manera efectiva.

Pues es necesario la creación de confianza de las partes interesadas, por lo que se ha hecho el análisis con la información del ANEXO, que refleja un estudio previo del 2023 que necesita ser comparado con las políticas que se han desarrollado en 2024, con procedimientos escuetos e información no tan trascendental,

5.5.2.2 Políticas Desarrolladas en 2024 -01 -08

Política de Software de la Empresa Camaronera Santa Cecilia

1.-Declaración del Propósito: La Empresa Camaronera Santa Cecilia reconoce la importancia de gestionar de manera efectiva el uso y la distribución de software dentro de la organización para garantizar la seguridad, la legalidad y el rendimiento óptimo de los sistemas informáticos, se alinea con los objetivos de seguridad de la información establecidos por las normas ISO 27001 y 27002.

2.-Alcance: Se aplica a todos los empleados, contratistas y terceros que utilicen software en dispositivos propiedad de la Empresa Camaronera Santa Cecilia o en dispositivos personales utilizados para llevar a cabo actividades relacionadas con la empresa.

3.- Responsabilidades:

- Departamentos de TI, en cumplimiento con el control A.6.1.1 de ISO 27001, son responsables de gestionar la adquisición, instalación, mantenimiento y licenciamiento de todo el software utilizado en la organización.
- Gerentes de departamento, conforme al control A.6.1.2 de ISO 27001, son responsables de asegurarse de que sus equipos cumplan con esta política y de reportar cualquier incumplimiento al área de TI.
- Empleados, en línea con el control A.6.1.3 de ISO 27001, son responsables de utilizar el software de manera ética, legal y conforme lo dispone las directrices establecidas por esta política.

4.- Uso Aceptable del Software:

- Se prohíben el uso de software no autorizado o ilegal en cualquier dispositivo utilizado en el entorno de trabajo de la Empresa camaronera Santa Cecilia, conforme al control A.8.1.1 de la ISO 27001.
- Se permite el uso de software personal en dispositivos propiedad de la empresa, solo si está autorizado por el área de Sistemas y TI y este no entra en conflicto con las políticas de seguridad de la empresa, como se indica en el control A.8.1.2 de ISO 27001.

5. Seguridad del Software:

- Se deben implementar medidas de seguridad para proteger el software de la empresa contra accesos no autorizados, incluyendo la utilización de contraseñas seguras y la actualización regular de parches de seguridad, en cumplimiento con los controles A.12.3.1 y A.12.6.1 de ISO 27001.
- Se prohíbe ademas la instalación de software sin autorización previa del área de TI, ya que esto puede comprometer la seguridad de los sistemas, en línea con el control A.12.5.1 de ISO 27001.

6. Licenciamiento:

- Todo el software utilizado en los dispositivos de la Empresa Camaronera Santa Cecilia debe estar perfectamente licenciado y en conformidad con los términos y condiciones establecidos por los proveedores de software, según el control A.12.3.2 de ISO 27001.
- Se prohíbe además el uso de software pirata o sin licencia en cualquier dispositivo propiedad de la empresa o utilizado en el contexto laboral, conforme al control A.12.3.3 de ISO 27001.

7. Auditoría y Cumplimiento:

- El área de Sistemas y TI realizará auditorías regulares para garantizar el cumplimiento de esta política y tomará medidas correctivas en caso de incumplimiento, en alineación con el control A.18.1.1 de ISO 27001.
- Se proporcionará formación y orientación a los empleados sobre las políticas y procedimientos relacionados con el uso de software, según el control A.7.2.2 de ISO 27002.

8. Sanciones por Incumplimiento:

- El incumplir esta política puede resultar en medidas disciplinarias, incluyendo advertencias, suspensión o terminación del empleo, según la gravedad y la repetición del incumplimiento, en línea con el control A.7.3.1 de ISO 27002.

9. Revisión y Actualización:

- Esta política será revisada anualmente por el área de Sistemas y TI para asegurar su relevancia y eficacia, y se actualizará según sea necesario para reflejar los cambios en la tecnología y los requisitos comerciales, en conformidad con el control A.12.1.1 de ISO 27001.

REVISADO Y APROBADO POR:	DESARROLLADO POR
ING. FRANCIS CAMACHO LOOR	JOHN GARCIA

Política para el Hardware de Servidores de Camaronera Santa Cecilia usando controles ISO27001 y 27002

1.-Declaración del Propósito: La empresa Santa Cecilia reconoce que es importante gestionar de manera efectiva y eficiente el hardware de los Servidores para de esta manera garantizar la alta disponibilidad, así como la integridad y confidencialidad sus datos, y se alinea con los estándares de seguridad de la información establecidos por las normas ISO 27001 y 27002.

2.- Alcance: Esta será aplicada a todos los servidores utilizados en la infraestructura de tecnología de la información de la empresa Santa Cecilia, incluyendo los servidores físicos y virtuales que existan, así como sus datos y sus sistemas que se encuentren alojados en estos.

3. Responsabilidades:

- El área de sistemas y TI, conforme se dispone en el control A.12.1.1 de ISO27001, es el responsable de la adquisición, instalación, así como su mantenimiento y disposición segura del hardware de los servidores.
- Usuarios finales, según el control A.7.1.2 de ISO 27002, deben cumplir con las políticas y procedimientos establecidos para el uso de los recursos de los servidores.
- Administradores de sistemas, en línea con el control A.12.1.2 de ISO 27001, son responsables de gestionar y supervisar el funcionamiento adecuado de los servidores, así como de implementar medidas de seguridad para protegerlos contra amenazas físicas y lógicas.

4. Configuración y Mantenimiento:

- Todos los servidores deben ser configurados y mantenidos de acuerdo con las mejores prácticas de seguridad, incluyendo la aplicación de actualizaciones de software y parches de seguridad, conforme al control A.12.6.1 de ISO 27001.
- Se deben implementar medidas de control de acceso físico y lógico para proteger los servidores contra accesos no autorizados, en línea con los controles A.11.1.1 y A.11.2.1 de ISO 27001.

5. Respuesta a Incidentes:

- Se deben establecer procedimientos de respuesta a incidentes para detectar, reportar y mitigar posibles violaciones de seguridad o fallos en los servidores, conforme al control A.16.1.1 de ISO 27001.
- Se deben realizar pruebas periódicas de recuperación de desastres para garantizar la disponibilidad y la integridad de los datos alojados en los servidores, en cumplimiento con el control A.17.1.1 de ISO 27001.

6. Monitoreo y Auditoría:

- Se recomienda la implementación de sistemas de monitoreo para supervisar el rendimiento y la disponibilidad de los servidores, así como para detectar posibles intrusiones o comportamientos irregulares, según el control A.12.4.1 de ISO 27001.
- Además, es recomendable realizar auditorías periódicas de los servidores para garantizar el cumplimiento de esta política y de los estándares de seguridad establecidos, en alineación con el control A.18.1.1 de la normativa ISO27001.

7. Sanciones por Incumplimiento:

- El incumplir esta política puede resultar en medidas disciplinarias, incluyendo advertencias, suspensión o terminación del empleo, según la gravedad y la repetición del incumplimiento, en línea con el control A.7.3.1 de ISO 27002.

8. Revisión y Actualización:

- Esta política será revisada anualmente por El área de Sistemas y TI para asegurar su relevancia y eficacia, y se actualizará según sea necesario para reflejar los cambios en la tecnología y los requisitos comerciales, en conformidad con el control A.12.1.1 de ISO 27001.

REVISADO Y APROBADO POR:	DESARROLLADO POR
ING. FRANCIS CAMACHO LOOR	JOHN GARCIA

Política de Autenticación de la Empresa Camaronera Santa Cecilia con Controles ISO 27001 y 27002

1. Declaración de Propósito: La Empresa Camaronera Santa Cecilia reconoce la importancia de establecer procedimientos de autenticación sólidos para proteger los sistemas y datos de acceso no autorizado, garantizando la confidencialidad, integridad y disponibilidad de la información, en conformidad con los estándares de seguridad de la información establecidos por las normas ISO 27001 y 27002.

2. Alcance: Esta política se aplica a todos los sistemas y servicios de información utilizados en la infraestructura tecnológica de la Empresa Camaronera Santa Cecilia que requieran autenticación para acceder.

3. Responsabilidades:

- El área de TI , conforme al control A.12.1.1 de ISO 27001, es responsable de establecer y mantener los controles de autenticación de acuerdo con esta política.
- Los administradores de sistemas, según el control A.12.1.2 de ISO 27001, son responsables de configurar y gestionar los sistemas de autenticación de manera segura y eficaz.
- Los usuarios finales, en línea con el control A.7.1.1 de ISO 27002, son responsables de utilizar adecuadamente los mecanismos de autenticación y proteger sus credenciales de acceso.

4. Mecanismos de Autenticación:

- Se deben utilizar métodos de autenticación sólidos, como contraseñas, certificados digitales, biometría u otros factores de autenticación multifactorial, en cumplimiento con los controles A.11.2.7 y A.11.2.8 de ISO 27001.
- Se debe implementar un proceso seguro para la gestión de contraseñas, que incluya políticas de complejidad, rotación periódica y prohibición de reutilización de contraseñas antiguas, en alineación con los controles A.9.2.4 y A.9.4.3 de ISO 27001.

5. Gestión de Credenciales:

- Se debe establecer un proceso seguro para la asignación y revocación de credenciales de usuario, en cumplimiento con el control A.9.2.5 de ISO 27001.
- Se debe implementar un control de acceso basado en roles (RBAC) para garantizar que los usuarios tengan los privilegios de acceso adecuados de acuerdo con sus funciones laborales, en línea con el control A.9.1.2 de ISO 27001.

6. Monitoreo y Auditoría:

- Se debe implementar un sistema de registro de eventos de autenticación para registrar y monitorear los intentos de inicio de sesión y las actividades de los usuarios, en alineación con el control A.12.4.1 de ISO 27001.
- Se deben realizar auditorías periódicas de los registros de autenticación para detectar posibles intentos de acceso no autorizado o comportamientos anómalos, conforme al control A.12.4.2 de ISO 27001.

7. Sanciones por Incumplimiento:

- El incumplir esta política puede resultar en medidas disciplinarias, incluyendo advertencias, suspensión o terminación del empleo, según la gravedad y la repetición del incumplimiento, en línea con el control A.7.3.1 de ISO 27002.

8. Revisión y Actualización:

- Esta política será revisada anualmente por El area de Sistemas y TI para asegurar su relevancia y eficacia, y se actualizará según sea necesario para reflejar los cambios en la tecnología y los requisitos comerciales, en conformidad con el control A.12.1.1 de ISO 27001.

