UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

Facultad de Ciencias Administrativas, Contables y Comercio

Carrera de Gestión de la información Gerencial

TRABAJO DE UNIDAD DE INTEGRACIÓN CURRICULAR

Previo a la obtención del título de:

Licenciada en Gestión de la Información Gerencial

TEMA:

La Seguridad de Datos como Estrategia en la Gestión de Información en el Departamento de Talento Humano de la Empresa Fresh Fish del Ecuador, 2024 (Estudio de caso).

AUTORA:

María Fernanda Anchundia Briones

MANTA – ECUADOR

2024

Tema:

La Seguridad de Datos como Estrategia en la Gestión de Información en el Departamento de Talento Humano de la Empresa Fresh Fish del Ecuador, 2024 (Estudio de caso).

Uleam UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ	**NOMBRE DEL DOCUMENTO:** **CERTIFICADO DE TUTOR(A).**	**CÓDIGO: PAT-04-F-004**
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO BAJO LA UNIDAD DE INTEGRACIÓN CURRICULAR	**REVISIÓN: 1**
		Página 1 de 1

CERTIFICACIÓN

En calidad de docente tutor de la Facultad Ciencias Administrativas, Contables y Comercio de la Universidad Laica "Eloy Alfaro" de Manabí, CERTIFICO:

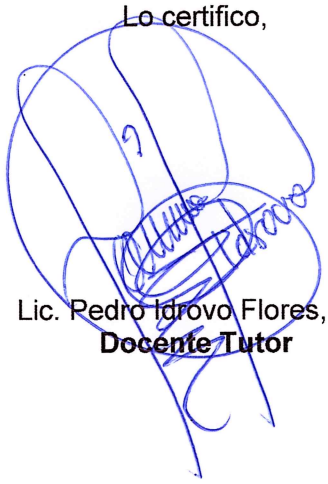
Haber dirigido, revisado y aprobado preliminarmente el Trabajo de Integración Curricular: Estudio de Caso bajo la autoría de la estudiante ANCHUNDIA BRIONES MARÍA FERNANDA legalmente matriculada en la carrera de Gestión de la Información Gerencial, período académico 2024 (2), cumpliendo el total de 240 horas (96 FASE I: DISEÑO y 144 horas FASE II: Análisis de Resultados), cuyo tema del proyecto es "La seguridad de datos como estrategia en la gestión de información en el departamento de Talento Humano de la Empresa Fresh Fish del Ecuador, 2024 (Estudio de caso)".

La presente investigación ha sido desarrollada en apego al cumplimiento de los requisitos académicos exigidos por el Reglamento de Régimen Académico y en concordancia con los lineamientos internos de la opción de titulación en mención, reuniendo y cumpliendo con los méritos académicos, científicos y formales, y la originalidad del mismo, requisitos suficientes para ser sometida a la evaluación del tribunal de titulación que designe la autoridad competente.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

Manta, 13 de diciembre de 2024.

Lo certifico,



Lic. Pedro Idrovo Flores, Mg
Docente Tutor

Autoría

Yo, María Fernanda Anchundia Briones, con cédula de identidad N° **131683861-2**, perteneciente a la Universidad Laica Eloy Alfaro de Manabí, egresada de la Carrera de Gestión de la Información Gerencial de la Facultad de Ciencias Administrativas, Contables y Comercio, declaro libremente que soy autora de la investigación bajo la modalidad estudio de caso cuyo tema es: "La Seguridad de Datos como Estrategia en la Gestión de Información en el departamento de Talento Humano de la Empresa Fresh Fish del Ecuador, 2024", la cual expreso que el contenido generado en este estudio es de mi propiedad intelectual.

Referente a esto, reconozco que el conocimiento adquirido en este trabajo corresponde únicamente a la Universidad Laica Eloy Alfaro de Manabí (ULEAM).

María Anchundia

Srta. María Fernanda Anchundia Briones

Dedicatoria

Dedico este trabajo especialmente a Dios:

Por haberme dado la vida y por permitirme llegar hasta aquí, debido a que, me dio la fuerza y sabiduría necesaria para desarrollar este estudio y porque nunca me abandonó en las adversidades de mi carrera, gracias por siempre estar ahí y por llenarme de tu bendita esperanza cada día.

A mis padres Sr. Darwin Anchundia Cedeño y Sra. Mónica Briones Vega:

Por su determinada paciencia y apoyo que me dieron a través de los años, por los valores y la formación académica que me proporcionaron, la cual fue de mucha ayuda para que yo pudiera llegar hasta donde estoy, es por ello, que su guía ha sido un motor fundamental en mi vida, porque gracias a ello soy una persona dedicada, grata y responsable en cada actividad que realizo.

A mis hermanos: Angie Andrea Anchundia y Darwin Maximiliano Anchundia Briones:

Por ser cómplices en este proceso y darme el ánimo necesario de continuar y nunca rendirme, además, por ser partícipes de cada aventura ejecutada y por haber estado en cada etapa difícil de mi vida, por su acompañamiento y apoyo incondicional, para el cumplimento de mis objetivos.

Srta. María Fernanda Anchundia Briones

Reconocimiento

En esta travesía estudiantil le agradezco a la universidad por haberme recibido y darme la oportunidad de estudiar, además, de la preparación estudiantil que me dio a través de los años, así mismo, a la Facultad de Ciencias Administrativas, Contables y Comercio, que me apoyó en este trayecto académico. Además, le agradezco a los docentes de la carrera de Gestión de la Información Gerencial por haberme acogido y dado los conocimientos necesarios para mi formación profesional, llenos de paciencia y de consejos brindados en estos cuatro años.

Por último, le agradezco a mi tutor el Lic. Pedro Manuel Idrovo Flores, Mg., porque su conocimiento me ayudó a gestionar cada una de las actividades de mi estudio, además, sus consejos y enseñanzas quedarán impregnadas en mí, dado que, su orientación y perseverancia me ayudó a cumplir con este objetivo de vida. Es por ello, que este proyecto no hubiera sido posible sin su apoyo, debido a que, creyó en mí y nunca me abandonó en esta fase que es fundamental para mi vida.

Srta. María Fernanda Anchundia Briones

Índice

Introducción

El presente estudio de caso tiene como asunto la Seguridad de Datos como Estrategia en la Gestión de la Información en el Departamento de Talento Humano de la Empresa Fresh Fish del Ecuador, año 2024. Así mismo, la motivación para realizar este estudio es ayudar a las entidades a salvaguardar la información de manera sólida, para asegurar su autenticidad y vigor en los métodos que maneja cada área. Por ende, es esencial brindar estrategias para impulsar a las organizaciones que padecen por lo mismo, dado que, puedan combatirlos sin problema alguno, por causa de que, estos dañan la decencia de la documentación y perjudican los métodos de gestión.

Este estudio refleja la importancia de una buena seguridad de datos, puesto que, es prestigioso proteger la documentación digital o física de la entidad contra acceso no delegados o robo de reseñas que se desarrolle durante el período de existencia de los archivos; por otra parte, la gestión de información reside en administrar los registros que manejan los departamentos, para garantizar que los informes sean útil y accesible para quienes lo soliciten.

La finalidad de esta investigación es revisar las múltiples estrategias que existen alrededor del mundo, para garantizar una buena protección de documentos en una organización, dado que con ello se puede reconstruir la administración de la información, para asegurar la durabilidad y decencia. Por otro lado, el propósito principal de este estudio de caso es analizar la seguridad de datos para ayudar a la gestión de información en el departamento de talento humano de la empresa Fresh Fish del Ecuador en el año 2024.

Por otra parte, para alcanzar los objetivos de la investigación se opta por utilizar el alcance explicativo y descriptivo, para exponer los acontecimientos encontrados, así mismo, para su desarrollo se utiliza el método análisis-Síntesis, bibliográfico, inductivo-deductivo la cual

permite una explicación clara y precisa sobre el estudio. Además, las técnicas que se aplica en esta indagación son: la investigación documental, la observación directa y una entrevista estructurada dentro del campo de labor, para obtención de información relevante del tema.

Este estudio de caso se divide en dos partes, para ofrecer una estructura más clara y organizada de la investigación. Se comienza con la primera fase, donde se sumerge con el tema para comprender la problemática, de igual modo, la introducción, antecedentes investigativos, definición del caso, justificación, objetivos, marco conceptual y marco metodológico. Finalmente, en la segunda fase se ejecuta los resultados obtenidos, análisis de resultados, conclusiones, recomendaciones, referencias, anexos y propuestas de la investigación.

En definitiva, se espera que los resultados alcanzados en este estudio sean una columna fundamental para la empresa Fresh Fish, debido a que, permite una senda firme en los datos que se ejecuta en cada una de las actividades, de esta manera el departamento de talento humano certifica que su información no es vulnerable contra los ataques cibernéticos, que afectan la integridad de sus documentos en el sistema.

Antecedentes Investigativos

Fresh Fish del Ecuador, es una empresa privada, procesadora de pescado ubicada en el cantón Manta vía San Mateo Km 4.5 sitio Piedra Larga; tiene como finalidad ofrecer productos frescos de alta calidad como los son el atún, dorado, albacora, bonito, wahoo entre otros. Esta empresa forma parte del Grupo Corporativo Buehs el cuál ha sido dirigido por el capitán Bernardo Buehs por más de cuarenta años consecutivos, dicho hombre quien desde los catorce años empezó con la pesca artesanal y con esfuerzo y dedicación logró levantar cinco barcos pesqueros con alta tecnología junto a sus tres hijos.

Así mismo, su misión es "ofrecer los mejores productos de pescado congelado y /o fresco a todos los mercados del mundo. Siendo conscientes de nuestra responsabilidad con el medio ambiente y generaciones futuras. No solo entendemos la riqueza como la utilidad para nuestros accionistas sino también como el crecimiento de nuestros clientes, empleados, proveedores y sectores sociales asociados con nuestro negocio, manteniendo siempre nuestro compromiso ético, moral y transparente en cada una de las actividades que desempeñamos."; por otro lado, su visión es que "FRESH FISH del Ecuador será el referente mundial de productos congelados y/o frescos del mar, con una alta calidad y disponibilidad en los mercados a los que atiende."

En la presente investigación se tomó como referencia investigaciones internacionales, nacionales y locales realizadas por varios autores sobre las variables: Seguridad de Datos y Gestión de Información, con la finalidad de servir de soporte para orientar el estudio:

Asurza (2022), en Lima-Perú realiza una tesis la cual tiene como tema "Diseño de una Arquitectura de Seguridad Informática para Incrementar la Seguridad de Información en la Empresa Bafing S.A.C. en 2021", el objetivo de su investigación es demostrar que el diseño de una arquitectura de seguridad informática puede mejorar la seguridad de información de la

empresa Bafing S.A.C. Así mismo, este estudio utiliza la entrevista, análisis documental, observación y encuesta como instrumentos para la recolección de datos. Los resultados obtenidos mostraron mejoras en la seguridad de información analizadas en base a la situación actual de la empresa auditada Bafing S.A.C.

Este trabajo de investigación concluye que, un entorno de seguridad gestionado a través de soluciones de seguridad ofrece un mayor potencial de cobertura de seguridad frente a arquitectura o plataforma conformada por una única suite. Por tanto, las empresas deberán buscar las combinaciones de software de seguridad, que en conjunto brinden una mayor seguridad al ambiente de TI y a sus servicios.

Miranda (2021) tiene como investigación el "Mapeo sistemático de metodologías de Seguridad de la Información para el control de la gestión de riesgos informáticos", está indagación se desarrolla en Guayaquil-Ecuador, con el propósito de implementar metodologías de seguridad que funcionen como base en la elaboración de prototipos de modelos. Para el desarrollo de este trabajo, se realiza un mapeo sistemático en varios repositorios online como: SCIENCEDIRECT, WEB OF SCIENCE (WOS), EBRARY, SCOPUS, entre otros. Por otro lado, se utiliza el método analítico-descriptivo, de tipo experimental con enfoque cuantitativo para el análisis de trabajos, además, se realiza una matriz de posibles riesgos que afecten la seguridad de los datos o información.

Los resultados conseguidos en los 28 artículos selectos muestran una utilidad en las ventajas y desventajas que ayuda a las metodologías de seguridad, a través de la identificación de activos, debilidades, amenazas y riesgos para así solucionar los problemas en la integridad de la información y mejorar así la gestión en función de los resultados alcanzados en estudios anteriores. Se concluye que, los métodos de seguridad planteadas proveen un sistema de

seguridad óptimo para organizaciones públicas y privadas; las cuales son la base para la cooperación de prototipos de seguridad para reducir vulnerabilidades y amenazas en los sistemas de información.

