UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

EXTENSIÓN "EL CARMEN"

CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

Creada Ley No. 10 – Registro Oficial 313 de noviembre 13 de 1985

PROYECTO INTEGRADOR PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN TECNOLOGÍAS DE LA INFORMACIÓN

TEMA:

AUDITORÍA INFORMÁTICA EN LA SEGURIDAD DE LA INFORMACIÓN SEGÚN LA ISO 27001 EN EMPRESAS COMERCIALES DE EL CARMEN

AUTOR

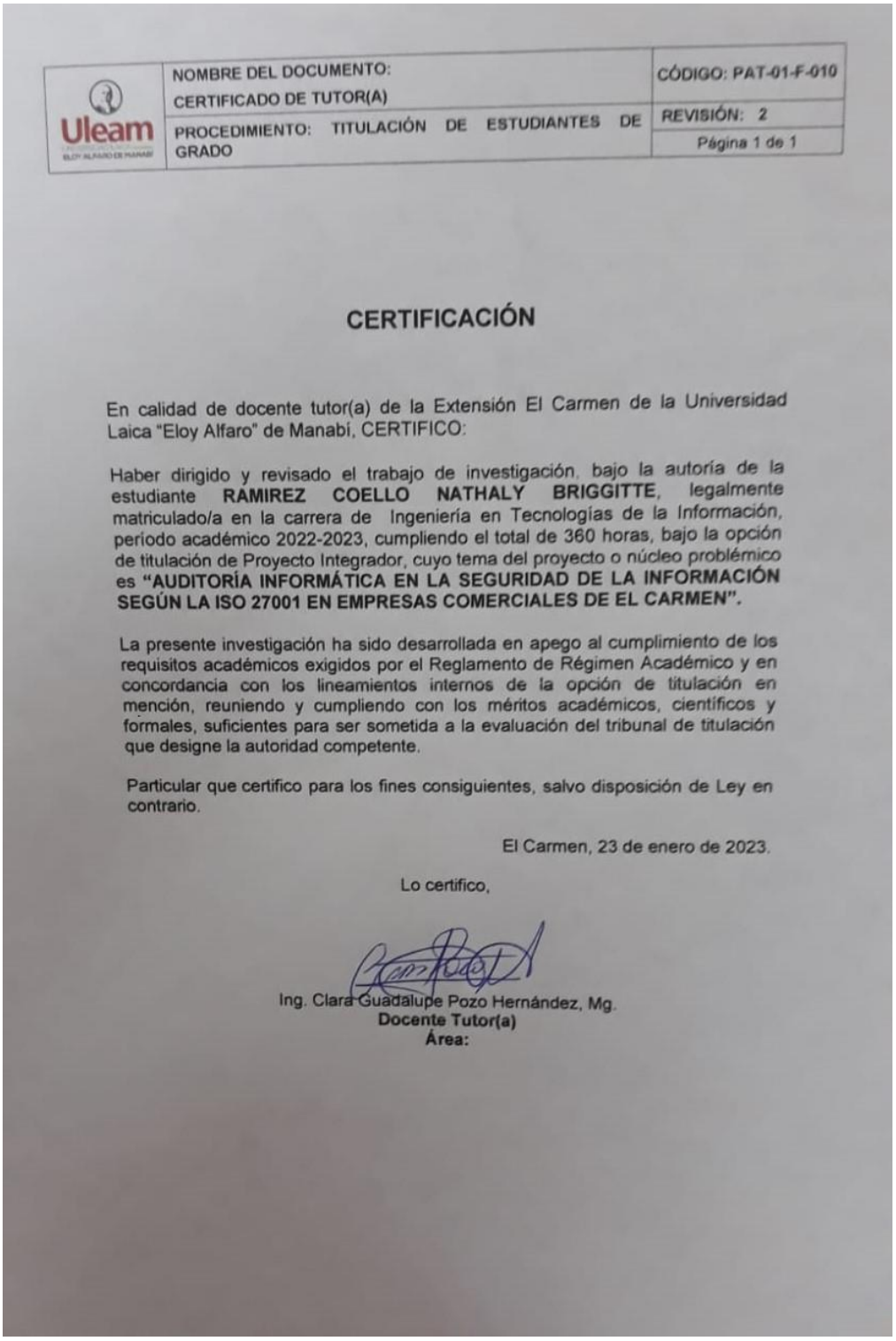
RAMIREZ COELLO NATHALY BRIGGITTE

TUTOR

ING. CLARA GUADALUPE POZO HERNANDEZ, Msc.

EL CARMEN, 2023

CERTIFICACIÓN DEL DIRECTOR DE TRABAJO DE GRADUACIÓN



Uleam	NOMBRE DEL DOCUMENTO: CERTIFICADO DE TUTOR(A)	CÓDIGO: PAT-01-F-010
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO	REVISIÓN: 2
		Página 1 de 1

CERTIFICACIÓN

En calidad de docente tutor(a) de la Extensión El Carmen de la Universidad Laica "Eloy Alfaro" de Manabí, CERTIFICO:

Haber dirigido y revisado el trabajo de investigación, bajo la autoría de la estudiante **RAMIREZ COELLO NATHALY BRIGGITTE**, legalmente matriculado/a en la carrera de Ingeniería en Tecnologías de la Información, período académico 2022-2023, cumpliendo el total de 360 horas, bajo la opción de titulación de Proyecto Integrador, cuyo tema del proyecto o núcleo problémico es **"AUDITORÍA INFORMÁTICA EN LA SEGURIDAD DE LA INFORMACIÓN SEGÚN LA ISO 27001 EN EMPRESAS COMERCIALES DE EL CARMEN".**

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, 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.

El Carmen, 23 de enero de 2023.

Lo certifico,

Ing. Clara Guadalupe Pozo Hernández, Mg.
Docente Tutor(a)
Área:

DECLARACIÓN DE AUTORÍA

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ EXTENSIÓN EL CARMEN

Declaración de Autoría