REVISADO Y APROBADO POR:	DESARROLLADO POR
ING. FRANCIS CAMACHO LOOR	JOHN GARCIA

Política para usuarios comunes de la Empresa Camaronera Santa Cecilia con controles ISO27001 y 27002

1.-Declaración de Propósito: La Camaronera Santa Cecilia reconoce la importancia de establecer directrices claras para los usuarios finales con el fin de garantizar la seguridad de la información y el correcto uso de los recursos de tecnología de la información, en conformidad con los estándares de seguridad de la información establecidos por las normas ISO27001 y 27002.

2.-Alcance: Esta política se aplicará a todos los empleados y personas externas que brindan servicio técnico y que utilicen los sistemas de información y recursos de TI de la Empresa Camaronera Santa Cecilia en el curso de sus actividades laborales.

3.-Responsabilidades:

- Los usuarios finales son responsables de utilizar los recursos de TI de manera segura y responsable, en cumplimiento con las políticas y procedimientos establecidos por la empresa y en línea con el control A.7.1.1 de ISO 27002.
- El área de Sistemas y TI es la responsable de proporcionar orientación y apoyo a los usuarios finales para asegurar el cumplimiento de esta política, conforme al control A.12.1.1 de ISO 27001.

4.-Uso Aceptable de los Recursos de TI:

- Se deben utilizar los recursos de TI de la empresa Camaronera Santa Cecilia únicamente para fines comerciales autorizados, se debe evitar el acceso a sitios web no relacionados con el trabajo o uso indebido de recursos tecnológicos, en cumplimiento con el control A.8.1.1 de ISO 27002.
- Los usuarios no deben instalar software no autorizado o no licenciado en los dispositivos de la empresa, en conformidad con el control A.12.3.1 de ISO 27001.

5.-Seguridad de la Información:

- Los usuarios deben proteger sus credenciales de acceso, incluyendo contraseñas y dispositivos de autenticación, y no compartirlas con otros empleados, conforme al control A.9.2.1 de ISO 27001.
- Se debe informar al área de TI de cualquier incidente de seguridad o sospecha de compromiso de la información, en alineación con el control A.16.1.1 de ISO 27001.

6. Formación y Concientización:

- Se proporcionará formación y orientación periódica a los usuarios finales sobre las políticas de seguridad de la información, las mejores prácticas de seguridad y los riesgos potenciales asociados con el uso de los recursos de TI, en cumplimiento con el control A.7.2.2 de ISO 27002.

7. Sanciones por Incumplimiento:

- El incumplir esta política puede resultar en medidas disciplinarias, incluyendo advertencias, formación adicional o suspensión del acceso a los recursos de TI, según la gravedad y la repetición del incumplimiento, en línea con el control A.7.3.1 de ISO 27002.

8. Revisión y Actualización:

- Esta política será revisada anualmente por el departamento de sistemas para asegurar su relevancia y eficacia, y se actualizará según sea necesario para reflejar los cambios en la tecnología y los requisitos comerciales, en conformidad con el control A.12.1.1 de ISO 27001.

REVISADO Y APROBADO POR:	DESARROLLADO POR
ING. FRANCIS CAMACHO LOOR	JOHN GARCIA

Política para el manejo de Bases de Datos de la empresa camaronera Santa Cecilia con Controles ISO27001 y 27002

1.-Declaración del Propósito: La Empresa Santa Cecilia reconoce la importancia de establecer procedimientos seguros y eficientes para el manejo de bases de datos con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, en conformidad con los estándares de seguridad de la información establecidos por las normas ISO27001 y 27002.

2.-Alcance: Aplicado a todos los empleados y personal contratista externo que trabajen con bases de datos de la empresa camaronera Santa Cecilia y a los sistemas y recursos asociados a dichas bases de datos.

3.-Responsabilidades:

- El administrador de bases de datos, conforme se dispone el control A.12.1.1 de norma ISO27001, es la persona responsable de supervisar y manejar de forma segura y eficiente de las bases de datos y garantizar el cumplimiento de esta política.
- Usuarios de bases de datos, en línea con el control A.7.1.1 de la ISO27002, son responsables de utilizar las bases de datos de manera segura y de acuerdo con las políticas establecidas por la empresa.

4.-Acceso y Control de Datos:

- Se debe establecer políticas de control de accesos basadas en roles RBAC, para garantizar que los usuarios tengan acceso solamente a los datos necesarios para realizar sus laborales, en conformidad con el control A.9.1.2 de ISO 27001.
- Es necesario implementar medidas de seguridad para protección de los datos almacenados en bases de datos contra accesos no autorizados, incluyendo la encriptación de datos sensibles, esto en cumplimiento con controles A.11.1.1 y A.11.1.2 de ISO 27001.

5.-Respaldo y Recuperación:

- Debe establecerse un programa de respaldos regulares que permita garantizar la disponibilidad e integridad de los datos almacenados en las bases de datos, en conformidad con el control A.12.3.1 de ISO 27001.
- Se deben realizar pruebas periódicas de recuperación ante desastres para verificar la efectividad de los procedimientos de respaldo y restauración, según el control A.17.1.1 de ISO 27001.

6.- Monitoreo y Auditoría:

- Se debe implementar un sistema de monitoreo para supervisar la actividad en las bases de datos y detectar posibles violaciones de seguridad o actividades anómalas, en alineación con el control A.12.4.1 de ISO27001.
- Es necesario que se realicen auditorías periódicas de bases de datos para evaluar el cumplimiento de esta política y sus estándares de seguridad establecidos, conforme lo dispone el control A.18.1.1 de ISO27001.

7.- Sanciones por Incumplimiento:

- Incumplir esta política puede acarrear medidas disciplinarias, incluyendo advertencias, formación adicional o suspensión del acceso a las bases de datos, según la gravedad y la repetición del incumplimiento, en línea con el control A.7.3.1 de ISO27002.

8. Revisión y Actualización:

- Esta política será revisada anualmente por El área de Sistemas y TI para asegurar su relevancia y eficacia, y se actualizará según sea necesario para reflejar los cambios en la tecnología y los requisitos comerciales, en conformidad con el control A.12.1.1 de ISO 27001.

REVISADO Y APROBADO POR:	DESARROLLADO POR
ING. FRANCIS CAMACHO LOOR	JOHN GARCIA

Política para el Cuidado de Activos de la Empresa Camaronera Santa Cecilia con Controles ISO 27001 y 27002

1.-Declaración de Propósito: La Empresa Camaronera Santa Cecilia reconoce la importancia de proteger sus activos, incluyendo recursos de tecnología de la información (TI), propiedad intelectual, instalaciones y equipos, para garantizar su disponibilidad, confidencialidad e integridad, en conformidad con los estándares de seguridad de la información establecidos por las normas ISO 27001 y 27002.

2.-Alcance: Esta política se aplica a todos los empleados, contratistas y terceros que utilicen, accedan o gestionen activos de la Empresa Camaronera Santa Cecilia en el curso de sus actividades laborales.

3.-Responsabilidades:

- El área de TI, conforme al control A.12.1.1 de ISO 27001, es responsable de supervisar el cuidado y la protección de los activos de TI, así como de establecer y mantener los controles necesarios para garantizar su seguridad.
- Gerentes departamentales, alineados con el control A.12.1.2 de ISO 27001, son los responsables de garantizar que los activos bajo su responsabilidad sean utilizados y protegidos de manera adecuada por sus equipos.
- Empleados, conforme dispone el control A.7.1.1 de ISO 27002, son responsables de utilizar y proteger los activos de la empresa de acuerdo con las políticas y procedimientos establecidos.

4.-Protección de Activos de TI:

- Deben implementarse medidas físicas, técnicas y organizativas para proteger los activos de TI contra accesos no autorizados, daños, robo o pérdida, en conformidad con los controles A.11.1.1 y A.11.1.2 de ISO27001.
- Deben establecerse controles de acceso y políticas de seguridad para restringir el acceso a los activos de TI solo a personal autorizado, según el control A.9.1.1 de ISO 27001.

5. Uso Aceptable de Activos:

- Los activos de la empresa deben utilizarse únicamente para fines comerciales autorizados, evitando el uso no autorizado o inapropiado, en cumplimiento con el control A.8.1.1 de ISO 27002.
- Los empleados deben seguir las políticas de uso aceptable establecidas para los activos de TI, incluyendo el uso adecuado de software licenciado y la protección de datos confidenciales, conforme al control A.7.2.1 de ISO 27002.

6. Respaldo y Recuperación:

- Se debe establecer un programa de respaldo regular para garantizar la disponibilidad y la integridad de los datos almacenados en los activos de TI, en conformidad con el control A.12.3.1 de ISO 27001.
- Se deben realizar pruebas periódicas de recuperación ante desastres para verificar la efectividad de los procedimientos de respaldo y restauración, según el control A.17.1.1 de ISO 27001.

7. Sanciones por Incumplimiento:

- El incumplir esta política puede resultar en medidas disciplinarias, incluyendo advertencias, formación adicional o suspensión del acceso a los activos, según la gravedad y la repetición del incumplimiento, en línea con el control A.7.3.1 de ISO 27002.

8. Revisión y Actualización:

- Esta política será revisada anualmente por el área de Sistemas y TI para asegurar su relevancia y eficacia, y se actualizará según sea necesario para reflejar los cambios en la tecnología y los requisitos comerciales, en conformidad con el control A.12.1.1 de ISO 27001.

REVISADO Y APROBADO POR:	DESARROLLADO POR
ING. FRANCIS CAMACHO LOOR	JOHN GARCIA

Política para la red de datos y recursos de red de la empresa camaronera Santa Cecilia con Controles ISO 27001 y 27002

1.-Declaración del Propósito: La empresa camaronera Santa Cecilia reconoce que es importante establecer procedimientos seguros y eficientes para la buena gestión y protección de su red y recursos de red con el fin de garantizar la disponibilidad, confidencialidad e integridad de los datos e información, en conformidad con los estándares de seguridad de la información establecidos por las normas ISO 27001 y 27002.

2.-Alcance: Política aplicable a todos los empleados, contratistas y terceros que utilicen, accedan o gestionen la red y recursos de red de la empresa camaronera Santa Cecilia, incluyendo equipos de red, sistemas de comunicaciones y servicios relacionados.