Marín et al. (2021), presenta el estudio: "La Seguridad Informacional en el Ministerio de Transporte y Obras Públicas", en Portoviejo-Ecuador, cuyo objetivo principal es evaluar el estado de la Seguridad Informacional en el Ministerio de Trasporte y Obras Públicas en Portoviejo, en este estudio se utiliza el método de tipo descriptivo y retrospectivo con un enfoque cuantitativo-cualitativo, a través de la aplicación de métodos y técnicas, tales como: histórico-lógico, inductivo-deductivo, analítico-sintético, que ayuda a fundamentar la investigación.

Por otro lado, los resultados muestran un nivel de efectividad, debido a que, se determina que la empresa cuenta con buena Seguridad Informacional. Por ende, los análisis específicos realizados y el recorrido cognitivo seguido se transformaron en sustento teórico del trabajo; al expresar las potencialidades en el interior del Ministerio de Transporte y Obras Públicas en Portoviejo, alineadas administrativamente ayudan a tener una buena seguridad informacional en la institución seleccionada para este estudio.

Pérez, Geizzelez y Rosales (2021), desarrolla una investigación en Colombia, titulado "Gestión de información para la vigilancia tecnológica en empresas del sector energético de la Guajira colombiana", la finalidad de la investigación es identificar el enfoque de la gestión de información para la vigilancia tecnológica en las empresas de energía solar fotovoltaica de uso residencial en la provincia de La Guajira, Colombia. La metodología del trabajo es descriptiva, diseño no experimental, transeccional, la técnica de recolección de datos es la encuesta, y se utiliza como instrumento un cuestionario escala Likert de 60 puntos con 5 opciones de respuesta.

Por lo tanto, los resultados evidencian una templada apariencia de todos los indicadores oportunos a la dimensión, articulados con la gestión de información orientada a la toma de decisiones y la tecnología. Esto permite tener la base diagnóstica que determina la enunciación de la propuesta, para llegar a la conclusión de que los lineamientos planteados forman una estrategia efectiva para fortificar la gestión de la información como soporte al proceso de levantamiento de tecnología para sistemas solares residenciales.

Terán (2021), presenta como trabajo de grado la "Seguridad en la gestión de la información para las organizaciones públicas desde el enfoque ISO/IEC 2700: un mapeo sistemático" en Guayaquil-Ecuador, con el objetivo de analizar los riesgos que enfrentan las organizaciones públicas, para resolver el robo en las bases de datos de la información ingresada y tener en cuenta el uso de la metodología para preservar la garantía de la seguridad de la información y al administrar los riesgos de forma más efectiva. Por otro lado, se utiliza el método deductivo y la investigación exploratoria, así mismo, se realiza un estudio a la metodología MAGERIT que protege la información en su confidencialidad y disponibilidad dando garantía a la seguridad del sistema en organizaciones públicas.

Finalmente, los resultados obtenidos en el artículo seleccionado, da un enfoque de interés y un control de factores de seguridad de la información, para tomar en cuenta que MAGERIT sigue siendo una medida de seguridad que mitiga las amenazas y riesgos de sus procesos, estos incluyen el mapeo, debido a que, da como requerimiento una validación para ser considerados en la industria del desarrollo de software. En definitiva, el prototipo de gestión de riesgo mejora la seguridad e incluso la privacidad de la información en las organizaciones públicas.

Barzaga et al. (2019), efectúa un artículo titulado "Gestión de la información y toma de decisiones en organizaciones educativas", en Portoviejo-Ecuador, su estudio tiene como

finalidad analizar la gestión de la información y el conocimiento para la toma de decisiones de las organizaciones educativas de Portoviejo. Por otro lado, la metodología reside en el análisis documental, así mismo, el método auténtico lógico y el sistémico estructural funcional.

Por ende, los resultados destacan la industria de la interacción entre administración de la información, la comprensión y la toma de decisiones, con la gerencia en las entidades educativas, así como la mejora de la gestión de riesgo y el conocimiento, en las organizaciones e instituciones educativas. Los autores concluyen que, el proceso de transformación de los datos en indagación y conocimiento es primordial, para la toma de decisiones informadas en las organizaciones educativas de Portoviejo.

Definición del Caso de Estudio

Fresh Fish del Ecuador, es una empresa dedicada a la producción y distribución de pescado de manera nacional e internacional, fue fundada en el 2007 y cuenta con un organigrama que representa gráficamente la jerarquía de la compañía como: el departamento administrativo, el responsable de recepción de pesca y logística, mantenimiento, seguridad física, producción y un responsable del aseguramiento de la calidad del producto, entre otros. Por otro lado, la entidad cuenta con máquinas de alta tecnología para ejecutar sus procesos y así cumplir con las exigencias de cada uno de sus clientes.

Es por ello, que la seguridad de datos es importante en cualquier empresa a nivel mundial, debido a la demanda creciente de información que se gestiona hoy en día y al aumento de amenazas cibernéticas que afectan la integridad de esta. Por lo tanto, al implementar mecánicos de privacidad, confidencialidad y disponibilidad de la información, asegura que los documentos no se encuentren en riesgo de ser alterados por cualquier usuario.

Sin embargo, dentro del departamento de talento de la empresa Fresh Fish, se pudo observar varias falencias internas sobre la seguridad informática, la cual genera un incumplimiento normativo que afecta significativamente la eficiencia y eficacia de los procesos que maneja el departamento. Una de las dificultades evidentes es la pérdida de datos del personal, carpetas de los trabajadores desordenadas e incompletas, además, no cuentan con un control de acceso a los sistemas de información, ni mecanismos de seguridad; estas cuestiones generan dificultad en la toma de decisiones informadas y al acceso oportuno de los mismos.

Si bien es cierto, la seguridad de datos hoy en día es fundamental, puesto que, si no la administran de manera adecuada la privacidad y la integridad de la información estarían en peligro de ser modificadas. Por tanto, es primordial que Fresh Fish tome medidas relevantes para

salvaguardar los datos que se gestiona en la empresa y así evitar conflictos internos y externos ocasionados entre los colaboradores del departamento de talento humano.

Así mismo, este estudio se relacionó con varias asignaturas vistas en la carrera de Gestión de la Información como: ecología de la información, gestión de procesos, ética y responsabilidad social en la información, gestión de la información y la calidad total de la información. Estas materias se relacionan entre sí para asegurar que la información se gestione de manera ética, consciente, eficaz y eficiente en cualquier organización.

Ante estas dificultades focalizadas, se formula el problema de la siguiente manera: ¿Cómo ayudará la seguridad de datos en la gestión de información en el departamento de talento humano de la empresa Fresh Fish del Ecuador en el año 2024?, esta interrogante permitirá salvaguardar el uso eficiente de los documentos que han sido generados, recibidos, examinados y guardados en la compañía y así certificar que esta pueda desarrollar sus operaciones sin ningún riesgo.

Finalmente, se presentan las principales interrogantes que guiará de forma efectiva el estudio a realizar.

- ¿Cuáles son los soportes teóricos de la seguridad de datos y gestión de la información?
- ¿Cuál es el estado actual de la seguridad de datos en la gestión de información?
- ¿Cuáles son los efectos ocasionados de la seguridad de datos en la gestión de información?
- ¿Cuál es el diseño de los protocolos para la implementación de la norma ISO en la seguridad de datos como estrategia en la gestión de información?

Justificación del Caso de Estudio

El presente estudio de investigación se enfoca en analizar la seguridad de datos para ayudar a la gestión de información, en el departamento de talento humano de la empresa Fresh Fish del Ecuador, año 2024. Este trabajo se orienta en mejorar el respaldo y ética de documentos de la empresa, para garantizar una buena administración de información en los procesos que realiza el departamento.

Según Rodríguez et al. (2020) “Al carecer de mecanismos de seguridad, las organizaciones se encuentran vulnerables y puede ser responsables de crear riesgos de alto impacto, daños innecesarios causando pérdida de información confidencial” (2020, pág. 4).

Es por ello, que es importante ejecutar este estudio de caso, debido a que, si no se toman medidas necesarias para preservar la información, la empresa corre peligro en tener fugas de datos que perjudiquen la imagen y reputación de esta. Por lo tanto, al adoptar disposiciones de seguridad la entidad protege la documentación de sufrir algún percance o manipulación que afecte la toma de decisiones.

Esta investigación es factible porque se cuenta con el apoyo de bibliografías y documentación que respaldan de una manera efectiva este estudio, así como la colaboración del personal del departamento de talento humano de la empresa Fresh Fish, debido a que brindan información que se requiera para desarrollar esta investigación, así mismo, se cuenta con el apoyo del tutor quien guía de forma apta el estudio para el cumplimiento de los objetivos propuestos.

La relevancia de este estudio radica en la prevención de documentos confidenciales en la gestión de información, debido a que, es esencial proteger los activos de la empresa y así mantener la confianza del cliente y de los proveedores viables. Además, sin una seguridad de

datos sólida, los archivos pueden estar expuestos a amenazas del interior y exterior que podrían perturbar la estabilidad de la entidad y exhibir los datos confidenciales de los procesos que esta realiza.

Por otro lado, el impacto social de este estudio consiste en los beneficios que obtendrá la empresa y el personal al culminar esta investigación, puesto que, se plantearán soluciones para optimizar la seguridad de datos que maneja la empresa; de ese modo, Fresh Fish no correrá riesgo en la pérdida ni divulgación de información que afecte la integridad de esta y de sus procesos. Dicho de otra manera, la compañía va a amenorar riesgos y fortalecer la confianza del comprador, para mantenerse competitiva en un entorno empresarial cada vez más moderno.

Objetivos del Estudio de Caso

Objetivo General

Analizar la seguridad de datos para ayudar a la gestión de información en el departamento de talento humano de la empresa Fresh Fish del Ecuador en el año 2024.

Objetivos Específicos

- Definir la seguridad de datos y la gestión de información.
- Determinar el estado actual de la seguridad de datos en la gestión de información en el departamento de talento humano de la empresa Fresh Fish.
- Identificar los efectos ocasionados en la seguridad de los datos y la gestión de información.
- Diseñar protocolos para la implementación de la norma ISO en la seguridad de datos como estrategia en la gestión de información.

Marco Conceptual

Seguridad de Datos

Qué es Seguridad

Sin bien es cierto, la seguridad es un activo sustancial para cualquier interesado, debido a, la magnitud que tiene alrededor del mundo, Gomez (2022) redacta lo siguiente:

> Hace referencia a la protección frente a un peligro o amenaza potencial, o a la ausencia de riesgo; o bien a la certeza e inexistencia de dudas. Se utiliza de manera específica en áreas muy diversas, como ejemplos de ello, se puede mencionar: seguridad social, seguridad ciudadana, seguridad informática, seguridad alimentaria, seguridad vial, entre otros (pág. 8).

En concordancia con el autor, la seguridad viene siendo la protección total ante cualquier amenaza o peligro que perjudique la estabilidad de un usuario, así mismo, permite promover prácticas o políticas que cause el respaldo de los ciudadanos ante posibles amenazas que afecten la decencia, además, es fundamental para los individuos, porque con ello se puede disminuir cualquier peligro. Sin embargo, la mayoría de las personas enfrentan desafíos significativos con su estabilidad, debido a que, existen ataques cibernéticos que manipulan la información que se ha establecido y afectan la moralidad de sus datos e información, no obstante, mantener una buena seguridad afirma que la documentación no esté expuesta ante nadie.

Seguridad de Datos

Gamboa (2020), en su estudio Importancia de la seguridad informática y ciberseguridad en el mundo actual, redacta lo siguiente:

> Es el conjunto de medidas preventivas y reactivas que permiten resguardar o proteger la información, manteniendo la confidencialidad, integridad y la autenticación de los datos,

> tanto en el almacenamiento como en el tránsito. Cabe aclarar que el término seguridad de información difiere a seguridad informativa, debido a que el primero abarca un rango más amplio, llegando a tener una importancia global en otros aspectos que no involucran a la Ciberseguridad (pág. 2).

Según lo mencionado, la seguridad de datos son procedimientos anticipados la cual permite a las compañías proteger la información que manejan en todos los departamentos, por ende, es importante un monitoreo de todas las actividades que maneja la entidad, para mantener la confidencialidad de los datos. Es por ello, que es decisivo implementar disposiciones para precautelar y asegurar la confidencialidad de los datos de cada individuo, debido a que, la información juega un papel primordial en cualquier organización.

Por otro lado, esto ayuda a las instituciones a tener más control sobre su documentación para que esta no pueda ser transformada por ninguna persona, la cual permite tener una evaluación constante en los procesos que gestiona cada departamento, para que no haya involucrados que perjudiquen la reputación de la compañía e inquieten las actividades que realizan al exponer cada información de la empresa.