La responsabilidad del contenido de este Trabajo de titulación, con el siguiente tema: Auditoría informática en la seguridad de la información según la ISO 27001 en empresas comerciales de El Carmen, corresponde exclusivamente a: Ramirez Coello Nathaly Briggitte con cédula de ciudadanía N° 2350998049, y los derechos patrimoniales de la misma corresponden a la Universidad Laica "Eloy Alfaro" de Manabí.

_____

Ramirez Coello Nathaly Briggitte

C.C 2350998049

DEDICATORIA

La presente tesis está dedicada a Dios, ya que gracias al logrado concluir mi carrera, a mis padres porque ellos siempre estuvieron a mi lado brindándome apoyo y sus consejos para hacer de mí una mejor persona y a mis hermanas por sus palabras y su compañía, gracias por brindarme amor y el tiempo necesario para realizarme profesionalmente, a mis amigos, compañeros y todas las personas que de una u otra manera ha contribuido para el logro de mis objetivos.

Nathaly Briggitte Ramirez Coello

AGRADECIMIENTO

En estas líneas quiero agradecer a todas las personas que hicieron posible esta investigación y que de alguna manera estuvieron conmigo en los momentos difíciles, alegres, y tristes. Estas palabras son para ustedes. A mis padres por todo su amor, comprensión y apoyo, pero sobre todo gracias infinitas por la paciencia que me han tenido. No tengo palabras para agradecerles las incontables veces que me brindaron su apoyo en todas las decisiones que he tomado a lo largo de mi vida, unas buenas, otras malas, otras locas. Gracias por darme la libertad de desenvolverme como ser humano.

A mis hermanas por llenarme de alegría día tras día, por todos los consejos brindados, por compartir horas y horas de películas, series y muchos juegos, por las peleas, los gritos y herir mi cuerpo de puro amor.