3.-Responsabilidades:

- Área de tecnologías, conforme lo dispone el control A.12.1.1 de ISO 27001, es la responsable de supervisar la gestión y protección de la red y recursos de red, así como de establecer y mantener los controles necesarios para garantizar su seguridad.
- Administradores de red, que estarán alineados con el número de control A.12.1.2 de la norma ISO27001, son responsables de configurar y administrar los dispositivos de red y servicios relacionados de manera segura y eficaz.
- Usuarios finales, conforme con el control A.7.1.1 de ISO27002, son responsables de utilizar los recursos de red de manera segura y de acuerdo con las políticas establecidas.

4.-Seguridad de la Red:

- Es necesario implementar medidas de seguridad físicas y lógicas para proteger la red de accesos no autorizados, así como ataques cibernéticos y demás amenazas, en conformidad con los controles A.11.1.1 y A.11.1.2 de ISO 27001.
- Es necesario además tener un firewall para controlar todo el tráfico de red entrante y saliente y proteger los sistemas y datos de la empresa, según el control A.13.1.1 de ISO 27001.

5. Control de Acceso a la Red:

- Se deben implementar controles de acceso para restringir el acceso a la red y a los recursos de red solo a usuarios autorizados, en cumplimiento con el control A.9.1.1 de ISO 27001.
- Se debe utilizar la autenticación multifactorial para aumentar la seguridad al acceder a los recursos de red críticos, conforme al control A.11.2.7 de ISO 27001.

6. Monitoreo y Detección de Intrusiones:

- Se deben implementar un sistema de monitoreo de red para supervisar el tráfico de red y detectar posibles actividades maliciosas o comportamientos anómalos, en alineación con el control A.12.4.1 de ISO27001.
- Así mismo, es necesario establecer procedimientos de respuesta a incidentes para gestionar y mitigar las intrusiones de red de manera eficaz, según el control A.16.1.1 de ISO27001.

7. Sanciones por Incumplimiento:

- El incumplir esta política puede resultar en medidas disciplinarias, incluyendo advertencias, formación adicional o suspensión del acceso a la red y recursos de red, según la gravedad y la repetición del incumplimiento, en línea con el control A.7.3.1 de ISO 27002.

8. Revisión y Actualización:

- Esta política será revisada anualmente por el área de Sistemas y TI para asegurar su relevancia y eficacia, y se actualizará según sea necesario para reflejar los cambios en la tecnología y los requisitos comerciales, en conformidad con el control A.12.1.1 de ISO 27001.

REVISADO Y APROBADO POR:	DESARROLLADO POR
ING. FRANCIS CAMACHO LOOR	JOHN GARCIA

5.6 Resultados esperados de la Propuesta de Aplicación

Se espera que de aplicarse su seguridad aumente en un 90%

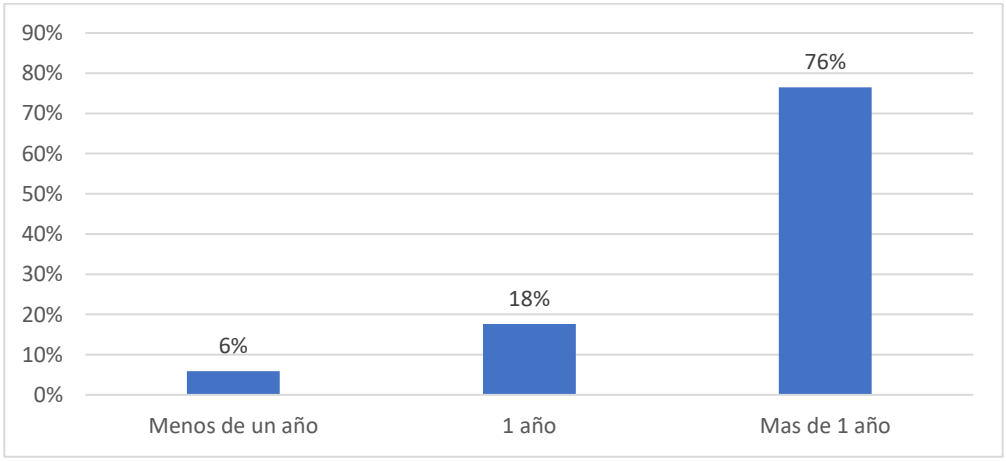
En relación a la investigación plasmada con un instrumento encuesta, se han obtenido los resultados siguientes:

Fecha de toma de datos: **28 de febrero del 2024**

Tabla 13. **Resultado de: ¿Cuánto tiempo lleva en la empresa contratado o laborando?**

	FRECUENCIA	PORCENTAJE
Menos de un año	4	6%
1 año	12	18%
Mas de 1 año	52	76%
	68	**100%**

Gráfica 11. **Resultado de: ¿Cuánto tiempo lleva en la empresa contratado o laborando?**

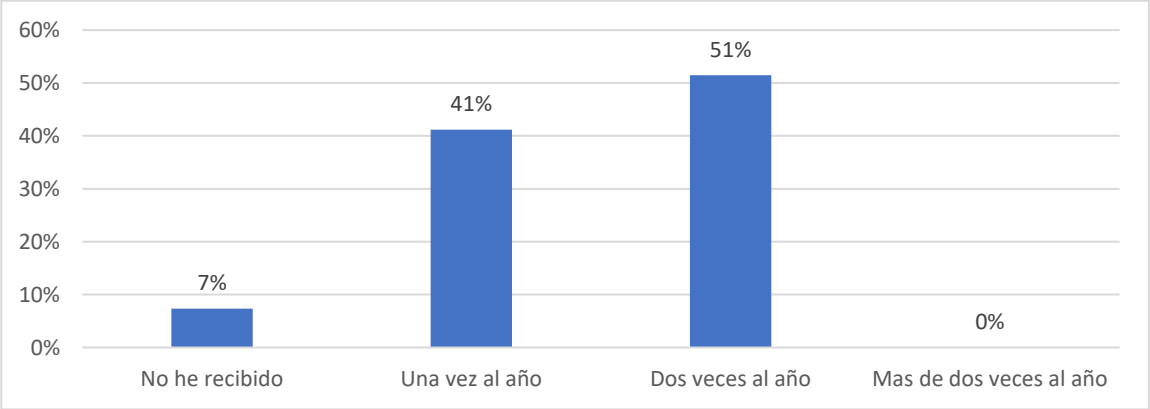


En relación con el primer diagnóstico, no se han producido cambios importantes en esta pregunta.

Tabla 14. **¿Cada cuanto recibe capacitación relacionada con informática y cuidado de los datos en la empresa?**

	FRECUENCIA	PORCENTAJE
No he recibido	5	7%
Una vez al año	28	41%
Dos veces al año	35	51%
Mas de dos veces al año	0	0%
	68	**100%**

Gráfica 12. **¿Cada cuanto recibe capacitación relacionada con informática y cuidado de los datos en la empresa?**



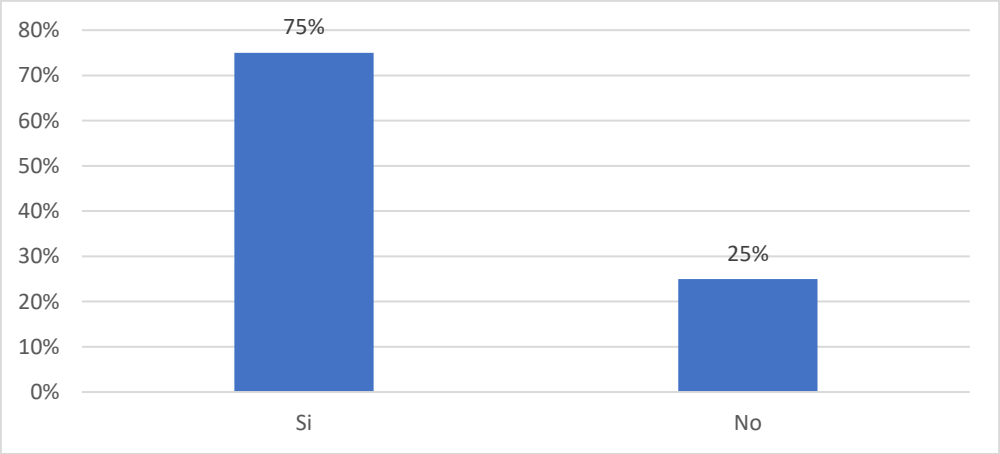
En relación con el primer diagnóstico, se ve reflejado un cambio, pues se ha capacitado casi al 100% del personal, es decir, el no recibido ya disminuyó a 7%, que posiblemente fueron personas que no les toco asistir el día de la capacitación informática.

Si se evidenció un cambio importante, al menos ya se ha sentido que han tenido una capacitación inclusive personal poco relacionado con sistemas de información.

Tabla 15. **¿Sabes si existen políticas y procedimientos que permitan cuidar datos en la empresa?**

	FRECUENCIA	PORCENTAJE
Si	51	75%
No	17	25%
	68	100%

Gráfica 13. **¿Sabes si existen políticas y procedimientos que permitan cuidar datos en la empresa?**

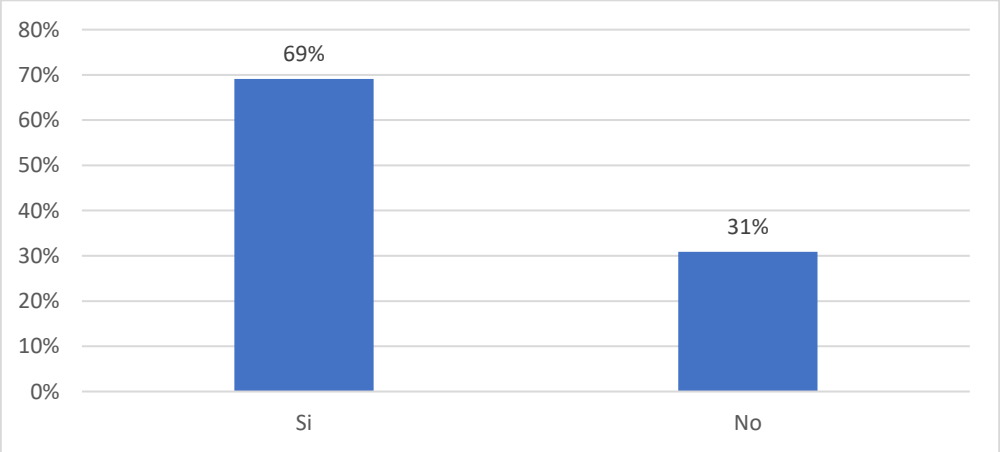


En relación a esta consulta, ya el 75% conoce la existencia de lineamientos a seguir para cuidar los datos, antes solo conocían el 3%; de esta forma se evidencia el cambio importante en esta investigación

Tabla 16. ¿Usas sistemas informáticos para alguna actividad en la empresa?