Importancia de la Seguridad de Datos

Según el artículo, Análisis de las características del sector microempresarial en Latinoamérica y sus limitantes en la adopción de tecnologías para la seguridad de la información, el autor redacta lo siguiente:

> La seguridad de información hace referencia a la protección del activo más importante que produce una empresa como lo es la información relacionada a su actividad, esta debe ser protegida de cualquier situación ya sea por eventos naturales o provocados, que

> produzcan falla en la infraestructura de red, incluye también los ataques por el uso de virus informáticos, vandalismo entre otros (Jurado, Yarad, & Carrión, 2020, pág. 4).

Según lo planteado, la importancia de la seguridad de datos radica en la protección total de los documentos que maneja una organización, puesto que, se debe resguardar la información ante cualquier situación que afecte su moralidad y estabilidad. Además, esto implica preservar los informes de una empresa ante una variedad de amenazas, debido a que, puede ser ocasionado por acciones intencionadas de un individuo. Sin embargo, a pesar de lo relevante que es la seguridad de los datos para las empresas, muchas de estas no la aplican adecuadamente, lo que causa que su reputación se vea afectada por la sociedad. Es por ello, que al tener un respaldo de seguridad de datos mejora la estabilidad e integridad de la documentación de una empresa.

Principios de la Seguridad de Datos

Según Cando (2024), en su trabajo de grado para mejorar la seguridad de la información digital, manifiesta lo siguiente sobre los principios:

> La tríada CID, compuesta por los principios de Confidencialidad, Integridad y Disponibilidad, es un conjunto de conceptos fundamentales en el ámbito de la seguridad de la información. Estos principios se utilizan para garantizar la protección y el adecuado manejo de los datos y sistemas en entornos digitales" (pág. 29).

Según lo indicado por el autor, para lograr una buena seguridad de datos en una entidad, es importante considerar la aplicación de la CID, debido a que, con ello se garantiza una adecuada conservación en los documentos y archivos de una institución, así mismo, la aplicación de estos principios permite certificar la protección total de la información brindada. Esto no solo mejora la estabilidad, sino que permite gestionar adecuadamente la documentación que se ha

determinado, para salvaguardar de manera correcta los informes de una empresa y lograr una confianza efectividad y eficaz en los fundamentos.

Efectos de la Seguridad de Datos

Pérez (2009), citado en Ochoa (2023), explican que, “un riesgo de seguridad de la información es cuando se da una amenaza con una vulnerabilidad, como consecuencia se da la pérdida o daño de información, falta de privacidad, fraude, y una posible caída de la confianza de los clientes”. (2023, pág. 10)

Como señala el autor, existe varias secuelas al no tener decretos de seguridad en los datos que maneja una empresa u organización como: extravío o daño de información que afecta totalmente la integridad de estos, debido a que ocasiona conflictos en la reputación y pérdida de competitividad en los productos que ofrece la compañía. Es por ello, que una mala protección de datos trae varios desenlaces negativos en una entidad, puesto que, si no se cuenta con una buena estabilidad en los datos, estos estarían perjudicados por una falta de privacidad en la documentación.

Normas y Estándares Internacionales de Seguridad de Datos

Se afirma que “existen numerosas normas y estándares internacionales que proporcionan pautas y mejores prácticas para la seguridad de la información, como ISO 27001, NIST SP 800-53, PCI DSS, HIPAA, entre otros”. (Cando, 2024, pág. 36)

Como señala el autor, al efectuar estas normas se espera mantener un control en la seguridad de los datos en las entidades, dado que, la aplicación de cualquiera de estos estándares va a asegurar que la documentación se encuentre en total privacidad y así prevenir riesgos de cualquier tipo en las organizaciones, además, va a mejorar los sistemas informáticos.

Gestión de Información

Qué es Gestión

El autor en su investigación manifiesta lo siguiente sobre que es la gestión:

> Conjunto de acciones o diligencias que permiten la realización de cualquier actividad o el cumplimiento de un deseo. Dicho de otra manera, al hablar de una gestión se hace referencia a todos aquellos trámites que se deben realizar con la finalidad de resolver una situación o de materializar un proyecto" (Martínez, 2024, pág. 1).

Desde el punto de vista del escritor, la gestión viene siendo un compuesto de funciones con la cual se realiza cualquier proceso, puesto que, con esto se puede desarrollar trámites que las instituciones necesiten. Además, la gestión es un asunto que inicia desde la planificación hasta la ejecución y seguimiento continuo de las actividades, para lograr con los objetivos propuestos. No obstante, esto no solo permite realizar diligencias para cumplir con los planes establecidos, sino que elabora los métodos planteados, para mejorar su productividad y que esta pueda ser gestionada de una manera efectiva en los departamentos o áreas de una organización.

Qué es Información

Se denomina información a un "Conjunto de datos, ya procesados y ordenados para su comprensión, que aportan nuevos conocimientos a un individuo o sistema sobre un asunto, materia, fenómeno o ente determinado" (Valls, 2021, pág. 7).

De acuerdo con el autor, la información es un grupo de documentos que ya han sido procesados para la compresión de cualquier individuo, así mismo, es fundamental porque con ella se puede tomar decisiones informadas y actualizadas. Además, esta no solo brinda datos transformados, si no que ayuda aumentar el conocimiento sobre un hecho o asunto que haya

sucedido. Es decir, la indagación es importante en cualquier entidad, puesto que, brinda ilustraciones notables a los usuarios, para que estos pueden descifrar un tema en específico.

Gestión de Información

Jumbo y Salguero (2024), en su tesis Gestión de la información en la Extensión Pujilí de la Universidad Técnica de Cotopaxi, redacta lo siguiente:

> La Gestión de la Información se define como un conjunto de acciones que abarcan desde la prospección hasta la diseminación de información, así como la aplicación de métodos y herramientas que respalden estas actividades. Este enfoque abarca todo el ciclo informativo y tiene como objetivo principal proporcionar un fundamento sólido para las actividades y tareas llevadas a cabo por los sujetos organizacionales (pág. 24).

La gestión de la información son acciones con la cual se recopila, se almacena y se distribuye la documentación, con el fin de llevar un orden de todos los datos que maneja una entidad. Por lo tanto, es relevante tener herramientas que respalden los procesos que ejecuta un área y así mantener el ciclo de la información en todos sus ámbitos. Además, permite administrar de manera efectiva los datos que maneja una empresa, para tener una mejor organización de los informes que se manipulan y se pueda asegurar que los archivos estén ordenados correctamente, por consiguiente, muchas compañías tienen equipos que permiten gestionar de manera correcta sus datos, para su clasificación, reserva y protección de una manera eficaz, para garantizar su uso consecutivo.

Importancia de la Gestión de Información

Según Inca (2023) “la gestión de datos desempeña un rol crucial en la época digital, al ofrecer a las empresas un sólido fundamento para la toma de decisiones estratégicas, el reconocimiento de áreas de mejora y la optimización de operaciones empresariales” (pág. 28).

La gestión de información es trabajador significativo para garantizar áreas de mejora continua, esto implica la recolección de documentación, así como su análisis e interpretación de datos en distintas fuentes informáticas. Si bien es cierto, esto ofrece una base en la toma de decisiones estratégicas en una organización, puesto que la investigación tiene que estar en orden y completa para ser interpretada de forma adecuada por los usuarios existentes. Además, las organizaciones utilizan los datos para automatizar los procesos que manejan y así mejorar sus servicios de acuerdo con las expectativas de los consumidores.

Retos que Implica la Gestión de Información

> Hay grandes desafíos que enfrenta la gestión de la información dentro de las empresas, incluida la digitalización y la automatización, la seguridad, los silos de información, la integración con aplicaciones heredadas, la mala calidad de la información, la menor aceptación de la tecnología por parte de los usuarios y el reemplazo de aplicaciones heredadas (Abdel, 2022, p. 29).

De acuerdo con el autor, hay retos significativos que afrontas las entidades en su gestión de información, debido a que, muchas de ellas tienen que estar adaptadas a los objetivos de la empresa, con el fin de cumplir con cada uno de ellos. Así mismo, tiene que salvaguardar su información, puesto que, no están del todo protegido por los usuarios, dado que, es un gran desafío por las fugas de datos que suele haber. Además, estos tienen que estar adecuados a las nuevas tecnologías cambiaste alrededor del mundo, para mejorar su administración de archivos.

Procesos de la Gestión de Información

Según Ibarrera (2022), los Procesos de la gestión de la información son:

- ***Captura e integración de datos:*** Esto permite garantizar la captura datos, para que sea utilizados en momento oportuno.

- ***Almacenamiento de datos:*** Permite asegurar que los datos sean almacenados en una nube u otros para resguardar su información.
- ***Seguridad de los datos:*** Certificar que los datos estén seguros ante cualquier amenaza que quiera afectar la información.
- ***Gestión de la calidad de los datos:*** Garantiza ante todo que la información sea de calidad y sin ningún error, para que pueda ser interpretada de manera correcta.
- ***Disponibilidad de los datos:*** Esto ayuda a que la información sea disponible cuando se la necesite, para tomar decisiones informadas con la documentación que ha sido facilitada.

Qué es una Estrategia

Según Laoyan (2024) "una estrategia es un plan de acción que se implementará en el futuro para lograr un objetivo final. Las estrategias te permiten definir los objetivos a largo plazo y cómo trabajarás para alcanzarlos". (pág. 5)

Una estrategia es un plan para dirigir un objetivo o meta que se haya planteado, para lograr los propósitos propuestos, esto es importante, puesto que, se pueden tomar procedimientos necesarios para una buena toma de decisiones en una empresa, y así tomar procedimientos necesarios para el buen regir organizacional. Además, es un conjunto de directrices que guían de forma efectiva las decisiones que se toman dentro de una entidad.

Qué son Protocolos

Se afirma que "un protocolo puede ser un documento o una normativa que establece cómo se debe actuar en ciertos procedimientos. De este modo, recopila conductas, acciones y técnicas que se consideran adecuadas ante ciertas situaciones" (Pérez & Merino, 2021, pág. 3).

Los protocolos son normas que se encuentran establecidas en un documento que una entidad tiene que seguir, para cumplir con un objetivo en común. Así mismo, ese documento describe el comportamiento y las técnicas que un individuo debe de alcanzar para que sean apropiadas en una institución. Además, la recopilación y formalización de técnicas apropiadas a través de protocolos no sólo mejora la efectividad y la calidad de los procesos que maneja una entidad, sino que también fomenta el cumplimiento de las reglas establecidas.

Tipos de Protocolos

Según Coll (2020), los tipos de protocolos son:

- ***Protocolo social:*** Son normas que se establen para el comportamiento social de los individuos.
- ***Protocolo oficial:*** Este protocolo suele aplicarse en actos presidenciales para seguir un orden de esto.
- ***Protocolo de empresa:*** Son normas o reglas que se establen para un buen trabajo colaborativo en una empresa.
- ***Protocolo diplomático:*** Son reglas que se aplican en actos diplomáticos

Norma ISO

Se dice que “las normas ISO son una serie de reglas que son reconocidas a nivel internacional y fueron creados con el fin de que las compañías establezcan unos parámetros en la creación de productos y servicios en la industria” (Brutti, 2023, pág. 4).

La norma ISO, es un certificado que se les brindan a las entidades, para afirmar que los productos y servicios que estas ofrecen estén seguros y que sean de calidad para el consumo humano, con esto se puede ratificar que no cuentan con ningún peligro en sus mercancías. Por

tanto, si una empresa no cuenta con un diploma ISO, quiere decir que no tiene un estado de seguridad en las mercaderías que brinda. Además, estas normas influyen a que las entidades las establezcan, debido a que, la estandarización de sus mercancías es esencial para facilitar el comercio internacional de sus intereses y garantizar que estos sean factibles para la venta.

Norma ISO 27001

Rodríguez et al. (2020), en palabras de Bernardo y Fiorella (2024) explican en su tesis de grado que la norma ISO 27001:

> Proporciona un marco detallado que orienta en la salvaguardia de privacidad en la administración de la información. En lo que respecta a la integridad, su enfoque principal radica en proteger la información para prevenir cualquier tipo de cambios no autorizados por la entidad responsable (pág. 20).

La norma ISO 27001, es un método internacional con el fin de brindar seguridad de información en los procesos que maneja una organización, ya sea de manera física o digital, esta norma se encarga de salvaguardar los datos de la empresa para que no sean manipulados ni alterados por nadie. De igual forma, esto permite que los datos sean protegidos, para que la empresa siga su persistencia y se fortalezca su productividad, además, esto requiere el compromiso y dedicación de la organización, para garantizar soluciones efectivas en la privacidad de los documentos de la compañía.