Quiero agradecer a las empresas que me colaboraron con la información de la auditoría, la empresa Translatin S.A, la empresa Hermanos Loor y la empresa Alcívar.

Nathaly Briggitte Ramirez Coello

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

RESUMEN

El presente trabajo de titulación tuvo por objetivo realizar una auditoría informática a la gestión de seguridad de la información según la ISO 27001 a 3 empresas comerciales de El Carmen, se empezó por identificar la problemática realizando una entrevista y encuesta a los empleados de dichas empresas para justificar la presente investigación, llegando a determinar que no existía un conocimiento sobre Gestión de seguridad de la información y su importancia, por ello como propuesta se aplicó una auditoría de seguridad inicial para determinar la brecha GAP que consiste en encontrar el porcentaje de incumplimiento según el estándar de los requisitos y controles de seguridad, que contiene un conjunto de 7 ítems que deberían cumplir las organizaciones para considerar que la gestión de seguridad garantiza la integridad, confidencialidad y disponibilidad de su información. Como resultados relevantes se obtuvo que, la empresa Translatin tiene un nivel de madurez alto y las empresas Hermanos Loor y Alcívar tienen un nivel de madurez medio, finalmente se propone un manual para la gestión de seguridad de la información para las empresas ya mencionadas.

SUMMARY

The objective of this degree work was to conduct a computer audit of information security management according to ISO 27001 to 3 commercial companies in El Carmen, we began by identifying the problem by conducting an interview and survey of employees of these companies to justify this research, coming to determine that there was no knowledge about information security management and its importance, Therefore, as a proposal, an initial security audit was applied to determine the GAP, which consists of finding the percentage of non-compliance according to the standard of security requirements and controls, which contains a set of 7 items that organizations should comply with to consider that security management guarantees the integrity, confidentiality and availability of their information. As relevant results it was obtained that the company Translatin has a high maturity level and the companies Hermanos Loor and Alcívar have a medium maturity level, finally a manual for information security management is proposed for the aforementioned companies.

CAPÍTULO I

1.1 Introducción

La auditoría informática es un motor de la gestión de la seguridad de la información. El propósito de la auditoría informática es garantizar la seguridad e integridad de la información, los sistemas y los programas. Una auditoría informática es una verificación periódica y completa de la configuración de una computadora para garantizar que sea segura. La auditoría puede ser manual o automatizada. Existen muchos estándares para la auditoría informática como es la ISO 27001.

Una auditoría manual es realizada por un auditor que realiza él mismo una verificación exhaustiva de la configuración de seguridad en un sistema informático. Una auditoría automatizada es realizada por un sistema o programa informático que verifica la configuración de seguridad en un sistema informático en sí mismo sin intervención humana. El alcance de una auditoría puede limitarse a ciertas áreas o puede ser universal. Una auditoría de alcance limitado se centra en una sola área, como los controles de acceso de usuarios o los controles de aplicaciones. Una auditoría de alcance ilimitado verifica todos los controles en todas las áreas del sistema informático.

El término auditoría deriva de la palabra latina “audire” que significa “oír”. En informática, la auditoría se refiere a la realización de comprobaciones periódicas para asegurarse de que los sistemas electrónicos funcionan con corrección y están configurados correctamente con fines de seguridad. Una auditoría se considera una medida preventiva, ya que expone los problemas antes de que se vuelvan lo suficientemente graves como para causar una pérdida importante de datos o un tiempo de inactividad del sistema.

Las herramientas y técnicas de auditoría mejoran la eficiencia al realizar auditorías informáticas para garantizar que los sistemas cumplan con las normas requeridas para la protección de datos. También ayuda a las organizaciones a cumplir con estándares internacionales como ISO 27001 al diseñar su entorno informático. Las auditorías periódicas ayudan a las organizaciones a mantener su entorno informático para que cumpla con las reglamentaciones necesarias para la protección de datos y la gestión de la seguridad.