	FRECUENCIA	PORCENTAJE
Si	47	69%
No	21	31%
	68	100%

Gráfica 14. ¿Usas sistemas informáticos para alguna actividad en la empresa?

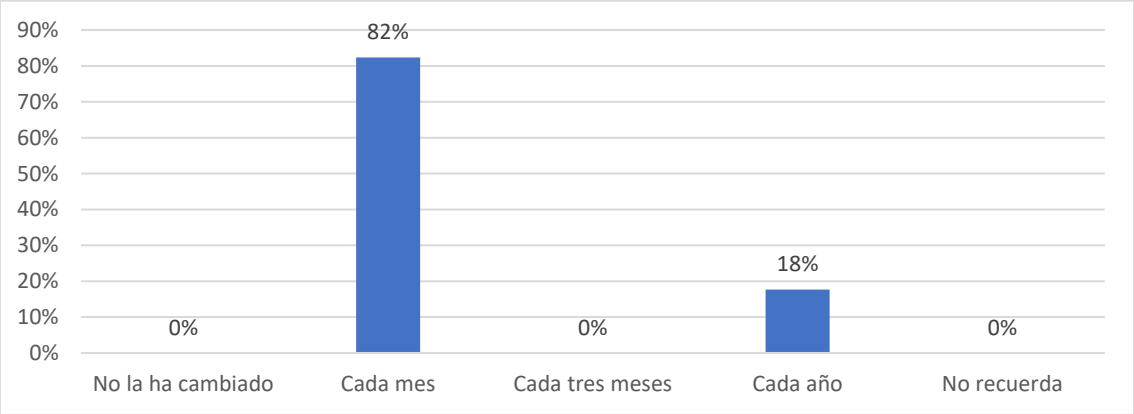


Se nota una variación muy sutil, pues seguramente se han incrementado en poco porcentaje quienes usan sistemas para alguna parte de la automatización de los procesos en la planta

Tabla 17. ¿Cada que tiempo cambia o le ayudan a cambiar sus contraseñas de acceso a los sistemas de la empresa?

	FRECUENCIA	PORCENTAJE
No la ha cambiado	0	0%
Cada mes	56	82%
Cada tres meses	0	0%
Cada año	12	18%
No recuerda	0	0%
	68	**100%**

Gráfica 15. ¿Cada que tiempo cambia o le ayudan a cambiar sus contraseñas de acceso a los sistemas de la empresa?

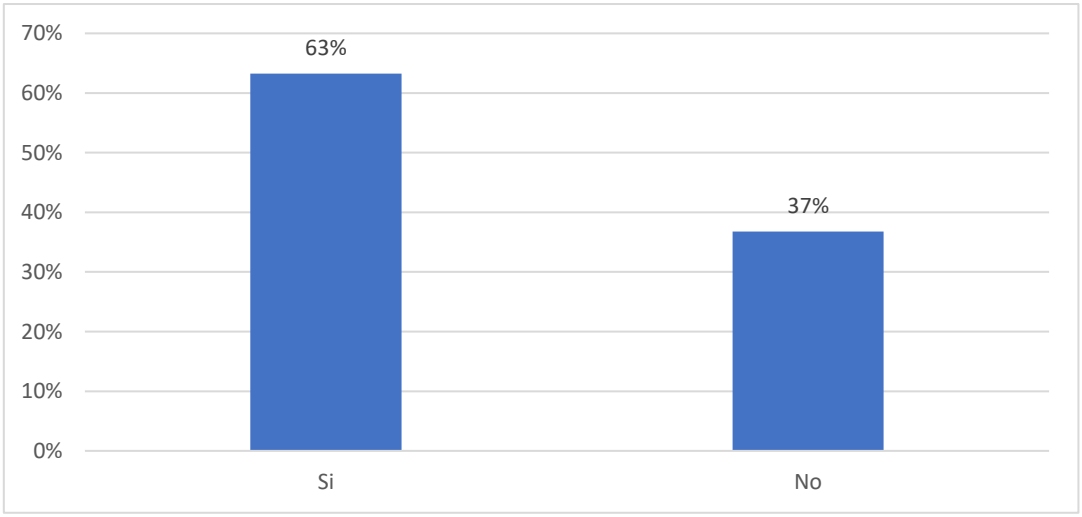


En esta pregunta, se evidencia cambio, ya se lo realiza cada mes en un alto porcentaje, de una variación de antes tener 0% en cada mes y 50% que no ha cambiado sus contraseñas, representa un indicador de que las políticas aplicando ISO27001 con soporte de ISO27002 han tenido una influencia importante.

Tabla 18. ¿En alguna ocasión ha tenido que compartir su contraseña con algún compañero del trabajo?

	FRECUENCIA	PORCENTAJE
Si	43	63%
No	25	37%
	68	100%

Gráfica 16. ¿En alguna ocasión ha tenido que compartir su contraseña con algún compañero del trabajo?

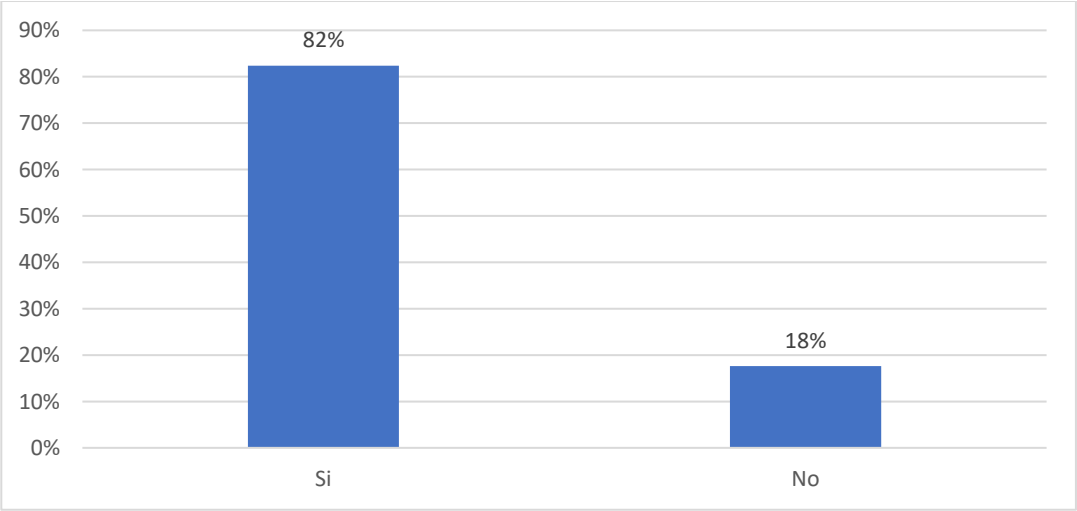


En este caso, aun se mantiene, porque es parte de la historia de lo que antes se hacía, aun faltaría un tiempo para medir una evolución a esto, pero con las políticas propuestas, seguramente esta mala practica ya se anula.

Tabla 19. ¿Cree usted que en la empresa le proporciona el suficiente recurso tecnológico como computadoras, software, tablets, donde con estos se pueda proteger información confidencial?

	FRECUENCIA	PORCENTAJE
Si	56	82%
No	12	18%
	68	100%

Gráfica 17. ¿Cree usted que en la empresa le proporciona el suficiente recurso tecnológico como computadoras, software, tablets, donde con estos se pueda proteger información confidencial?

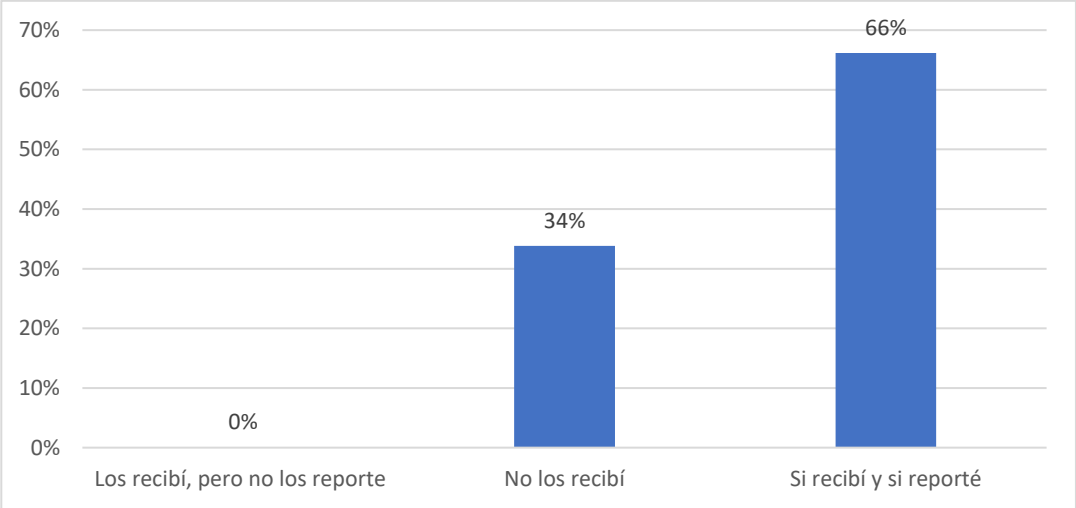


Esta pregunta se mantiene, se sigue evidenciando que si invierten recursos en tecnologías.

Tabla 20. ¿Ha recibido durante los últimos tres meses correos electrónicos sospechosos en la cuenta de mail empresarial o la personal y los has reportado?

	FRECUENCIA	PORCENTAJE
Los recibí, pero no los reporte	0	0%
No los recibí	23	34%
Si recibí y si reporté	45	66%
	68	100%

Gráfica 18. ¿Ha recibido durante los últimos tres meses correos electrónicos sospechosos en la cuenta de mail empresarial o la personal y los has reportado?