Marco Metodológico

La metodología que se utilizó en esta investigación fueron las siguientes:

Tipo y Alcance de la Investigación

El estudio es de tipo descriptivo-explicativo, debido a que, se desarrolló previo a un diagnóstico que permitió comprender la situación real de la empresa dando paso al estudio de caso desde un enfoque cualitativo. Esta investigación buscó resolver conflictos relacionados al objeto de estudio, la cual permitió una compresión profunda de los inconvenientes que se encontró en el departamento de talento humano de la empresa Fresh Fish del Ecuador, dando posibles alternativas para su solución.

Por otro lado, en cuanto al alcance descriptivo, se observó con detalle las condiciones del departamento de Talento Humano, que proporcionó un panorama claro del contexto organizacional. Además, se ofreció una descripción precisa de los eventos y dinámicas internas que afectan la seguridad de los datos que genera un marco detallado para proponer soluciones prácticas y aplicables.

Así mismo, el estudio tuvo un alcance explicativo, puesto que, durante el desarrollo de la investigación se manifestó los motivos por el cual se ejecuta el caso que dio a conocer sobre los hechos presentes que vive Fresh Fish y sobre las consecuencias que esta perpetra, debido a que, no cuentan con una buena seguridad de datos en la gestión de información, la cual afecta la integridad de la empresa.

Contactos Claves

Los participantes claves que ayudaron a que esta investigación se hiciera posible son:

Jefe de talento humano: El jefe de talento humano fue uno de los informantes claves, debido a que, es la responsable y encarga de llevar actividades del departamento para el cumplimiento de los objetivos propuestos en la empresa, es por ello, que al considerarla como informador secreto se pudo obtener información relevante sobre el estudio.

Trabajador social: Se consideró un individuo clave, debido a, su experiencia con el bienestar general de los usuarios, este personal llevaba un registro de los disgustos que existe en la empresa y de la información de cada sujeto, además, identificaba las necesidades de cada persona en la entidad.

Asistente de talento humano: La asistente de Talento Humano se consideró como informante clave, puesto que, tenía el acceso a toda la información que se desarrolla en la empresa, incluido los datos confidenciales e importantes, así mismo, tenía el contacto directo con el personal, la cual trata de temas relevantes manejados en la misma.

Métodos

Método Análisis-Síntesis: Se empleó el método de análisis para descomponer las teorías y elementos de un estudio, mientras que, la síntesis consintió en incorporar todas las partes examinadas de la investigación, para una mayor explicación del trabajo.

Método Bibliográfico: Se utilizó este método con la intención de recabar información necesaria sobre el objeto de estudio, en la cual se pudo obtener documentación concreta de cada una de las variables.

Método Inductivo-Deductivo: Se aplicó el método inductivo, dado que, parte de las observaciones específicas que se realizan en la investigación, por otro lado, el método deductivo permitió generar premisas generales que conducen a conclusiones específicas del estudio.

Técnicas e Instrumentos de Investigación

Investigación documental: La investigación documental permitió recopilar y escoger información de diferentes fuentes como: libros, revistas, videos, artículos, bibliografías, entre otros. Esto sirvió de apoyo para la recaudación de información de hechos pasados y presentes del estudio, para la interpretación y análisis de los documentos.

Observación directa: Esta técnica permitió estar al tanto sobre las deficiencias que existen en la empresa en cuanto a la seguridad de datos en la gestión de información, la cual dio a conocer los procesos que maneja el departamento de talento humano, para identificar las inconsistencias que tiene en el manejo de los documentos.

La entrevista semiestructurada: Este instrumento se utilizó de soporte, para la recolección de información importante y relevante para la investigación, debido a que, esta técnica está orientada al personal departamento de talento humano de la empresa Fresh Fish del Ecuador, dado que se desarrolló a través de una conversación casi planificada con el fin de tener un aporte esencial en el estudio.

Universo, Población y Muestra

El universo para el desarrollo de esta investigación es la empresa Fresh Fish del Ecuador; y, por otro lado, la población está constituida por los empleados de la entidad, además, la muestra seleccionada es el personal de talento humano, la cual se escogió a tres miembros del departamento conformados por: la jefa, el trabajador social y la asistente.

Tiempo de Realización de la Investigación

Este estudio fue ejecutado durante los dos últimos semestres de la carrera Gestión de la Información Gerencial, donde se abordó dos fases para la realización de este trabajo, se inició con la etapa de diseño, la cual ocurrió en el séptimo semestre, así mismo, se terminó en la fase de

resultados del octavo semestre de la carrera, donde se alcanzó los efectos esperados del estudio de caso. Esta investigación tuvo una duración aproximada a nueve meses, un periodo relevante para el desarrollo y planificación del estudio.

Resultados Obtenidos

Las técnicas ejecutadas en este estudio de caso incluyeron una observación directa al campo de investigación y una entrevista semiestructura al personal de Talento Humano de la empresa Fresh Fish del Ecuador, esto permitió la obtención de información importante para el análisis de datos. En base a los resultados obtenidos del Anexo 1 se constante lo siguiente:

Una política o reglamento de seguridad de datos son medidas que se encuentran establecidas para el manejo de información integra, si no se cumple con la ley establecida la empresa puede recibir sanciones referentes a su mal uso. Durante la entrevista desarrollada, los colaboradores mencionaron que al ingresar a la empresa firmaban un acuerdo de confidencialidad de información; sin embargo, no indicaron un reglamento que maneje la empresa para la protección de datos, lo que llevó a la deducción de que no cuentan con uno en específico o el personal no sabía si existe, esto se debe a una falta de comunicación.

Por otro lado, el manejo de la documentación en una entidad pública o privada tiene que ser utilizada de una forma eficiente y eficaz, dado que, tiene que estar organizada y almacenada de la forma correcta para su completo control. Así mismo, se debe de contar con una herramienta para la protección de información sensible y solo debe tener acceso al personal autorizado. En este contexto, se visualizó que el personal no hace un buen uso de la información, debido a, la pérdida de documentación relevante que se ha suscitado en el departamento.

Además, la información de los empleados en cualquier entidad siempre tiene que estar de manera ordenada y completa como actualizaciones periódicas, copias de seguridad y protección de los formatos físicos y digitales. Desde esta perspectiva, se pudo determinar que no se llevan un control de este proceso, porque la documentación se encontró de manera desordenada y sin protección alguna.

En este sentido, la eliminación de datos es el proceso de identificar documentación innecesaria de una empresa, para ayudar a controlar de manera adecuada la gestión de información en base a la privacidad. En este caso, se observó que la destrucción de informes se hace de manera adecuada, a través de un triturador de hojas, con el fin de que la información no se visualice ante cualquier usuario.

De la misma manera, la integridad de la información es un elemento clave, para certificar la confianza, honestidad y responsabilidad en cualquier entidad. No obstante, el departamento de talento humano no protegía adecuadamente la información personal y laboral de los individuos, dado que, la documentación no estaba almacenada ni procesada de manera adecuada por la falta de mecanismo de seguridad en la empresa.

Además, la información oportuna es un proceso fundamental para la toma de decisiones en el momento adecuado, si esta es entregada de forma tardía las decisiones tomadas pueden afectar los resultados. En este contexto, se observó que el personal del departamento cumple con sus responsabilidades en el momento establecido; es decir, que la información es precisa y actualizada de manera efectiva.

En efecto, la privacidad de los datos confidenciales de los empleados en una empresa es crucial para la protección de información relevante y sensible de ellos, para mantener un entorno laboral seguro y saludable para los individuos; además, de realizar copias de seguridad para su protección total. Desde esta perspectiva, se determinó que el personal de talento humano no cumple con lo requerido, debido a que, existía pérdida de información del trabajador que generaba conflicto en la búsqueda de este.

Es por ello, que las medidas de seguridad de datos son fundamentales para definir los objetivos de una empresa, de tal forma, permite desarrollar copias de seguridad y cambio de

contraseñas. En este sentido, se reflejó que el departamento carecía de estrategias definidas para el manejo de información, lo que llevó a la determinación de que los datos no estaban seguros en la entidad por la falta de esta.

Así mismo, un análisis de riesgos es un proceso primordial en cualquier entidad, debido a que, permite evaluar y proteger la información, además, de anticipar posibles amenazas que podrían afectar a la misma. En este caso, se visualizó que la empresa no realizaba un análisis de riesgos, debido a que, no contaban con un sistema tecnológico de seguridad capaz de detectar las posibles amenazas que pudieran afectar los activos de la entidad.

Los controles de acceso a la información en los sistemas son importantes en cualquier empresa, para mantener una vigilancia y revisión de los procesos que se ejecutan en una entidad, así mismo, esto sirve para detectar cualquier anomalía. Conforme a esto, se visualizó que no hay un control específico en los sistemas informáticos de la empresa, debido a que, se observó que existe un dispositivo tecnológico que pasa en manos de pasantes de cada área, esto podría generar la manipulación de documentos confidenciales de la misma.

Finalmente, tener un personal capacitado para enfrentar cualquier anomalía en la gestión de información es crucial, debido a que, debe poseer los conocimientos y habilidades necesarias para proteger la documentación de manera efectiva y acorde a las políticas de la empresa. En este contexto, se observó que el personal no estaba lo suficientemente capacitado para llevar los procesos de la empresa, debido a la falta de conocimiento en este tema.

Tabla 1

Triangulación de la Información de la Entrevista

Pregunta	Participante 1	Participante 2	Participante 3	Cita textual	Análisis del autor
¿Conocía anteriormente sobre el tema seguridad de datos?	La seguridad de datos como tal a lo que es tipo empresarial, claro que sí, en este caso es más que todo la confidencialidad que se le da a cada una de las partes y miembros de esta empresa.	Bueno, por lo general sí se ha tratado este tema y habitualmente se pone en práctica en todas las empresas, más que toda la salida de información del empleado donde en talento humano reposa toda la información confidencial del mismo.	Si, ha habido seminarios, capacitaciones, pero también ahora por todos los medios también se informa de este tema, entonces sí he escuchado algo relacionado a la seguridad de datos.	La seguridad de la información es fundamental en el funcionamiento de cualquier organización en la era digital actual. Consiste en la implementación de medidas y procedimientos diseñados para proteger la confidencialidad, integridad y también la disponibilidad de los datos (Marreros,	El personal de talento humano conocía del término seguridad de datos, tema que lo habían escuchado por otros medios o porque se ha tratado la temática, sin embargo, no tenían un conocimiento profundo de lo que trata seguridad de datos, por el hecho de que, no poseían una idea clara de lo que es este asunto. De acuerdo con la

				Acosta, & Mendoza, 2024).	teoría, este tema es importante para preservar la seguridad de la documentación de la compañía, debido a, su relevancia en la industria empresarial, para mantener los datos en total privacidad.
¿Qué comprende sobre protección de datos en la gestión de información?	Por ejemplo, entra un nuevo trabajador de nuestra empresa y en este caso es una persona que va a trabajar por un largo tiempo, el personal está obligado a firmar un contrato y acuerdos de	Nosotros recopilamos toda la información del empleado, tratándose desde que ingresa hasta que termina la contratación, hay que almacenar toda la información de este, por ejemplo: si	Entiendo que es como proteger la información, por ejemplo, la empresa tiene que asegurar que la información no sea hackeada o que no sea abordada por gente que de pronto tienen intereses de	La protección de datos se ha erigido como un pilar fundamental debido al crecimiento exponencial de la información y el incremento de conexiones. Es imperativo manejar de forma efectiva la	Los interrogados comunicaron que la seguridad de datos en la gestión de información es reposar la información confidencial de cada individuo, no obstante, la respuesta es un

	confidencialidad estos documentos son guardados en talento humano.	un empleado tiene un accidente o algo, aquí tenemos toda la información de la esposa, de los hijos, todo para tratarnos de comunicar por alguna emergencia o cualquier cosa que nos soliciten en cuestión de auditoría del ministerio. Además, a veces somos inspeccionados por ellos, para ver que todo esté en orden.	hacerle daño a la empresa. Entonces la seguridad de datos es como proteger y mantener en confidencia los datos personales y de la empresa.	información para preservar su solidez, privacidad y accesibilidad en variados ámbitos como el gubernamental, sanitario, educativo y empresarial (Ávila, 2024).	poco imprecisa dado que va más allá; es decir, que no siempre se trata de firmar acuerdos como lo decían los entrevistados. Por otro lado, la cita proporcionada indica que la seguridad de la información es fundamental dado al creciente aumento de información en las entidades, es por ello, que es importante proteger la documentación y manejarla con rigurosidad.

¿Cómo asegura la integridad y privacía de la información el departamento de Talento Humano?	Muy buena porque dentro del departamento de talento humano se manejan muchos prototipos, para el bienestar del personal, así mismo, se manipulan varios documentos desde el bienestar social, la responsabilidad social, nómina, etc. Esto se maneja con el fin de tener una base de datos con la información proporcionada.	Por lo general aquí se manejan datos del empleado que solamente tiene acceso ciertas personas, en este caso tres, la asistente de talento humano, el trabajador social y la jefatura de talento humano, nadie más puede tener acceso a la información del empleado, excepto que la gerencia la solicite, pero por eso es la confiabilidad que el empleado tiene con la empresa, es	Primero como equipo sabemos que firmamos un acuerdo confidencial, que garantiza que los empleados no pueden andar regando o hablando de la información que es confidencial de la empresa.	De acuerdo con Ortiz, Villacorta y Mendoza (2024), la nube está expuesta a diversas amenazas digitales, como ataques de hackers, malware, phishing y robo de datos, que pueden comprometer la confidencialidad e integridad de la información almacenada. Privacidad de los datos: La transferencia y almacenamiento de datos en la nube generan inquietudes acerca de la	De acuerdo con la información recolectada, el personal entrevistado asegura que la información de la empresa es completamente privada, no obstante, lo aseguran porque los empleados firman un contrato de confidencialidad de datos, y no porque tienen la certeza de que es así. Es por ello, que según la cita proporcionada los miembros de una empresa deben

		decir, los trabajadores están netamente seguro de la información que tenemos. Aparte, hacemos firmar un acuerdo de confiabilidad al empleado, donde obviamente están todas las cláusulas requeridas.		privacidad de la información. Los usuarios deben confiar en que los proveedores de servicios en la nube protejan de manera adecuada sus datos y prevengan el acceso no autorizado (pág. 7).	de asegurar su documentación a través de una nube donde almacenaría la información de manera sólida, íntegra y segura, para certificar que los datos sean precisos y concisos durante el período de vida de los documentos.
¿El departamento actualmente cuenta con un sistema para la protección de datos?	Claro si, actualmente tenemos sistemas, como Enterprise donde está toda la información del personal, donde podemos sacar datos de	Actualmente no, pero la información que tenemos solamente es en archivo hasta el momento.	El departamento de sistema sí trata de brindar al máximo toda esa parte, han intentado inclusive introducirse en la base de datos o en información confidencial, pero	Según Campo (2024), el Sistema de Gestión de Seguridad de la Información (SGSI) se posiciona como un enfoque esencial y completo para salvaguardar los	Los entrevistados informaron que en la actualidad la empresa cuenta con un sistema de seguridad de datos, sin embargo, existe cierta confusión porque el sistema

	nacimiento, datos de sueldos, la forma de pago, datos de puestos de trabajo, etc. Además, hay datos de manera física que tenemos archivados como el currículo, es decir, todos los datos personales de los trabajadores que solo se puede compartir con el usuario, más no con una persona particular.	se ha descubierto a tiempo.	activos de información críticos en el contexto empresarial actual, su carácter holístico se deriva de la consideración integral del ciclo de vida de la información, desde su concepción hasta su eliminación, abarcando todas las etapas intermedias (pág. 35).	Enterprise que mencionaron sirve para almacenar datos del empleado, no para resguardar los datos de cada individuo. Así mismo, no todos tienen la misma respuesta, dado que, uno de los entrevistados notifica que no existe un sistema para proteger la información relevante de la empresa, esto genera preocupación en la confidencialidad de información. Es por

					ello, que el autor en su cita destaca, que un sistema de seguridad de datos es fundamental, debido a que, sirve como soporte para asegurar la documentación de una entidad, para que no sea hackeada ni manipulada por un usuario.
¿Qué reglamento de protección de datos están implementados actualmente en la empresa, para proteger la documentación	Cuando un colaborador viene a trabajar acá, les hacemos firmar un documento de confidencialidad, que viene detallado con artículos. Si no	El empleado antes de entrar a la empresa se hace un sinnúmero de preguntas para el compromiso. Además, tienen que guardar toda la	Bueno, entre el departamento de talento humano y el departamento de sistemas se ha socializado este tema para proteger los datos. Por	Según la CONAFIPS (2021), la ley orgánica de protección de datos personales garantiza a los ciudadanos el derecho a la	El departamento de talento humano ha ejecutado varias medidas para proteger los datos relacionados a la producción y distribución de su

sensible relacionada a la fabricación y comercialización de su producto?	se cumple con las cláusulas requeridas pueden ser penalizados.	información de la empresa, es por ello, que se les hace firmar un contrato de confiabilidad antes de la contratación, donde están todas cláusulas requeridas de la empresa.	ejemplo, si un correo sospechoso llega, se le informa al departamento de sistemas para que ellos puedan ver de qué se trata y bloquearlo.	seguridad documental, además, multa a aquellos individuos que quebrantan las leyes establecidas. De esta manera, el gobierno ayuda a cumplir con las normas constituidas, para el buen uso de la información en las entidades.	producto, como: capacitaciones y acuerdos de confidencialidad, sin embargo, parece que los reglamentos se centran más en la concientización que en aplicar herramientas o normas que ayuden al control y salida de datos. Con respecto a la cita, un reglamento de seguridad permite cumplir con la privacidad total de los datos, dado que, si no lo hacen existe sanción por el incumplimiento

					de las normas establecidas. Es por ello, que en el artículo 1 y 2 de la Ley Orgánica de Protección de Datos Personales, india lo relevante que es el uso de este reglamento, dado a, la protección de datos y al resguardo de información de un individuo de manera eficaz.
¿Qué controles existen en el departamento de talento humano, para garantizar que solo el personal autorizado tenga	Antes de acceder a una información se debe tener la autorización de la jefa de talento humano. Además, cuando es así se	Bueno, como le indique está el asistente de talento humano, el trabajador social, que él más que todo debe de estar al	Cada persona tiene un usuario y ellos a través de distintos programas pueden ver qué persona tiene el acceso hasta tal punto de la	El control de acceso es un elemento fundamental de la seguridad de cualquier empresa que permite determinar quién	Los entrevistados indicaron que el departamento y la empresa en sí, tiene controles de acceso a información sensible como la

acceso a los datos delicados de la empresa?	pide también ingresar la aprobación por un correo, para dar el permiso correspondiente.	pendiente, dado que, él maneja el personal en cuanto a visitas y parte social. Además, aquí solamente se maneja un archivo y prácticamente está con llave, y solo tiene acceso tres personas.	información. Igual el departamento anda chequeando en donde está la persona, en el momento que está trabajando. Por ejemplo, tiene que venir un fin de semana a ver en el historial de las páginas para verificar hasta donde han llegado. Ellos están permanentemente inspeccionando y revisando. Aparte que cada área y cada departamento se percata de una	tiene acceso a qué información y bajo cuáles circunstancias. Dicho de otra forma, se trata de un tipo de tecnología que puede permitir o denegar el acceso a un usuario a ciertos datos, plataformas o espacios físicos de la empresa (Santos, 2024).	autorización previa. No obstante, se indicó que una parte de la información digital que tiene la empresa se encuentra bajo llave, la cual aumenta el riesgo de ser manipulada y alterada por un usuario, al estar en ese estado. Es por ello, que el autor en su cita indica, que mantener un control de acceso, permite certificar que no todo usuario tiene entrada a la información

			amenaza, de un correo.		establecida y sobre todo de forma física.
¿Realizan monitoreos continuos en la gestión de información para mantener su privacidad?	Sí, incluso cada vez que un colaborador nos deja es desvinculado de la empresa, sea por terminación de contratos, renuncia o indiligencia. Apenas el trabajador salga, ya no se puede permitir nuevamente el ingreso en la empresa. Además, se monitorea por el sistema, desde que el trabajador entra hasta que el	Monitoreos constantes no se hacen, simplemente se hacen para actualizar datos.	Sí, en el departamento de sistema hay dos personas, pero aparte ellos tratan de que cada persona sea como un inspector o vigile en lo que concierne a la protección de datos, si llega un link o algo que es sospechoso, como le dije anteriormente, ellos están permanentemente chequeando, es decir, existen	La monitorización de sistemas es el proceso de supervisar y controlar constantemente el rendimiento y el estado de un sistema informático o una red de sistemas para detectar posibles problemas, errores o anomalías (Sobrino, 2023).	Según lo dicho, si existen monitoreo en la gestión de información de la empresa, para asegurar los datos, pero estos no suelen ser constantes, dado que la supervisión más concurrente es sobre el empleado al finalizar su contrato laboral, no obstante, todas estas inspecciones lo realizan el departamento de sistema, dado que, ayuda a mantener el

	trabajador sale, se hace un tipo de marcación, dentro de ello se supervisa.		cámaras que están viendo el manejo del personal.		control de este, pero las inspecciones no son regulares, lo cual genera cierta inseguridad. Por otra parte, la cita revela que monitorear frecuentemente el estado actual de la gestión de información es importante, dado que, se pueden detectar falencias antes de que ocurra.
¿Qué tácticas certifican la seguridad de datos en el departamento?	Estrategia como tal no se manejan.	Bueno, la información está aquí en el sistema, la cual monitorea el departamento de	El departamento casi siempre esta hablando de esos temas. Además, a habido	Olivares (2024), en su cita resalta la necesidad de proponer cinco medidas de	En base a lo mencionado, el departamento de talento humano no maneja estrategias

	sistema. Además, nadie puede sacar información de aquí porque eso ellos lo controlan, así mismo, la documentación física se mantiene con llave para que solamente la persona indicada pueda tener acceso a la misma.	capacitaciones de ciberseguridad, de protección de datos, entre otros. Debido a que, cada día salen herramientas para proteger lo información.	seguridad de información, para la protección de datos de las entidades, como: hacer copias de seguridad o respaldos de las mismas, fomentar una cultura de contraseñas directas, proteger el correo electrónico, utilizar antivirus y controlar el acceso a la información (Olivares, 2024).	formales para mantener un control en la seguridad de datos, por otro parte, se ha mencionado que la empresa brinda capacitaciones sobre la ciberseguridad, esto garantizaría que el personal esté al tanto del tema, pero pesar de ello, no son estrategias seguras. Sin embargo, la teoría indica que las mejores estrategias para mantener segura la información es el

					cambio de contraseñas cada cierto tiempo, desarrollar copias de seguridad y manejar antivirus para proteger los documentos.
¿Fresh Fish cuenta con alguna norma ISO para salvaguardar la información?	La norma ISO, si la manejan aquí, pero no para salvaguardar la información.	Si, se cuenta con una norma ISO pero no para proteger la información, si no para la gestión de calidad de la producción, que es la ISO 9000.	No.	De cuerdo con Estalla y Morales (2024), la norma ISO/IEC 27001 en sus herramientas tecnológicas se presenta como una estrategia clave. Esta norma posibilitará el establecimiento y desarrollo de un Sistema de Gestión de la Seguridad de	Conforme a la información dada, Fresh Fish no cuenta con una Norma ISO para salvaguardar la información, sino con la norma ISO 9000, que técnicamente se basa en la calidad del producto. Conforme a la referencia, la norma

				la Información, proporcionando así un marco sólido para salvaguardar la integridad, confidencialidad y disponibilidad de la información manejada por la entidad (pág. 15).	ISO 27001 es una habilidad que proporcionaría una base segura para el manejo de documentación sutil.
¿Tiene algún conocimiento sobre la norma ISO 27001?	No	No.	He escuchado, pero no me he introducido a fondo.	Pendolema (2024), la norma ISO 27001, centrada en la seguridad de la información, ayuda a las empresas a cumplir con los requisitos legales establecidos en los contratos de seguridad de la información, los	Basada en la información recolectada, los entrevistados no tienen el conocimiento de esta norma, lo cual es relevante, dado que se puede capacitar al personal del tema para la aplicación

				cuales deben estar claramente definidos, documentados y actualizados en cada Sistema de Gestión de Seguridad de la Información (pág. 20).	de esta. Conforme a lo indicado, la norma ISO 27001, permitiría la seguridad de información en las entidades, basándose en normas y leyes que se deben de cumplir, para su ejecución.
¿La empresa Fresh Fish puede considerar la proyección de un presupuesto a largo tiempo, para implementación de la norma ISO 27001?	Claro que sí, en este caso si va a ayudar a resguardar la información confidencial de la empresa y el personal, sería bueno ejecutarlo.	Claro, en este caso la empresa si estuviera dispuesta a implementar la ISO mencionada, para la protección de datos.	Claro, como sugerencia puede entrar en el plan de capacitación de la empresa para implementarla.	Certificar los Sistemas de Gestión de Seguridad de la Información mediante la norma ISO 27001 permite proteger los datos de empresas y organizaciones	Al implementar la norma ISO 27001, puede ser una transformación significativa para la empresa, dado que, no tendrán dificultades a futuro sobre un mal respaldo de