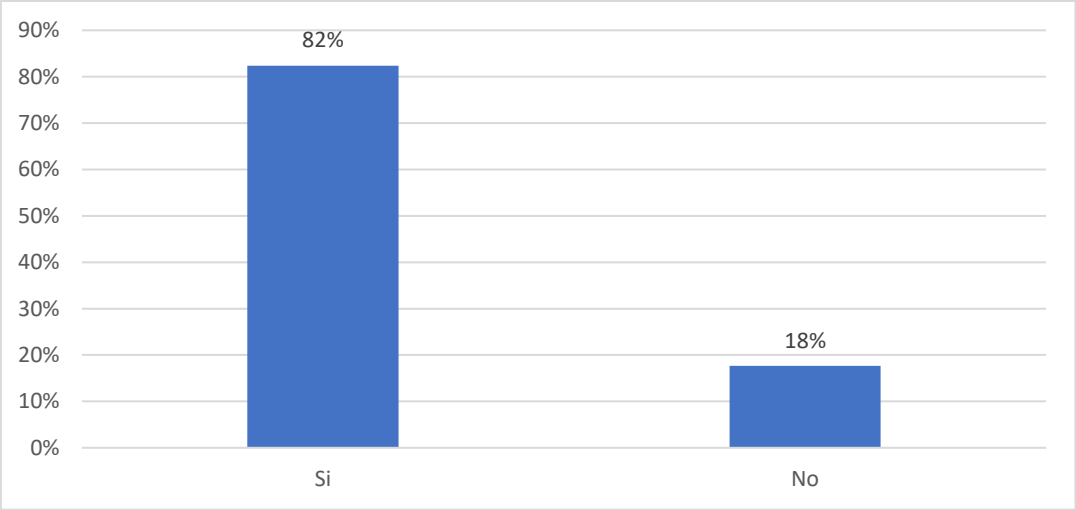


Se han evidenciado cambios importantes, ya que además existe una política relacionada con servidores, los cuales están mejor protegidos y el área de sistemas ya tiene solucionado un block spammer que permite reducir incidencias de spams, y es importante mencionar que el personal de la empresa si está reportando incidencias, así estas no sean spam.

Tabla 21. ¿Le han indicado de algunas reglas o políticas a seguir en relación a los cuidados de la información y datos de la empresa?

	FRECUENCIA	PORCENTAJE
Si	56	82%
No	12	18%
	68	100%

Gráfica 19. ¿Le han indicado de algunas reglas o políticas a seguir en relación a los cuidados de la información y datos de la empresa?

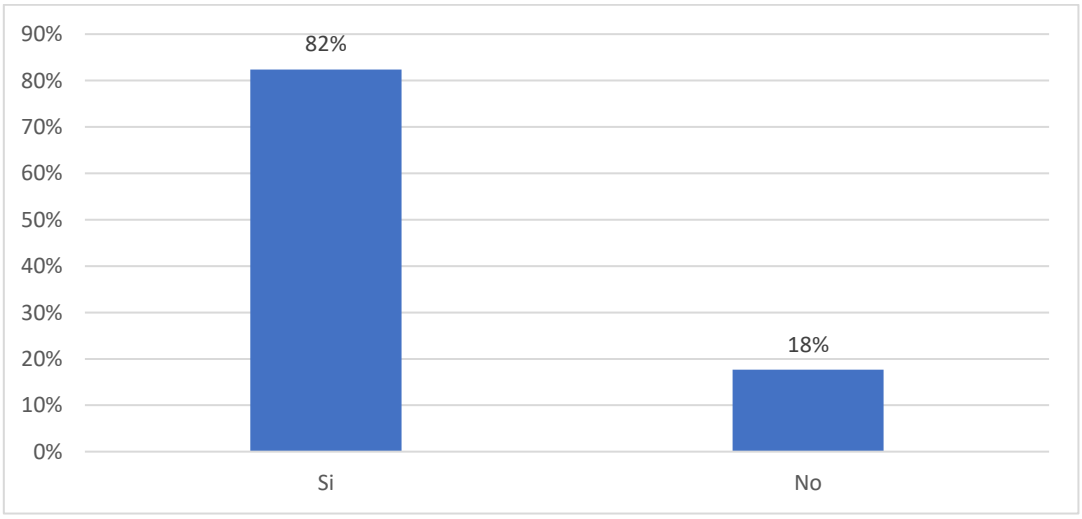


Esta vez si se ha notado que se le han entregado al personal reglas claras en cuanto al uso y cuidado de la información y datos de la empresa, así lo refleja el 82% que lo afirma.

Tabla 22. ¿Conoce o está al tanto de consecuencias graves de no seguir las políticas de seguridad informática de la empresa?

	FRECUENCIA	PORCENTAJE
Si	56	82%
No	12	18%
	68	100%

Gráfica 20. ¿Conoce o está al tanto de consecuencias graves de no seguir las políticas de seguridad informática de la empresa?



Así también, el personal ya conoce que representan consecuencias graves de no seguir las políticas de seguridad informática de la empresa, el 82% refleja que si han instruido al personal en relación a esto.

Este análisis que se ha realizado qui, es producto de la aplicación de las políticas desarrolladas en la sección 5.5.2 con este proyecto de investigación, por lo que se considera que si han tenido un efecto positivo.

5.6.1 Alcance de la alternativa

Esta alternativa debe tener alcance de aplicación en toda la empresa, esto implica las plantas de producción con las que cuenta y además donde se aplique el uso de tecnologías, esto es, si un empleado hace uso de algún sistema desde su casa, también debe aplicar y apegarse a los estándares delineados en las políticas descritas en la sección 5.5.2 de componentes.

REFERENCIAS BIBLIOGRAFICAS

- García, J. (2019). ISO 27001:2013. Guía para la implementación de un sistema de gestión de seguridad de la información. Madrid: Díaz de Santos
- Cindy, A. (2021). IT Governance: An International Guide to Data Security and ISO27001/ISO27002. Kogan Page Publishers
- Iker, J. (20019). *Plan de recuperación de negocios: En una semana.* Gestión 2000.
- Peltier, T. R. (2021). Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. CRC Press3
- Gutierrez, J. (2019). ISO 27001:2013. Implementación de un sistema de gestión de seguridad de la información. Madrid: Díaz de Santos
- Cyrulnik, B. (2022). *Resiliencia: Cómo superar los desafíos y salir fortalecido.* Paidós. ISBN: 9788449336132.
- Calder, A. (2020). ISO 27001 Risk Management in a Physical and Information Security Context. IT Governance Publishing
- Gobierno de España. (2022). *Plan de recuperación, transformación y resiliencia.* BOE. ISBN: 9788434028081.
- Matos Cuevas, M., Beriguete, M., Martire, M., Peña, G., & Reidy, M. (2015). *Diseño de un plan de recuperación ante desastre (DRP).* LAP Lambert Academic Publishing.
- Knaus, W. J. (2019). *La recuperación de la depresión: Un plan de acción para superar la depresión y mejorar tu vida.* Paidós. ISBN: 9788449328835.

- Alba Isabel Maldonado Núñez, C. L. (2023-10-26). *Avances en la gestión de riesgos: modelo ISO 31000 y enfoques actuales.* Obtenido de https://www.fipcaec.com/index.php/fipcaec/article/view/912/1544

- Banco de España. (2020). *Informe anual 2019. Madrid: Banco de España.*

- Blanco, J. (2019). *Planificación de la continuidad del negocio: Una perspectiva estratégica. Madrid: Colegio Oficial de la Psicología de Madrid.* Madrid.
- Colegio Oficial de la Psicología de Madrid. (2020). *Planificación de la continuidad del negocio: Guía práctica. Madrid: Colegio Oficial de la Psicología de Madrid.*
- Culot, G. N. (16 de marzo de 2021). *emerald*. Obtenido de emerald: https://www.emerald.com/insight/content/doi/10.1108/TQM-09-2020-0202/full/html
- Fernández Orozco, G. P. (30 de septiembre del 2021). *Análisis y diseño de un sistema de gestión de la seguridad de la información.* Obtenido de https://repositorio.espe.edu.ec/bitstream/21000/26482/1/T-ESPE-050862.pdf
- GALLO, U. E. (2021). *Implementación de un sistema integrado de gestión.*
- Giovanna Culot, G. N. (16 de marzo de 2021). *The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda*. Obtenido de The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda: https://www.emerald.com/insight/content/doi/10.1108/TQM-09-2020-0202/full/html
- Normalización, O. I. (10 de 10 de 2022). *¿Qué es ISO/IEC 27001?* Obtenido de ¿Qué es ISO/IEC 27001?: https://www.iso.org/standard/27001
- Servicio Público de Empleo Estatal (SEPE) . (2020). *Informe anual 2019. Madrid: SEPE.*

- Taylor, M. J. (4 de 07 de 2014). *Revisión sistemática de la aplicación del método planificar-hacer-estudiar-actuar para mejorar la calidad asistencial* . Obtenido de Revisión sistemática de la aplicación del método planificar-hacer-estudiar-actuar para mejorar la calidad asistencial : https://qualitysafety.bmj.com/content/23/4/290

- Tomás, U. S. (23 de agosto de 2019). *Metodología para la implementación.* Obtenido de https://www.redalyc.org/journal/5604/560465477007/560465477007.pdf

ANEXO 1

DISEÑO DE INSTRUMENTOO ENCUESTA

ENCUESTA A LA EMPRESA CAMARONERA SANTA CECILIA DE LA CIUDAD DE GUAYAQUIL

FECHA: 6 DE FEBRERO DEL 2024

¿Cuanto tiempo lleva en la empresa contratado o laborando?

Menos de un año

1 año

Mas de 1 año

¿Cada cuanto recibe capacitación relacionada con informática y cuidado de los datos en la empresa?

No he recibido

Una vez al año

Dos veces al año

Mas de dos veces al año

¿Sabes si existen políticas y procedimientos que permitan cuidar datos en la empresa ?

Si
No

¿Usas sistemas informáticos para alguna actividad en la empresa?

Si
No

¿Cada que tiempo cambia o le ayudan a cambiar sus contraseñas de acceso a los sistemas de la empresa?

No la ha cambiado
Cada mes
Cada tres meses
Cada año
No recuerda

¿En alguna ocasión a tenido que compartir su contraseña con algún compañero del trabajo?

Si
No

¿Cree usted que en la empresa le proporciona el suficiente recurso tecnológico como computadoras, software, tablets, donde con estos se pueda proteger información confidencial?

Si
no

¿Ha recibido durante los últimos tres meses correos electrónicos sospechosos en la cuenta de mail empresarial o la personal y los has reportado?

Los recibí, pero no los reporte
No los recibí
Si recibí y si reporté

¿Le han indicado de algunas reglas o políticas a seguir en relación a los cuidados de la información y datos de la empresa?

Si
no

¿Conoce o está al tanto de consecuencias graves de no seguir las políticas de seguridad informática de la empresa?

Si
no

ANEXO 2

Estudio del 2023 relacionado con la seguridad informática

Tabla con una lista de 5 activos informáticos del **grupo de servidores**, incluyendo marca, modelo, serie, capacidad de almacenamiento y procesador:

Activo	Marca	Modelo	Serie	Capacidad de Almacenamiento	Procesador
Servidor 1	HP	ProLiant DL380	DL380G10	4 TB SSD	Intel Xeon Gold 5218
Servidor 2	Dell	PowerEdge R740	R740-A784	6 TB HDD	Intel Xeon Silver 4210
Servidor 3	Lenovo	ThinkSystem SR650	SR650-ABCD	8 TB SSD	Intel Xeon Gold 6130
Servidor 4	Cisco	UCS C240 M5	C240M5-AB12	10 TB HDD	Intel Xeon Scalable Family
Servidor 5	Supermicro	SuperServer 2029U-TR4T	2029U-TR4T-ZR1	12 TB HDD	Intel Xeon Processor

activos informáticos del grupo de computadoras personales (PC), todas de marca "Clon":

Activo	Marca	Modelo	Serie	Capacidad de Almacenamiento	Procesador
PC001	Clon	Clon	PC001	512 GB SSD	Intel Core i5
PC002	Clon	Clon	PC002	1 TB HDD	AMD Ryzen 5
PC003	Clon	Clon	PC003	256 GB SSD	Intel Core i7
PC004	Clon	Clon	PC004	2 TB HDD	AMD Ryzen 7
PC005	Clon	Clon	PC005	512 GB SSD	Intel Core i3
PC006	Clon	Clon	PC006	1 TB HDD	AMD Ryzen 3
PC007	Clon	Clon	PC007	128 GB SSD	Intel Pentium
PC008	Clon	Clon	PC008	500 GB HDD	AMD Athlon
PC009	Clon	Clon	PC009	256 GB SSD	Intel Core i5
PC010	Clon	Clon	PC010	1.5 TB HDD	AMD Ryzen 5
PC011	Clon	Clon	PC011	512 GB SSD	Intel Core i7

Activo	Marca	Modelo	Serie	Capacidad de Almacenamiento	Procesador
PC012	Clon	Clon	PC012	2 TB HDD	AMD Ryzen 7
PC013	Clon	Clon	PC013	256 GB SSD	Intel Core i3
PC014	Clon	Clon	PC014	1 TB HDD	AMD Ryzen 3

Esta tabla proporciona información sobre cada computadora personal (PC), incluyendo detalles como marca, modelo, serie, capacidad de almacenamiento y tipo de procesador. Este tipo de información es útil para la gestión de inventario y seguimiento de activos en un entorno informático.

tabla que lista los equipos de red, incluyendo 4 puntos de acceso (AP) Unifi, 1 router Cisco, 1 router MikroTik y 2 switches de 48 puertos:

Activo	Marca	Modelo	Tipo	Descripción
AP1	Unifi	UAP-AC-PRO	Punto de Acceso	Punto de acceso Unifi para redes Wi-Fi.
AP2	Unifi	UAP-AC-PRO	Punto de Acceso	Punto de acceso Unifi para redes Wi-Fi.
AP3	Unifi	UAP-AC-PRO	Punto de Acceso	Punto de acceso Unifi para redes Wi-Fi.
AP4	Unifi	UAP-AC-PRO	Punto de Acceso	Punto de acceso Unifi para redes Wi-Fi.
Router Cisco	Cisco	ISR 4000 Series	Router	Router Cisco para interconexión de redes.
Router MikroTik	MikroTik	RB2011UiAS-RM	Router	Router MikroTik para funciones de enrutamiento y seguridad.
Switch 1	Cisco	Catalyst 2960	Switch	Switch Cisco de 48 puertos para la red local.
Switch 2	Cisco	Catalyst 2960	Switch	Switch Cisco de 48 puertos para la red local.

tablas separadas que muestran las vulnerabilidades por cada grupo de activos:

Vulnerabilidades de Servidores:

Activo	Vulnerabilidades
Servidor 1	- Falta de actualizaciones de firmware para corregir vulnerabilidades conocidas.

Activo	Vulnerabilidades
Servidor 2	- Configuraciones predeterminadas no seguras en el sistema operativo que podrían permitir acceso no autorizado.
Servidor 3	- Falta de auditorías de seguridad regulares para identificar posibles brechas de seguridad.
Servidor 4	- No implementación de medidas de control de acceso adecuadas para proteger contra accesos no autorizados.
Servidor 5	- Exposición a ataques de denegación de servicio (DDoS) debido a la falta de mitigaciones adecuadas.

Vulnerabilidades de Computadoras Personales (PC):

Activo	Vulnerabilidades
PC001	- Uso de contraseñas débiles o predeterminadas que podrían ser vulneradas.
PC002	- Falta de protección antivirus actualizada, dejando el sistema expuesto a malware.
PC003	- Configuraciones de seguridad inadecuadas que podrían permitir el acceso no autorizado.
PC004	- No implementación de actualizaciones de seguridad del sistema operativo y las aplicaciones.
PC005	- Riesgo de pérdida de datos debido a la falta de copias de seguridad regulares.

Vulnerabilidades de Equipos de Red:

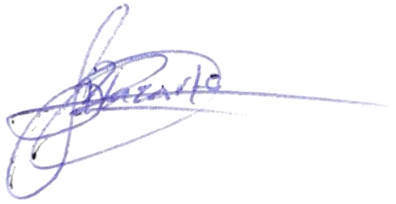
Activo	Vulnerabilidades
AP1	- Falta de actualizaciones de firmware para corregir vulnerabilidades de seguridad conocidas.
AP2	- Uso de encriptación débil o configuraciones inseguras en la red inalámbrica.
AP3	- Riesgo de ataques de denegación de servicio debido a configuraciones incorrectas del punto de acceso.
AP4	- Posibilidad de interceptación de tráfico de red debido a falta de cifrado en la conexión inalámbrica.
Router Cisco	- Vulnerabilidades conocidas en el software del router que podrían ser explotadas por hackers.
Router MikroTik	- Configuraciones de seguridad débiles que podrían permitir el acceso no autorizado al router.
Switch 1	- Riesgo de ataques de spoofing o envenenamiento ARP debido a la falta de medidas de seguridad adecuadas.
Switch 2	- Posibilidad de ataques de acceso no autorizado a través de puertos abiertos o mal configurados.

Estas tablas destacan algunas de las posibles vulnerabilidades asociadas con cada grupo de activos. Es importante realizar evaluaciones de vulnerabilidades regulares y tomar

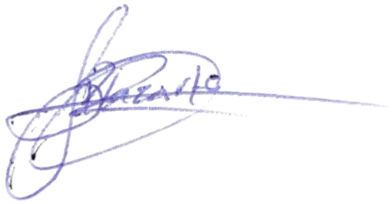
medidas de mitigación adecuadas para proteger los sistemas contra posibles ataques y brechas de seguridad.

ESTRATEGIA 1

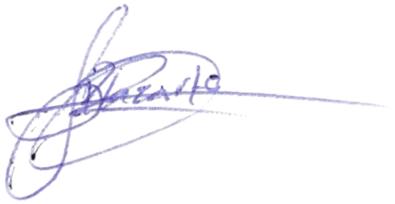
Formulario de Identificación de Activos de Información Fecha de Creación del Formulario: 8 de marzo de 2023
1. Información del responsable:
Nombre del responsable: Ing. Ana García Roman
Cargo: Coordinadora de Seguridad de la Información
2. Identificación del Activo:
Nombre del Activo: Base de Datos de Clientes
Descripción del Activo: Base de datos que contiene información personal y financiera de los clientes de la empresa.
Ubicación Física: Centro de Datos Principal
Ubicación Lógica (si aplica): Servidor de Base de Datos "DB_Server_01"
3. Clasificación del Activo:
Confidencialidad: ALTA (x) MEDIA( ) BAJA ( )
Integridad: ALTA (x) MEDIA( ) BAJA ( )
Disponibilidad: ALTA ( ) MEDIA(x) BAJA ( )
4. Riesgos y Amenazas:
Descripción de los riesgos y amenazas potenciales para este activo: Posible acceso no autorizado por parte de empleados descontentos o ciberdelincuentes. Riesgo de pérdida de datos debido a fallos en el sistema o ataques de malware.
5. Medidas de Protección:
Descripción de las medidas de protección implementadas para este activo: Acceso restringido mediante autenticación de dos factores. Encriptación de datos sensibles. Auditorías regulares de seguridad. Respaldo diario de la base de datos.
6. Observaciones Adicionales:
Es importante mantener actualizado el inventario de la base de datos y realizar pruebas de seguridad periódicas para identificar posibles vulnerabilidades.



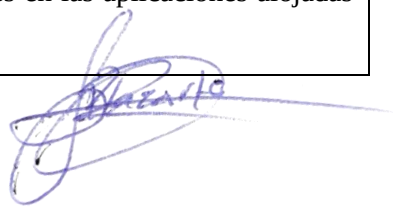
Formulario de Identificación de Activos de Información Fecha de Creación del Formulario: 8 de marzo de 2023
1. Información del responsable:
Nombre del responsable: Ing. Ana García Roman
Cargo: Coordinadora de Seguridad de la Información
2. Identificación del Activo:
Nombre del Activo: Aplicación Web de Gestión de Proyectos
Descripción del Activo: Aplicación web utilizada para la gestión y seguimiento de proyectos internos y externos de la empresa.
Ubicación Física: Servidor de Aplicaciones
Ubicación Lógica (si aplica): Aplicación "ProjectManager"
3. Clasificación del Activo:
Confidencialidad: ALTA (x) MEDIA( ) BAJA ( )
Integridad: ALTA (x) MEDIA( ) BAJA ( )
Disponibilidad: ALTA ( ) MEDIA(x) BAJA ( )
4. Riesgos y Amenazas:
Descripción de los riesgos y amenazas potenciales para este activo: Posible vulnerabilidad de seguridad en la aplicación que podría conducir a la exposición de información confidencial o alteración de datos. Riesgo de interrupción del servicio debido a fallos en el servidor o ataques de malware.
5. Medidas de Protección:
Descripción de las medidas de protección implementadas para este activo: Implementación de controles de acceso basados en roles para restringir el acceso a la información sensible. Monitoreo de seguridad continuo de la aplicación para detectar y mitigar posibles vulnerabilidades. Respaldo regular de la base de datos de la aplicación.
6. Observaciones Adicionales:
Es esencial realizar pruebas de penetración periódicas en la aplicación para identificar posibles puntos débiles y fortalecer las medidas de seguridad.