				generando, al mismo tiempo, ahorro de recursos, valor agregado y confianza entre clientes, proveedores y trabajadores (Gonzalez, 2023).	información que afecten su integridad. En este sentido, es importante señalar que al tener un certificado ISO se les va a dar confianza a sus consignatarios, esto permitiría un ingreso más satisfactorio en la empresa.
¿Cómo determinaría usted el desempeño de los distintos ámbitos de protección de datos que ejecuta el	La política de seguridad está ejecutada totalmente en la empresa. (De acuerdo)	La política de seguridad está ejecutada totalmente en la empresa. (Totalmente de acuerdo)	La política de seguridad está ejecutada totalmente en la empresa. (De acuerdo)	Según Angulo, Zambrano, García y Bolaños (2018), existen varios dominios de la seguridad de información, las cuales son: Política	Basado en la información suministrada, se revela que el departamento de talento humano, estarían conformes con las políticas y

departamento de talento humano? Marque con una X el grado de concordancia de los siguientes dominios de seguridad de datos, utilizando la escala de Likert.	La estructura de la información del departamento de talento humano cumple con las perspectivas manifestadas de seguridad. (De acuerdo) La protección de datos en talento humano se gestiona eficaz y eficientemente. (De acuerdo) Los registros de acceso a la documentación son eficaces en el resguardo de datos.	La estructura de la información del departamento de talento humano cumple con las perspectivas manifestadas de seguridad. (Totalmente de acuerdo) La protección de datos en talento humano se gestiona eficaz y eficientemente. (Totalmente de acuerdo) Los registros de acceso a la documentación son eficaces en el	La estructura de la información del departamento de talento humano cumple con las perspectivas manifestadas de seguridad. (De acuerdo) La protección de datos en talento humano se gestiona eficaz y eficientemente. (De acuerdo) Los registros de acceso a la documentación son eficaces en el resguardo de datos.	de seguridad, Organización de la seguridad de la información, Gestión de activos, Seguridad en recursos humanos, Seguridad física y ambiental, Gestión de comunicaciones y operaciones, Control de acceso, Adquisición, desarrollo y mantenimiento de sistemas de información, Gestión de incidencias de la seguridad de la información, Gestión de la	habilidades ejecutas en la empresa, dado que, el 56% están de acuerdo y el 44% están totalmente de acuerdo de que se cumplen con los ámbitos de seguridad, esto genera un aspecto positivo en los ámbitos valorados. De acuerdo con la cita, los dominios de seguridad de datos son el manejo de políticas, plan, evaluación, estabilidad, ejecución, verificación y

	(Totalmente de acuerdo) La adquisición de los sistemas de información es fomentada acorde a las normas de protección de datos de la empresa. (De acuerdo) El desempeño de las estrategias de seguridad de los documentos es agradable. (De acuerdo)	resguardo de datos. (Totalmente de acuerdo) La adquisición de los sistemas de información es fomentada acorde a las normas de protección de datos de la empresa. (Totalmente de acuerdo) El desempeño de las estrategias de seguridad de los documentos es agradable. (Totalmente de acuerdo)	(De acuerdo) La adquisición de los sistemas de información es fomentada acorde a las normas de protección de datos de la empresa. (Totalmente de acuerdo) El desempeño de las estrategias de seguridad de los documentos es agradable. (De acuerdo)	continuidad del negocio y cumplimiento.	cuidado. Estos dominios, permitirán un apoyo firme en la privacidad de datos relacionada a la situación empresarial.

Análisis de Resultados

En relación con la entrevista que fue aplicada al personal del departamento de talento humano de la Empresa Fresh Fish del Ecuador, se reveló lo siguiente:

Conocimiento de Seguridad de Datos

En relación con la seguridad de datos, son mecanismos de protección de información relevante y sensible de la empresa, debido a que, se debe mantener confidencial la información ante cualquier amenaza que afecte la integridad de esta. "Esto implica salvaguardar los datos de acceso no autorizado, alteraciones no deseadas o pérdidas, ya sea por factores humanos o tecnológicos" (Rios, 2024, pág. 20). Desde esta perspectiva, se pudo determinar que el personal de talento humano no tiene un conocimiento amplio en este tema; por tanto, no lo ponen en práctica. Es por ello, que este limitado conocimiento puede afectar los procesos que maneja la entidad y poner en riesgo la documentación importante de la empresa.

Definición de la Seguridad de Datos en la Gestión de Información

Se trata de asegurar la información confidencial, íntegra, accesible y manejada correctamente en forma ética y de acuerdo con la ley, para reducir los riesgos y asegurar su cumplimiento; no obstante, el personal del departamento no tiene una comprensión clara de lo que trata este asunto, debido a que, malinterpretan este tema con otros asuntos que no tiene sentido, dando un mal uso de este tema en la empresa. Entonces, es importante destacar que al no comprender este argumento la entidad corre el riesgo de no tener control sobre la salida de información por la falta de desconocimiento en este término.

Es por ello, que el autor en su cita expresa lo siguiente sobre la seguridad de datos en la gestión de información:

> Es un proceso cuyo objetivo principal, es proteger y mantener la integridad de los activos críticos como la información, los aplicativos (software) y los servicios que soportan la razón de ser de una organización, los cuales dependen de las infraestructuras tecnológicas" (Hoces, 2024, pág. 39).

Por lo tanto, se puede deducir que la protección de información firme se da a través de soporte de técnico, que contenga herramientas de protección de datos, vigilancia total y capacitaciones regulares para el personal. Este conocimiento ayudaría al personal del departamento a garantizar la ausencia de filtraciones que puedan exponer los activos críticos de la organización y respaldar tanto las operaciones como el ajuste legal de la entidad.

Integridad y Privacidad de la Información

Este asunto se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta (Pérez G. P., 2023, pág. 21).

El departamento asegura su documentación a través de un contrato de confidencialidad y el acceso autoritario de solo tres personas. Sin embargo, este simple acuerdo confidencial, aunque es fundamental en cualquier entidad, no a garantiza que los datos sean resguardados de la forma apropiada. Por lo tanto, es recomendable integrar medidas más estrictas con el objetivo de certificar sus datos de forma apropiada.

Sistemas de Seguridad

Un sistema de gestión de seguridad de información está "basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y

mejorar la seguridad de la información" (Niño, 2019, pág. 23). Desde esta perspectiva, se puede determinar que no se dispone de un sistema de seguridad de datos, según lo expresado por los entrevistados, esto genera que la documentación este insegura en la entidad. Es por ello, que un sistema de seguridad de datos es esencial dentro de cualquier empresa u organización, para controlar y asegurar que los datos que se manejan sean totalmente protegidos por los ciberataques.

Políticas o Reglamentos de Seguridad de Datos

Durante la entrevista desarrollada en el departamento, se pudo notar que los colaboradores tienen un desconocimiento de las políticas de seguridad de datos que maneja la empresa, debido a que, no mencionaron una norma que maneje la entidad, lo que lleva a la deducción de que el personal no está al tanto de la existencia de leyes en la empresa, sobre el resguardo y protección de información.

Es por ello, que al conocer sobre "las políticas de seguridad permiten que los departamentos de tecnología de la información disminuyan las brechas y vulnerabilidades que pueden afectar la privacidad de la información dentro de los distintos niveles de una empresa" (García, 2024, pág. 5). En este contexto, establecer políticas de seguridad claras ayudaría a la organización a disminuir riesgos de afecten la integridad de los datos.

Control y Monitoreo de Acceso a la Información

Según Guevara (2024), el monitoreo y la evaluación constante en la gestión de información es importante en cualquier empresa, para mantener una vigilancia y revisión de los procesos que se ejecutan en una entidad, así mismo, esto sirve para detectar cualquier anomalía (págs. 18-19). Desde esta perspectiva, los entrevistados informaron que se realizaban monitoreos

cuando un empleado es desvinculado de la empresa, no obstante, no se realiza una vigilancia para a cerciorar la efectividad de la seguridad de información de la empresa. En este sentido, se pudo determinar que no hay un control específico en la documentación física y digital de la empresa.

Tácticas de Seguridad de Datos

Se determinó que el departamento no tiene estrategias definidas para el manejo de información, lo que lleva a la deducción de que los datos no están seguros en la entidad por la falta de esta. En este sentido, CEPAL (2024), indica que las estrategias de seguridad de datos son fundamental para definir los objetivos de una empresa, dado a que, permite desarrollar copias de seguridad y cambio de contraseñas constantes.

Implementación de la Norma ISO 27001

Normativas como la ISO/IEC 27001 establecen estándares para la gestión de la seguridad de la información, incluida la protección de datos confidenciales y el cumplimiento de requisitos legales y reglamentarios (Cedeño, 2024, pág. 69). Es por ello, que la entidad debería de considerar la implementación de esta norma, no solo para un reconocimiento si no para resguardar toda la documentación que lleva en sus procesos, puesto que, no tienen un sistema de gestión de información en donde proteger la documentación confidencial.

Dominios de Seguridad de Datos

Según Vásquez (2023), indica que existen varios dominios de seguridad de datos que toda empresa u organización debe de cumplir, para certificar su documentación como un sistema de seguridad, normas, controles, mantenimiento y sobre todo la comunicación. Esto va a

permitir que los archivos de una entidad se encuentren bajo protección y sean resguardados de forma apropiada.

En este contexto, se ejecutó varias preguntas con valoración de escala de Likert, donde los participantes informaron tener un buen uso sobre los dominios de seguridad de información, no obstante, durante la entrevista que se desarrolló, varios de estos ámbitos no son aplicados en el departamento, lo que ocasiona que la empresa baje en su productividad y sobre todo en su seguridad de datos.

Conclusiones

- **O.E. 1. Definir la seguridad de datos y la gestión de información.**

  Se concluye, que importante resguardar la documentación física y digital de la empresa, para el respaldo de información relevante. Además, que el nivel de conocimiento del personal del departamento de talento humano es un poco escaso, esto se debe a la falta de capacitación y al desinterés sobre estos temas de gran relevancia a nivel mundial. Es por ello, que esto afecta los procesos de seguridad, debido a, la falta de conocimiento del personal.

- **O.E. 2. Determinar el estado actual de la seguridad de datos en la gestión de información en el departamento de talento humano de la empresa fresh Fish del Ecuador.**

  Se puede concluir, que el estado actual del departamento de talento humano tiene repercusiones en su seguridad de datos, dado a que, existe una insuficiente enseñanza del tema y pérdida de documentación importante del personal, así mismo, de no contar con políticas precisas y un sistema que proteja la documentación privada de la empresa, esto genera inseguridad en los usuarios; además, no tienen un control adecuado al acceder a los sistemas informáticos, ni estrategias claras para el resguardo de la documentación.

- **O.E. 3. Identificar los efectos ocasionados en la seguridad de los datos y la gestión de información.**

  En definitiva, los efectos ocasionados que se sitúa en el departamento provocan que la toma de decisiones no sea precisa ni confiable. Así mismo, la ausencia de un sistema adecuado de seguridad datos, afecta negativamente a la gestión de la información de la

empresa, esto reduce la eficiencia y aumenta los riesgos de acceder a la documentación central de la entidad.

- **O.E. 4. Diseñar protocolos para la implementación de la norma ISO en la seguridad de datos como estrategia en la gestión de información.**

  Se concluye, que el personal del departamento tiene interés en aplicar la norma ISO 27001, debido a las bondades que ofrece para la protección de datos de manera eficaz. Esto ayuda a establecer un marco de gestión de seguridad claro y seguro, en base a las políticas y enfoque basado en riesgos; es por ello, que diseñar protocolos claros y seguros permitirá una implementación más rigurosa de la norma ISO.

Recomendaciones

De acuerdo con el estudio de caso ejecutado en la empresa Fresh Fish del Ecuador sobre la seguridad de datos en la gestión de información, se recomienda lo siguiente:

- Se recomienda que se tomen medidas proactivas en base a los conocimientos que el personal tiene de los temas mencionados, con ello, es importante capacitar al personal, para adquirir aprendizajes importantes sobre esta temática y así disminuir los riesgos que tienen en la seguridad de datos.
- Se sugiere aplicar reglas claras sobre la seguridad de datos, que describan el manejo de la gestión de archivos y protección de la información, estas pautas deberán incluir indagación acerca del buen uso de los expedientes del personal administrativo, la violación de la información y el acceso de documentos privados de la empresa, debido a que, esto garantizará la protección de los archivos personales de la entidad.
- Se recomienda realizar un seguimiento y monitoreo de las actividades diarias que ejecuta el personal del departamento de talento humano, para tener un control de ellos y certificar que se cumpla de forma correcta las directrices de seguridad, esto ayudará a disminuir riesgos para que no haya infracción de archivos corporativos.
- Es recomendable diseñar y ejecutar una serie de protocolos explícitos como guía, para una implementación eficaz de la norma ISO 27001, estas pautas deben ser claras y compresibles para el manejo del todo el personal, debido a que, esto asegurará una formación adecuada de los procesos que se desarrollan en el departamento y de la empresa en su totalidad.