Formulario de Identificación de Activos de Información Fecha de Creación del Formulario: 8 de marzo de 2023
1. Información del responsable:
Nombre del responsable: Ing. Ana García Roman
Cargo: Coordinadora de Seguridad de la Información
2. Identificación del Activo:
Nombre del Activo: Servidor de Correo Electrónico
Descripción del Activo: Servidor que gestiona el correo electrónico interno y externo de la empresa.
Ubicación Física: Centro de Datos Principal
Ubicación Lógica (si aplica): Servidor de Correo "Mail_Server_01"
3. Clasificación del Activo:
Confidencialidad: ALTA (x) MEDIA( ) BAJA ( )
Integridad: ALTA (x) MEDIA( ) BAJA ( )
Disponibilidad: ALTA ( ) MEDIA(x) BAJA ( )
4. Riesgos y Amenazas:
Descripción de los riesgos y amenazas potenciales para este activo: Posible interceptación de correos electrónicos confidenciales. Riesgo de interrupción del servicio debido a ataques de denegación de servicio (DDoS) o fallos en el sistema.
5. Medidas de Protección:
Descripción de las medidas de protección implementadas para este activo: Implementación de filtros de correo electrónico para detectar y bloquear correos no deseados y maliciosos. Actualizaciones regulares de seguridad del servidor. Monitoreo constante del rendimiento y disponibilidad del servicio.
6. Observaciones Adicionales:
Es fundamental realizar copias de seguridad periódicas de los correos electrónicos y mantener una política de retención de datos adecuada para cumplir con los requisitos legales y de conformidad.

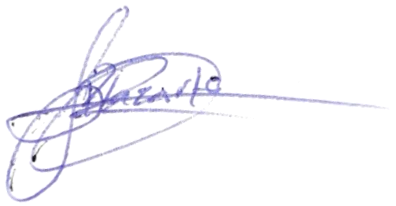


Formulario de Identificación de Activos de Información Fecha de Creación del Formulario: 8 de marzo de 2023
1. Información del responsable:
Nombre del responsable: Ing. Joel Veliz Albornoz
Cargo: Gerente de Tecnología
2. Identificación del Activo:
Nombre del Activo: Servidor de Aplicaciones Internas
Descripción del Activo: Servidor que aloja aplicaciones internas utilizadas para la gestión de recursos empresariales, como sistemas de contabilidad y recursos humanos.
Ubicación Física: Centro de Datos Principal
Ubicación Lógica (si aplica): Servidor "InternalApps_Server_01"
3. Clasificación del Activo:
Confidencialidad: ALTA (x) MEDIA( ) BAJA ( )
Integridad: ALTA (x) MEDIA( ) BAJA ( )
Disponibilidad: ALTA ( ) MEDIA(x) BAJA ( )
4. Riesgos y Amenazas:
Descripción de los riesgos y amenazas potenciales para este activo: Posible vulnerabilidad de seguridad en las aplicaciones que podrían permitir el acceso no autorizado o la manipulación de datos. Riesgo de interrupción del servicio debido a fallos en el servidor o ataques de malware.
5. Medidas de Protección:
Descripción de las medidas de protección implementadas para este activo: Implementación de parches de seguridad y actualizaciones regulares en las aplicaciones. Monitoreo continuo del rendimiento y la disponibilidad del servidor. Respaldos programados de las bases de datos de las aplicaciones.
6. Observaciones Adicionales:
Es importante establecer políticas de seguridad sólidas y realizar evaluaciones de riesgos periódicas para identificar posibles amenazas y vulnerabilidades en las aplicaciones alojadas en el servidor.



Formulario de Identificación de Activos de Información Fecha de Creación del Formulario: 8 de marzo de 2023
1. Información del responsable:
Nombre del responsable: Ing. Joel Veliz Albornoz
Cargo: Gerente de Tecnología
2. Identificación del Activo:
Nombre del Activo: Documentos Confidenciales de Proyectos
Descripción del Activo: Archivos electrónicos que contienen información confidencial relacionada con proyectos en curso, incluyendo planes estratégicos, presupuestos y cronogramas.
Ubicación Física: Carpeta compartida en el servidor de archivos
Ubicación Lógica (si aplica): Carpeta "Documentos_Proyectos" en el servidor de archivos
3. Clasificación del Activo:
Confidencialidad: ALTA (x) MEDIA( ) BAJA ( )
Integridad: ALTA (x) MEDIA( ) BAJA ( )
Disponibilidad: ALTA ( ) MEDIA(x) BAJA ( )
4. Riesgos y Amenazas:
Descripción de los riesgos y amenazas potenciales para este activo: Posible acceso no autorizado a los documentos confidenciales de proyectos. Riesgo de pérdida de información crítica debido a errores humanos o desastres naturales.
5. Medidas de Protección:
Descripción de las medidas de protección implementadas para este activo: Implementación de permisos de acceso basados en roles para restringir el acceso a los documentos solo a personal autorizado. Respaldo regular de los archivos de proyectos en un servidor seguro y fuera del sitio. Encriptación de archivos sensibles.
6. Observaciones Adicionales:
Es esencial sensibilizar al personal sobre la importancia de proteger la información confidencial de los proyectos y promover prácticas de seguridad de la información en todo momento.

Formulario de Identificación de Activos de Información Fecha de Creación del Formulario: 8 de marzo de 2023
1. Información del responsable:
Nombre del responsable: Ing. Ana García Román
Cargo: Coordinadora de Seguridad de la Información
2. Identificación del Activo:
Nombre del Activo: Documentos Confidenciales de Recursos Humanos
Descripción del Activo: Archivos electrónicos que contienen información personal y confidencial de los empleados de la empresa, como contratos, evaluaciones de desempeño y datos de nómina.
Ubicación Física: Carpeta compartida en el servidor de archivos
Ubicación Lógica (si aplica): Carpeta "Recursos_Humanos" en el servidor de archivos
3. Clasificación del Activo:
Confidencialidad: ALTA (x) MEDIA( ) BAJA ( )
Integridad: ALTA (x) MEDIA( ) BAJA ( )
Disponibilidad: ALTA ( ) MEDIA(x) BAJA ( )
4. Riesgos y Amenazas:
Descripción de los riesgos y amenazas potenciales para este activo: Posible acceso no autorizado por parte de empleados o ex empleados. Riesgo de divulgación de información confidencial debido a errores humanos o actividades maliciosas.
5. Medidas de Protección:
Descripción de las medidas de protección implementadas para este activo: Restricción de acceso basada en roles para limitar la visualización y modificación de los documentos solo a personal autorizado. Encriptación de archivos sensibles. Registro de auditoría para rastrear el acceso y las modificaciones realizadas en los documentos.
6. Observaciones Adicionales:
Es esencial capacitar al personal sobre las políticas de seguridad de la información y la importancia de proteger los documentos confidenciales de recursos humanos.



Formulario de Identificación de Activos de Información Fecha de Creación del Formulario: 8 de marzo de 2023
1. Información del responsable:
Nombre del responsable: Ing. Ana García Roman
Cargo: Coordinadora de Seguridad de la Información
2. Identificación del Activo:
Nombre del Activo: Servidor de Respaldos
Descripción del Activo: Servidor dedicado para almacenar copias de seguridad de los datos críticos de la empresa.
Ubicación Física: Centro de Datos Secundario
Ubicación Lógica (si aplica): Servidor de Respaldo "Backup_Server_01"
3. Clasificación del Activo:
Confidencialidad: ALTA ( ) MEDIA( ) BAJA (x)
Integridad: ALTA (x) MEDIA( ) BAJA ( )
Disponibilidad: ALTA (x) MEDIA( ) BAJA ( )
4. Riesgos y Amenazas:
Descripción de los riesgos y amenazas potenciales para este act ivo: Riesgo de pérdida de datos críticos debido a fallos en el hardware o software del servidor de respaldo. Posible acceso no autorizado a las copias de seguridad almacenadas.
5. Medidas de Protección:
Descripción de las medidas de protección implementadas para este activo: Implementación de tecnologías RAID para garantizar la redundancia y la integridad de los datos almacenados. Restricción de acceso físico y lógico al servidor de respaldo mediante controles de seguridad física y autenticación de usuarios.
6. Observaciones Adicionales:
Es fundamental realizar pruebas de restauración periódicas para verificar la integridad y la disponibilidad de las copias de seguridad almacenadas en el servidor de respaldo.

Activo	Amenazas Potenciales	Ejemplo de Amenazas Identificadas
Base de Datos de Clientes	- Acceso no autorizado por parte de empleados descontentos o ciberdelincuentes. Pérdida de datos debido a fallos en el sistema o ataques de malware.	Acceso no autorizado a la base de datos por parte de empleados descontentos. Ataque de malware que comprometa la integridad de los datos.
Servidor de Correo Electrónico	- Interceptación de correos electrónicos confidenciales. - Interrupción del servicio por ataques de denegación de servicio (DDoS) o fallos en el sistema.	Phishing dirigido a empleados para obtener acceso a correos electrónicos confidenciales. Ataque DDoS que provoque la caída del servidor de correo.
Aplicación Web de Gestión de Proyectos	- Vulnerabilidad de seguridad que conduzca a la exposición de información confidencial o alteración de datos. - Interrupción del servicio debido a fallos en el servidor o ataques de malware.	Inyección de SQL que permita a un atacante acceder a información confidencial. Ataque de denegación de servicio que paralice la aplicación de gestión de proyectos.
Documentos Confidenciales de Recursos Humanos	- Acceso no autorizado por parte de empleados o ex empleados. - Divulgación de información confidencial debido a errores humanos o actividades maliciosas.	Acceso no autorizado a los archivos de recursos humanos por parte de un ex empleado. Divulgación accidental de información confidencial debido a un error en los permisos de acceso.
Servidor de Respaldos	- Pérdida de datos críticos debido a fallos en el hardware o software del servidor. - Acceso no autorizado a las copias de seguridad almacenadas.	Fallo en el disco duro del servidor de respaldo que cause la pérdida de copias de seguridad. Intrusión de un hacker que acceda a las copias de seguridad almacenadas.

tabla que muestra las posibles vulnerabilidades en los sistemas, redes y procedimientos que podrían ser explotadas por las amenazas identificadas en los activos mencionados:

Activo	Vulnerabilidades Potenciales
Base de Datos de Clientes	- Vulnerabilidades de inyección SQL debido a entradas de usuario no filtradas. - Configuraciones de permisos incorrectas que permiten acceso no autorizado. - Falta de parches de seguridad para el sistema de gestión de bases de datos.
Servidor de Correo Electrónico	- Falta de autenticación multifactor que deja las cuentas de correo vulnerables al phishing - Configuraciones inseguras que permiten el acceso no autorizado al servidor de correo. - Ausencia de actualizaciones de seguridad para el servidor de correo.
Aplicación Web de Gestión de Proyectos	- Vulnerabilidades de inyección de código debido a entradas no validadas. - Configuraciones de seguridad débiles que permiten la escalada de privilegios. - Falta de actualizaciones de seguridad para la aplicación web.
Documentos Confidenciales de Recursos Humanos	- Configuraciones de permisos incorrectas en las carpetas compartidas que permiten el acceso no autorizado. - Falta de cifrado de datos para proteger la información sensible almacenada en los documentos - Riesgo de fuga de datos debido a la falta de control sobre el acceso y la distribución de los documentos.
Servidor de Respaldos	- Fallos de hardware que podrían causar la pérdida de datos almacenados en el servidor. - Falta de medidas de seguridad física que permiten el acceso no autorizado al servidor de respaldo. - Vulnerabilidades en el software de respaldo que podrían ser explotadas para acceder a las copias de seguridad.