Referencias

Abdel, M. H. (26 de Enero de 2022). *¿Qué es la Gestión de la Información?* Recuperado el 10 de Julio de 2024, de DG.

Angulo, M. N., Zambrano, V. M., García, M. G., & Bolaños, B. F. (28 de Septiembre de 2018). Propuesta metodológica de seguridad de información para proveedores de servicios de internet en Ecuador. *Revista Científica Multidisciplinaria, 4*(4), 8. Recuperado el 24 de Septiembre de 2024, de Código Onclick.

Asurza, C. J. (2022). *Diseño de una arquitectura de seguridad informática para incrementar la seguridad de información en la empresa Bafing S.A.C. en 2021. [Tesis para optar el título profesional de: Ingeniero de Sistemas Empresariales]*. Repositorio Académico, Lima-Perú.

Ávila, C. A. (30 de Abril de 2024). Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano. *Journal of Economic and Social Science Research, 4*(2). Recuperado el 8 de Septiembre de 2024

Barzaga, S. O., Vélez, P. H., Nevárez, B. J., & Arroyo, C. M. (2019). Gestión de la información y toma de decisiones en organizaciones educativas. *Revista de ciencias sociales, 25*(2), 2-11.

Bernardo, I., & Fiorella, D. (2024). *Norma ISO 27001 e ISO 31000 en gestión de riesgos de activos de información de empresa de telecomunicaciones, Lima 2023 [Tesis para obtener el grado académico de: Maestra en Ingeniería de Sistemas con mención en Tecnologías de la Información]*. Repositorio Digital Institucional, Lima.

Brutti, F. (9 de Julio de 2023). *¿Qué son y cómo funcionan las normas ISO?* Recuperado el 24 de Junio de 2024, de The Power.

Campo, C. L. (2024). *Propuesta para la implementación de la Norma ISO 27001 en el Archivo Central de la Gobernación del Departamento del Magdalena [Maestría en Gestión de la Información Documental]*. Universidad de La Salle, Bogotá. Recuperado el 24 de Septiembre de 2024, de Pensemos.

Cando, C. E. (2024). *Propuesta de mejora de seguridad de la Información digital a desarrollarse en el centro de mediación Online Dispute Resolution Quito - Rumipamba, Ecuador [Trabajo de investigación, para obtener la maestría en Gestión de Tecnologías de la Información].* Repositorio Institucional, Tacna-Perú. Recuperado el 9 de Julio de 2024, de https://repositorio.epnewman.edu.pe/handle/20.500.12892/929

Cedeño, C. S. (2024). S*istema informático para el control de historias clínicas del consultorio odontológico vitaldent de la ciudad de Portoviejo [Proyecto de titulación Previo a la Obtención del Título de Ingenerio en Tecnologías de la Información].* Repositorio Digital UNESUM, Jipijapa, Manabí, Ecuador. Recuperado el 5 de Octubre de 2024, de https://repositorio.unesum.edu.ec/handle/53000/6998

CEPAL. (2024). *Gestión de datos de investigación.* Recuperado el 5 de Octubre de 2024, de Biblioguías - Biblioteca de la CEPAL.

Coll, M. F. (1 de Agosto de 2020). *Protocolo - Que es, Definición y Concepto*. Recuperado el 25 de Junio de 2024, de Economipedia.

CONAFIPS. (11 de Mayo de 2021). L*ey Orgánica de Protección de Datos.* Recuperado el 20 de Octubre de 2024, de finanzaspopulares.

CONAFIPS. (21 de Mayo de 2021). Ley Orgánica de Protección de Datos. *LEXIS S.A*, 1-38. Recuperado el 11 de Septiembre de 2024

Estalla, C. L., & Morales, M. M. (2024). *Propuesta de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 para la agencia de compras de las fuerzas armadas, 2023 [Tesis para Optar el Titulo Profesional de Ingeniero de Sistemas]*. Repositorio Institucional Digital, Perú. Recuperado el 14 de Septiembre de 2024, de https://repositorio.unac.edu.pe/handle/20.500.12952/8903

Gamboa, S. J. (2020). *Importancia de la seguridad informática y ciberseguridad en el mundo actual*. Repositorio Institucional, Colombia. Recuperado el 12 de Julio de 2024, de https://repository.unipiloto.edu.co/handle/20.500.12277/8668

García, M. J. (2 de Octubre de 2024). *Política de seguridad de la información: qué es, importancia y cómo gestionarla*. Recuperado el 5 de Octubre de 2024, de deltaprotect.

Gomez, L. (Diciembre de 2022). *Definición de Seguridad*. Recuperado el 1 de Julio de 2024, de Significado.

Gonzalez, F. (15 de Febrero de 2023). *Implementación eficiente de la norma ISO 27001: claves y consejos*. Recuperado el 14 de Septiembre de 2024, de DataScope.

Guevara, S. N. (2024). *Sistema de monitoreo de infraestructura de TI para soporte a la gestión de recursos de la Oficina de Tecnologías de la Información de la Universidad Nacional de Cajamarca [Tesis para Optar el Título Profesional de Ingeniero de Sistemas]*. Repositorio Institucional, Cajamarca, Perú. Recuperado el 6 de Octubre de 2024

Hoces, R. S. (2024). *Sistema de Gestión de Seguridad de la Información Para Disminuir Riesgos de Perdida de Información en CENARES Año 2022 [Para Optar el Titulo Profesional de:*

Ingeniero de Sistemas e Informática]. Repositorio Dspace, Lima, Perú. Recuperado el 2 de Octubre de 2024, de https://repositorio.upci.edu.pe/handle/upci/1146

Ibarrera. (1 de Agosto de 2022). *8 principios de la gestión de datos*. Recuperado el 24 de Junio de 2024, de Data Ladder.

Inca, L. E. (2023). *"La gestión de la información en el departamento de nivelación en la Universidad Técnica de Cotopaxi 2023".[Tesis previo a la obtención del título de Licenciatura en Gestión de la Información Gerencial]*. Repositorio Institucional, Cotopaxi.

Jumbo, Y. R., & Salguero, R. L. (2024). *"Gestión de la información en la Extensión Pujilí de la Universidad Técnica de Cotopaxi 2023"[Tesis Previo a la Obtención del Titulo de Licenciatura en Gestión de la Información Gerencial]*. Repositorio Institucional, Cotopaxi.

Jurado, P. F., Yarad, J. P., & Carrión, J. J. (2020). Análisis de las características del sector microempresarial en latinoamérica y sus limitantes en la adopción de tecnologías para la seguridad de la información. *Revista Científica Ecociencia, 7*(1), 4.

Laoyan, S. (21 de Febrero de 2024). *¿Cuál es la diferencia entre táctica y estrategia?* Recuperado el 2 de Julio de 2024, de Asana.

Marín, L. L., Cobacango, V. J., Loor, I. G., & Vera, V. L. (8 de Abril de 2021). La Seguridad Informacional en el Ministerio de Transporte y Obras Públicas en. *Revista Científica, 7*(2), 1-21.

Marreros, J., Acosta, D., & Mendoza, A. (22 de Enero de 2024). Mecanismos de seguridad de la información en una organización: una revisión sistemática. *Revista Científica Ciencias*

Ingenieriles. Recuperado el 14 de Septiembre de 2024, de https://revistas.unh.edu.pe/index.php/ricci/article/view/384

Martínez, A. (8 de Marzo de 2024). *Defenición de Gestión*. Recuperado el 2024 de Junio de 26, de ConceptoDefinición.

Miranda, J. J. (2021). *Mapeo sistemático de metodologías de Seguridad de la Información para el control de la gestión de riesgos informáticos. [Trabajo de Grado Previo a la Obtención del Título de: Ingeniera de Sistemas]*. Repositorio Institucional de la Universidad Politécnica Salesiana, Guayaquil-Ecuador.

Niño, M. N. (2019). *Modelo de un sistema de gestión de seguridad de información – SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el Instituto Nacional de Estadística e Informática - INEI filial Lambayeque.* Repositorio Institucional UNPRG, Lambayeque, Perú. Recuperado el 5 de Octubre de 2024, de https://repositorio.unprg.edu.pe/handle/20.500.12893/5935

Ochoa, C. J. (2023). *Diseño de un sistema de gestión del riesgo en seguridad de la información para la sede principal de la Corporación Autónoma regional del rio grande de la Magdalena (CORMAGDALENA).[Tesis de posgrado Universidad Cooperativa de Colombia]*. Repositorio Institucional, Bucaramanga.

Olivares, V. (2024). *¿Cuáles son las medidas de seguridad para proteger la información de tu negocio?* Recuperado el 14 de Septiembre de 2024, de telcel empresas.

Ortiz, E., Villacorta, C., & Mendoza, A. (22 de Enero de 2024). Seguridad de la Información en la Nube: Una revisión sistemática. *RevistaCientíficaCienciasIngenieriles, 4*(1), 7.

Recuperado el 14 de Septiembre de 2024, de https://revistas.unh.edu.pe/index.php/ricci/article/view/383

Pendolema, E. A. (2024). *Análisis de procedimientos para prevenir la filtración de datos mediante la implementación de controles de la norma ISO 27001 en el centro operativo local ECU 911 Babahoyo [Previo a la Obtención del Título de: Ingeniero en Sistemas de Información].* Universidad Técnica de Babahoyo, Babahoyo. Recuperado el 14 de Septiembre de 2024, de http://dspace.utb.edu.ec/handle/49000/15665

Pérez Illidge, N., Geizzelez Luzardo, M., & Rosales Larreal, L. (2021). Gestión de información para la vigilancia tecnológica en empresas del sector energético de la Guajira colombiana. *IPSA Scientia, Revista Científica Multidisciplinaria, 6*(1), 1-12.

Pérez, G. P. (2023). *Modelo de arquitectura de cadena de bloques (blockchain) que permita mantener la integridad y privacidad de la información aplicando contratos inteligentes [Proyecto de Investigación, previo a la obtención del título de Ingeniero en Tecnologías].* Repositorio Universidad Técnica de Ambato, Ambato, Ecuador. Recuperado el 3 de Octubre de 2024, de https://repositorio.uta.edu.ec/handle/123456789/39462

Pérez, P. J., & Merino, M. (21 de Agosto de 2021). *Protocolo - Qué es, definición y concepto*. Recuperado el 25 de Junio de 2024, de Definicion.de: https://definicion.de/protocolo/

Rios, R. E. (2024). *Evaluación de la seguridad de la información con hacking ético en la municipalidad distrital de san juan bautista – 2023 [Para Obtar el Titúlo Profesional Ingeniero Informático y de Sistemas]*. Repositorio Institucional, Perú. Recuperado el 5 de Octubre de 2024

Rodriguez Baca, L. S., Cruzado Puente de la Vega, C. F., Mejía Corredor, C., & Alarcón Diaz, M. A. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. *Monographic: Educational management and teaching skills, 8*(3), 4.

Santos, C. J. (29 de Abril de 2024). *Controles de acceso: ¿qué son y por qué son importantes para proteger tu empresa?* Recuperado el 11 de Septiembre de 2024, de Deltaprotect.

Sobrino, C. (27 de Marzo de 2023). L*a Monitorización de Sistemas y sus Ventajas.* Recuperado el 14 de Septiembre de 2024, de CAPTIA.

Terán, T. Y. (2021). *Seguridad en la Gestión de la información para las organizaciones públicas desde el enfoque ISO/IEC 2700: un Mapeo Sistemático. [Trabajo de Grado Previo a la Obtención del Título de: Ingeniera de Sistemas].* Repositorio Institucional de la Universidad Politécnica Salesiana, Guayaquil-Ecuador.

Valls, C. A. (13 de Octubre de 2021). *¿Cuál es la diferencia entre información y comunicación?* Recuperado el 11 de Julio de 2024, de Brand Ok.

Vásquez, G. (7 de Febrero de 2023). *Conoce los 14 Dominios de la Seguridad de la Información*. Recuperado el 5 de Octubre de 2024, de Código OnClick.

Anexos

Anexo 1. Checklist

Checklist Aplicado a el Departamento de Talento Humano de la Empresa Fresh Fish Del Ecuador

N-	PREGUNTA	SI	NO	OBSERVACIÓN
1	¿Cuentan con las políticas de seguridad de información?		X	Se observó que no cuentan con una, porque no la aplican.
2	¿El departamento maneja eficientemente la documentación?		X	Existe perdida de información.
3	¿Todos los trabajadores tienen acceso a los datos en el departamento de talento humano?	X		
4	¿La información de los trabajadores se encuentran de manera ordenada y completa en sus carpetas?		X	La documentación se encontró de manera desordenada e incompleta.
5	¿El departamento elimina de manera adecuada los datos obsoletos e incensarios?	X		
6	¿Talento Humano promueve la transparencia y la integridad en la información interna de la empresa?		X	Se observó una falta de integridad de documentos, por la falta de mecanismos de seguridad.

7	¿La información es oportuna cuando se lo necesita?	X		
8	¿Se protege la privacidad de los empleados?		X	No porque, se evidenció perdida de información del trabajador.
9	¿Realizan continuamente copias de seguridad de los datos sensibles?		X	No, porque no contaban con un respaldo de los documentos en caso de que se extraviara uno.
10	¿Manejan de manera ética la información de la empresa?	X		
11	¿Cuentan con alguna medida de seguridad para proteger los datos sensibles o confidenciales?		X	Carecia de estrategias definidas
12	¿Se lleva a cabo un análisis de riesgos para identificar cualquier amenaza?		X	No cuentan con un análisis de riesgo, porque su seguridad de datos es ineficiente.
13	¿Existe algún control para acceso a los reportes de sistema de información?		X	No, porque cualquier usuario puede ingresar.
14	¿Cuenta con un personal altamente capacitado para abordar cualquier problema en la gestión de información?		X	El personal no está capacitado para gestionar los problemas que surjan en el departamento , debido a, su falta de conocimiento.

Preguntas validadas por Ing. María Fernanda Zambrano, Mg., Docente de la Carrera Gestión de la Información Gerencial de la Facultad de Ciencias Administrativas, Contables y Comercial de la Universidad Laica Eloy Alfaro de Manabí.

Anexo 2. Entrevista

ENTREVISTA SEMI ESTRUCTURADA

Objetivo: Esta entrevista tiene como finalidad analizar la seguridad de datos para ayudar a la gestión de la información en el departamento de talento humano de la empresa Fresh Fish del Ecuador en el año 2024.

1. ¿Conocía anteriormente sobre el tema seguridad de datos?
2. ¿Qué comprende sobre protección de datos en la gestión de información?
3. ¿Cómo asegura la integridad y privacía de la información el departamento de Talento Humano?
4. ¿El departamento actualmente cuenta con un sistema para la protección de datos?
5. ¿Qué reglamento de protección de datos están implementados actualmente en la empresa, para proteger la documentación sensible relacionada a la fabricación y comercialización de su producto?
6. ¿Qué controles existen en el departamento de talento humano, para garantizar que solo el personal autorizado tenga acceso a los datos delicados de la empresa?
7. ¿Realizan monitoreos continuos en la gestión de información para mantener su confiabilidad?
8. ¿Qué tácticas certifican la seguridad de datos en el departamento?

9. ¿Fresh Fish cuenta con alguna norma ISO para salvaguardar la información?
10. ¿Tiene algún conocimiento sobre la norma ISO 27001?
11. ¿La empresa Fresh Fish puede considerar la proyección de un presupuesto a largo tiempo, para implementación de la norma ISO 27001?
12. ¿Cómo determinaría usted el desempeño de los distintos ámbitos de protección de datos que ejecuta el departamento de talento humano?

    Marque con una X el nivel de concordancia de los siguientes dominios de seguridad de datos, utilizando la escala de Likert.

Preguntas	**Totalmente de acuerdo**	**De acuerdo**	**Neutral**	**En desacuerdo**	**Totalmente en desacuerdo**
La política de seguridad está ejecutada totalmente en la empresa.					
La estructura de la información del departamento de talento humano cumple con las perspectivas manifestadas de seguridad.					
La protección de datos en talento humano se gestiona eficaz y eficientemente.					
Los registros de acceso a la documentación son eficaces en el resguardo de datos.					

La adquisición de los sistemas de información es fomentada acorde a las normas de protección de datos de la empresa					
El desempeño de las estrategias de seguridad de los documentos es agradable.					

Preguntas validadas por Ing. María Fernanda Zambrano, Mg., Docente de la Carrera Gestión de la Información Gerencial de la Facultad de Ciencias Administrativas, Contables y Comercial de la Universidad Laica Eloy Alfaro de Manabí.

Fotografías

Anexo 3. Evidencias Fotográficas de aplicación de entrevista

Entrevista con la Lic. María Eugenia Saldarriaga, jefa del departamento de talento humano

Entrevista con la Lic. Rosita Álava Torres, asistente del departamento de talento humano

Entrevista con el Lic. Carlos Xavier Alvarado, trabajador Social del departamento de talento humano

Empresa Fresh Fish del Ecuador

Propuesta de Estudio de Caso:

Protocolos Claves para Adoptar la Norma ISO 27001 en Seguridad de Datos: Estrategia para una Gestión de Información Eficaz en la Empresa Fresh Fish.

Autor: Anchundia Briones María Fernanda

Año: 2024

Facultad: Ciencias Administrativas, Contables y Comercio

Carrera: Gestión de la Información Gerencial

Propuesta

Protocolos Claves para Adoptar la Norma ISO 27001 en Seguridad de Datos: Estrategia para una Gestión de Información Eficaz en la Empresa Fresh Fish.

La seguridad de datos es indispensable actualmente en cualquier entidad, puesto que, la cantidad de información que se maneja es abundante. Es por ello, que la aplicación de directrices fundamentales ayudará a tener un control eficaz en cuanto a la información que registra y emite la empresa, de este modo, no se correrá el riesgo de tener fugas de información que afecten a la empresa y a sus colaboradores.

Para alcanzar lo requerido, es necesario proponer protocolos claves para la aplicación de la norma ISO 27001 y así fortalecer la gestión de información de la empresa. Esto potenciará los flujos de información y mejorará su protección de datos, dando, así como resultado una eficiente seguridad de documentación física y digital en los sistemas de información que maneja la entidad.

Aplicación del Ciclo PHVA para la Elaboración del Protocolo

Para garantizar una aplicación segura y positiva de la norma ISO 27001 en la gestión de información de la empresa Fresh Fish del Ecuador, se plantea seguir el ciclo de PHVA (Planificar, Hacer, Verificar, Actuar). Esta estrategia ayudará a tener una descripción más eficaz de los protocolos de seguridad, con el fin de cumplir con los objetivos requeridos de la propuesta.

Objetivos

Objetivo General:

Recomendar protocolos claves para la implementación de la norma ISO 27001 en la seguridad de datos, para garantizar una gestión de información eficaz en la empresa Fresh Fish.

Objetivo Especifico:

- Estructurar protocolos claves de seguridad de datos, para la aplicación de la norma ISO 27001.
- Implementar protocolos de seguridad para asegurar los datos sensibles.
- Evaluar la eficacia de los protocolos de seguridad mediante monitoreo y control de los procesos, para verificar su protección.
- Desarrollar acciones de mejora para corregir los protocolos de seguridad en caso de ser necesario.

Beneficiarios

A continuación, se presenta los beneficiarios directos e indirectos que se verán favorecidos con la propuesta planificada.

Directos

El personal de la empresa Fresh Fish del Ecuador.

Indirectos

Clientes, proveedores y colaboradores de la empresa Fresh Fish del Ecuador

Protocolos - Ciclo PHVA

Planificar. – En esta etapa se define los objetivos y metas que se desean alcanzar, además, se debe enfocar en mejorar un proceso o problema su citado en una entidad.

- Evaluar el entorno actual de la empresa.

Esto se refiere a comprobar el estado presente de la empresa en necesidades de seguridad de datos, para analizar las condiciones y el nivel de seguridad que se encuentra.

- Definir los posibles riesgos que pueden suscitar en la empresa.

Esto se debe a los riesgos tales como: amenazas cibernéticas, perdida de información importante, mal uso de la información, mal manejo de los sistemas.

- Tener un control de los procesos gestionados en la entidad, para tener una revisión eficaz en la seguridad de datos.

Hay que controlar que los procesos sean ejecutados de la manera correcta para evitar una mala seguridad de datos en la empresa.

- Establecer roles y obligaciones al personal, para el manejo de la seguridad de datos en la gestión de información.

Esto se debe a que el personal comprenda que responsabilidad va a ocupar, para mejorar la gestión de la información de la empresa, en base a la protección de datos.

Hacer. – En este paso se debe de ejecutar lo planeado y proceder con el proceso de mejora.

- Capacitar al personal por medio de un experto en protección documental y sobre los procedimientos a seguir en la seguridad de datos.

Esto ayudará a dar el conocimiento necesario al personal sobre el buen manejo y resguardo de la información para evitar conflictos internos y externos.

- Integrar controles en los sistemas de información y en la documentación física que maneja la entidad, para mantener una eficaz protección de datos.

Se sugiere tener controles de acceso a los sistemas que maneja la compañía tales como Enterprise y Genesis, así mismo, toda la documentación importante que tiene.

- Fortalecer los dispositivos de la empresa, para evitar fugas de datos.

Hay que asegurar que los quipos y máquinas portátiles de la empresa tenga un sistema de bloqueo para afirmar su privacidad.

Verificar. – Se refiere a reconocer y examinar los resultados obtenidos, para la mejora continua.

- Verificar que las directrices establecidas se cumplan.

Hay que comprobar que los protocolos, se ejecuten de manera precisa y correcta por parte del personal de la empresa.

- Evaluar el grado de conocimiento del personal a través de pruebas.

Esto ayudará a valorar el esfuerzo y dedicación que el personal tiene al aprender sobre una buena gestión de información y seguridad de datos.

- Realizar intervenciones periódicas por parte de la alta dirección, para evaluar el desempeño del personal.

Esto se refiere a que los ejecutivos y directos de la empresa deberán realizar auditorías trimestrales en cada área, para verificar que todo esté en orden y en progreso, además, que el personal vea la importancia que tienen en la seguridad de datos.

Actuar. – Este apartado se refiere a que si todo salió bien se puede ejecutar lo planeado, para tomar decisiones informadas y mejorar constantemente los procesos.

- Desarrollar operaciones anticipadas para evitar riesgos en el futuro.

Esto permitirá que la compañía pueda prevenir los problemas a futuro sin correr riesgo alguno, previniéndolos a través de controles internos y externos.

- Inspeccionar y restablecer los protocolos en caso de ser necesario.

Esto conllevará a verificar que los protocolos establecidos sean de adecuados y actualizados, además, mejorarlas con anticipación para prevenir incidencias.

- Incorporar nuevos métodos en base a las necesidades de la entidad.

Se refiere a integrar metodologías como análisis DAFO o FODA, seguridad de en nube, cambio de contraseñas en los sistemas informáticos, precaución de fuga de datos, entre otros.

- Ejecutar la norma ISO 27001.

Una vez que cada protocolo haya sido ejecutado eficientemente en la empresa, se debe de implementar la norma ISO 27001, para la obtención del certificado.

Cronograma Valorado de Actividades Acorde a la Aplicación de la Norma ISO 27001

Objetivo	Ciclo PHVA	Actividad	Presupuesto Total	CRONOGRAMA (PERIODO 2024)			
				Primer Trimestre	Segundo Trimestre	Tercer Trimestre	Cuarto Trimestre
Implementar la norma ISO 27001 como estrategia para la gestión de Información en el departamento de talento humano de la empresa Fresh Fish del Ecuador, año 2024.	**Planificar**	Evaluar el entorno actual de la empresa.	**900**				
		Definir los posibles riesgos que pueden suscitar en la empresa.	**1,000**				
		Tener un control de los procesos gestionados en la entidad, para tener una revisión eficaz en la seguridad de datos.	**600**				
		Establecer roles y obligaciones al personal, para el manejo de la seguridad de datos en la gestión de información.	**400**				
	Hacer	Capacitar al personal por medio de un experto en protección documental y sobre los procedimientos a seguir en la seguridad de datos.	**2,000**				
		Integrar controles en los sistemas de información y en					

		la documentación física que maneja la entidad, para mantener una eficaz protección de datos.	**1,500**	
		Fortalecer los dispositivos de la empresa, para evitar fugas de datos.	**3,000**	
	Verificar	Verificar que las directrices establecidas se cumplan.	**1,000**	
		Evaluar el grado de conocimiento del personal a través de pruebas.	**1,000**	
		Realizar intervenciones periódicas por parte de la alta dirección, para evaluar el desempeño del personal.	**1,500**	
	Actuar	Desarrollar operaciones anticipadas para evitar riesgos en el futuro.	**1,000**	
		Inspeccionar y restablecer los protocolos en caso de ser necesario.	**900**	
		Incorporar nuevos métodos en base a las necesidades de le entidad.	**1,000**	
		Ejecutar la norma ISO 27001.	**10,000**	
	TOTAL		**25,800**	