Estas vulnerabilidades representan áreas específicas que deben ser abordadas para fortalecer la seguridad de los sistemas, redes y procedimientos dentro de la organización. Al identificar y mitigar estas vulnerabilidades, se reduce significativamente el riesgo de que las amenazas identificadas puedan causar daños a los activos de información de la empresa.

tabla que muestra el análisis de riesgos, evaluando la probabilidad y el impacto de que cada amenaza explote las vulnerabilidades identificadas en los activos de información, utilizando matrices de riesgos para asignar niveles de riesgo a cada amenaza:

Amenaza	Probabilidad (P)	Impacto (I)	Riesgo (P * I)	Nivel de Riesgo
Acceso no autorizado a la Base de Datos de Clientes	Alta	Alto	Muy Alto	Crítico
Interrupción del Servidor de Correo Electrónico	Medio	Alto	Alto	Alto
Explotación de Vulnerabilidades en la Aplicación Web de Gestión de Proyectos	Alto	Medio	Alto	Alto
Divulgación de Documentos Confidenciales de Recursos Humanos	Medio	Alto	Alto	Alto
Pérdida de Datos en el Servidor de Respaldos	Bajo	Alto	Medio	Medio

En esta tabla, se han evaluado la probabilidad y el impacto de cada amenaza en una escala de baja, media y alta. Luego, se calculó el riesgo multiplicando la probabilidad por el impacto. Con base en este cálculo, se asignó un nivel de riesgo a cada amenaza, que va desde Crítico hasta Medio, lo que permite priorizar las acciones de mitigación de riesgos en función de su importancia. Las amenazas con niveles de riesgo más altos, como Acceso no autorizado a la Base de Datos de Clientes y Interrupción del Servidor de Correo Electrónico, deben abordarse con urgencia para minimizar su impacto potencial en los activos de información de la organización.

tabla extendida que incluye la selección de controles de seguridad adecuados para mitigar o reducir los riesgos identificados:

Amenaza	Probabilidad (P)	Impacto (I)	Riesgo (P * I)	Nivel de Riesgo	Controles de Seguridad
Acceso no autorizado a la Base de Datos de Clientes	Alta	Alto	Muy Alto	Crítico	- Autenticación de dos factores para acceso a la base de datos. - Auditorías regulares de seguridad para detectar y prevenir accesos no autorizados. - Encriptación de datos sensibles en la base de datos.
Interrupción del Servidor de Correo Electrónico	Medio	Alto	Alto	Alto	- Implementación de firewalls y sistemas de filtrado de correos electrónicos para prevenir ataques de denegación de servicio (DDoS). - Configuración de respaldos y planes de recuperación ante desastres para minimizar el impacto de una interrupción.
Explotación de Vulnerabilidades en la Aplicación Web de Gestión de Proyectos	Alto	Medio	Alto	Alto	- Implementación de pruebas de seguridad periódicas para identificar y corregir vulnerabilidades en la aplicación. - Actualizaciones regulares de seguridad del software de la aplicación. - Configuración de reglas de seguridad en el servidor web para mitigar ataques conocidos.
Divulgación de Documentos Confidenciales de Recursos Humanos	Medio	Alto	Alto	Alto	- Control de acceso estricto a los archivos confidenciales de recursos humanos mediante permisos y autenticación. - Implementación de políticas de seguridad

Amenaza	Probabilidad (P)	Impacto (I)	Riesgo (P * I)	Nivel de Riesgo	Controles de Seguridad
					de la información que regulen el manejo y la distribución de documentos confidenciales. - Capacitación regular del personal sobre la importancia de proteger la información confidencial.
Pérdida de Datos en el Servidor de Respaldos	Bajo	Alto	Medio	Medio	- Implementación de sistemas de respaldo redundantes para minimizar el riesgo de pérdida de datos. - Almacenamiento de copias de seguridad en ubicaciones fuera del sitio para protección contra desastres. - Implementación de políticas de control de acceso físico al servidor de respaldo.

Estos controles de seguridad están diseñados para abordar las vulnerabilidades identificadas y reducir los riesgos asociados con las amenazas. Al implementar estos controles, la organización puede mejorar significativamente su postura de seguridad y proteger sus activos de información contra posibles ataques y brechas de seguridad.

Tabla extendida que incluye la selección de controles de seguridad basados en la norma ISO 27002 para mitigar o reducir los riesgos identificados:

Amenaza	Probabilidad (P)	Impacto (I)	Riesgo (P * I)	Nivel de Riesgo	Controles ISO 27002
Acceso no autorizado a la Base de Datos de Clientes	Alta	Alto	Muy Alto	Crítico	- Control de acceso (A.9.1): Implementación de autenticación de dos factores para acceder a la base de datos. - Gestión de accesos de usuarios (A.9.2): Aplicación de políticas de acceso para limitar los privilegios de los usuarios según el principio de mínimo privilegio. - Seguridad de la información en los procesos de negocio (A.14.1): Desarrollo de procedimientos para asegurar la integridad y confidencialidad de los datos en la base de datos.
Interrupción del Servidor de Correo Electrónico	Medio	Alto	Alto	Alto	- Gestión de incidentes de seguridad de la información (A.16.1): Desarrollo de planes de respuesta a incidentes para mitigar el impacto de interrupciones en el servicio de correo electrónico. - Continuidad del negocio y plan de recuperación ante desastres (A.17.1): Implementación de medidas para garantizar la disponibilidad y la recuperación rápida del servicio de correo electrónico en caso de interrupciones.
Explotación de Vulnerabilidades	Alto	Medio	Alto	Alto	- Seguridad en el desarrollo de sistemas y

Amenaza	Probabilidad (P)	Impacto (I)	Riesgo (P * I)	Nivel de Riesgo	Controles ISO 27002
en la Aplicación Web de Gestión de Proyectos					aplicaciones (A.14.2): Implementación de controles para identificar y mitigar vulnerabilidades en la aplicación web de gestión de proyectos durante el desarrollo y mantenimiento del software. - Gestión de vulnerabilidades técnicas (A.12.6): Realización de evaluaciones de seguridad periódicas para identificar y abordar nuevas vulnerabilidades en la aplicación web.
Divulgación de Documentos Confidenciales de Recursos Humanos	Medio	Alto	Alto	Alto	- Gestión de documentos (A.8.1): Desarrollo de políticas y procedimientos para gestionar de forma segura los documentos confidenciales de recursos humanos, incluyendo el control de acceso, el almacenamiento y la distribución de la información. - Concienciación, formación y educación en seguridad de la información (A.7.2): Capacitación regular del personal sobre la importancia de proteger la información confidencial y las medidas de seguridad aplicables.
Pérdida de Datos en el Servidor de Respaldos	Bajo	Alto	Medio	Medio	- Gestión de registros (A.12.4): Implementación de controles para garantizar

Amenaza	Probabilidad (P)	Impacto (I)	Riesgo (P * I)	Nivel de Riesgo	Controles ISO 27002
					la integridad y disponibilidad de los registros de respaldo y la gestión adecuada de las copias de seguridad. - Control de acceso a los sistemas de información (A.9.4): Aplicación de controles para limitar el acceso físico y lógico al servidor de respaldos, incluyendo el control de acceso basado en roles y la autenticación de usuarios.

Estos controles basados en la norma ISO 27002 están diseñados para abordar las vulnerabilidades identificadas y reducir los riesgos asociados con las amenazas, siguiendo las mejores prácticas de seguridad de la información establecidas por esta norma internacional. Al implementar estos controles, la organización puede mejorar significativamente su postura de seguridad y proteger sus activos de información contra posibles ataques y brechas de seguridad.

RESULTADOS ADICIONALES CON NORMATIVA ISO 270005

Que proporciona directrices para la gestión de riesgos de seguridad de la información, incluyendo la identificación de amenazas y vulnerabilidades.

tabla más detallada con ejemplos de vulnerabilidades y amenazas para diferentes tipos de activos, incluyendo hardware y software:

Tipo de Activo	Ejemplos de Vulnerabilidades	Ejemplos de Amenazas
Hardware	- Fallos de hardware debido a componentes defectuosos o desgaste. - Configuraciones predeterminadas no seguras en dispositivos de red. - Falta de actualizaciones de firmware para corregir vulnerabilidades conocidas.	- Interrupción del servicio debido a fallos de hardware. - Acceso físico no autorizado a los dispositivos de hardware. - Ataques de ingeniería social para obtener acceso a dispositivos mediante engaños a los empleados.
Software	- Fallos de seguridad en el código, como vulnerabilidades de inyección de SQL o XSS.	- Explotación de vulnerabilidades de software por parte de hackers o malware.

Tipo de Activo	Ejemplos de Vulnerabilidades	Ejemplos de Amenazas
	- Configuraciones por defecto que permiten el acceso no autorizado. - Falta de parches de seguridad para corregir vulnerabilidades conocidas.	- Robo de datos confidenciales a través de brechas de seguridad en aplicaciones. - Ransomware que aprovecha vulnerabilidades de software para cifrar archivos y exigir rescates.
Redes	- Configuraciones de red no seguras, como contraseñas débiles o ausencia de firewalls. - Falta de segmentación de red que permite la propagación de ataques. - Protocolos desactualizados o sin cifrado.	- Ataques de denegación de servicio (DDoS) para saturar la red y dejarla inaccesible. - Intercepción de tráfico de red para robar información confidencial. - Ataques de phishing dirigidos a obtener credenciales de acceso a la red.
Datos	- Almacenamiento de contraseñas en texto plano en bases de datos. - Falta de cifrado de datos sensibles en tránsito y en reposo. - No implementación de políticas de retención y eliminación segura de datos.	- Fuga de datos debido a un acceso no autorizado a bases de datos. - Robo de información confidencial durante la transmisión de datos no cifrados. - Pérdida de datos debido a la eliminación accidental o maliciosa por parte de empleados.

Es importante realizar evaluaciones de riesgos regulares para identificar y abordar las vulnerabilidades específicas que puedan existir en el entorno de una organización.