1.2 Presentación del tema

Auditoría informática en seguridad de la información según la ISO 27001 en empresas comerciales de El Carmen

1.3 Ubicación y contextualización de la problemática

En la actualidad, los sistemas de información son utilizados por diversas empresas alrededor del mundo, convirtiéndose en un fenómeno social con un proceso de comercialización imparable.

Siendo en la mayoría de las empresas los sistemas de información son activos destacados que son críticos para la supervivencia y, por lo tanto, son conscientes de como los sistemas de información críticos reflejan sus operaciones y tienen altas vulnerabilidades, siendo lo más importante las políticas y regulaciones de seguridad vigentes.

En Ecuador existen instituciones que procesan datos a través de sistemas de información que muchas veces no funcionan bien, no cuentan con la seguridad necesaria y no son utilizados adecuadamente, por lo que es necesario implementar varios mecanismos para mejorar su uso (Aucapiña, 2012).

En las empresas comerciales de El Carmen son cada vez más conscientes que la información que se maneja debe estar bien protegida, así también de ser capaces de identificar y gestionar los riesgos de seguridad de la información y esto se lleva a cabo a través de la definición de un Sistema de Gestión de Seguridad de la Información mediante la implementación de la norma de seguridad informática ISO 27001.

1.4 Planteamiento del problema

La auditoría informática ayuda a controlar la función informática y a analizar eficientemente los Sistemas Informáticos, verificando el cumplimiento de las normativas generales de la empresa en este ámbito y la revisando la eficaz gestión de los recursos.

En la actualidad puede ayudar a una organización a organizar todas las cuestiones. Como cualquier otro sistema de gestión, como la calidad o medio ambiente, tiene como objetivo conseguir mejores resultados de forma precisa y ordenada.

Unos de los problemas más comunes dentro de una empresa es la pérdida de información, ya que muchas veces no se cuenta con un sistema informático para llevar el control de la información que maneja la empresa. Por esa razón, habrá una mala organización en trabajo, entre ellas se tienen:

- Amenazas informáticas
- Vulnerabilidades del sistema.
- Amenazas de ataques de denegación de servicio.
- Vulnerabilidades producidas por contraseñas.
- Vulnerabilidades producidas por usuarios.

1.4.1 Problematización

Uno de los problemas más urgentes de las instituciones en la actualidad es la falta de seguridad informática debido al desarrollo de la tecnología y la globalización de las redes de comunicación que van de la mano con internet, como lo son: Acceso a información peligrosa, Acceso a información poco fiables, Ataques al sistema, entre otros.

La información que manejan las empresas comerciales de El Carmen es de trascendental importancia para el progreso productivo, económico, social y cultural del cantón, ya que la mayoría de las transacciones se realizan haciendo uso de los sistemas informáticos. Se entiende que es fundamental para el desarrollo del comercio local y se asegura de que la información se maneje con precisión y seguridad.

La inexistencia de planes de seguridad en las empresas vuelve vulnerable los sistemas y aumenta la exposición a riesgos de seguridad y permite a un atacante comprometer la integridad, disponibilidad o confidencialidad del sistema.

1.4.2 Génesis del problema

Se origina el desconocimiento del proceso sobre la situación actual en cuanto a seguridad de la información en empresas comerciales de El Carmen, haciendo que la mayoría de empresas comerciales del cantón no conocen del tema de seguridad de la información, siendo un retraso en los procesos que realiza la empresa y a la vez habría muchos errores y demoras de los procesos, teniendo que con la falta del desconocimiento se tendría pérdida de la información siendo un problema tanto para la empresa como para sus clientes.

1.4.3 Estado actual del problema

El principal problema de las empresas es el desconocimiento de los procesos actuales en cuanto a seguridad de la información, siendo para las organizaciones actualmente carecen de seguridad y limitar los controles técnicos, evidentemente necesarios para gestionar las incidencias para evitar amenazas al sistema de gestión de seguridad.

1.5 Diagrama causa – efecto del problema

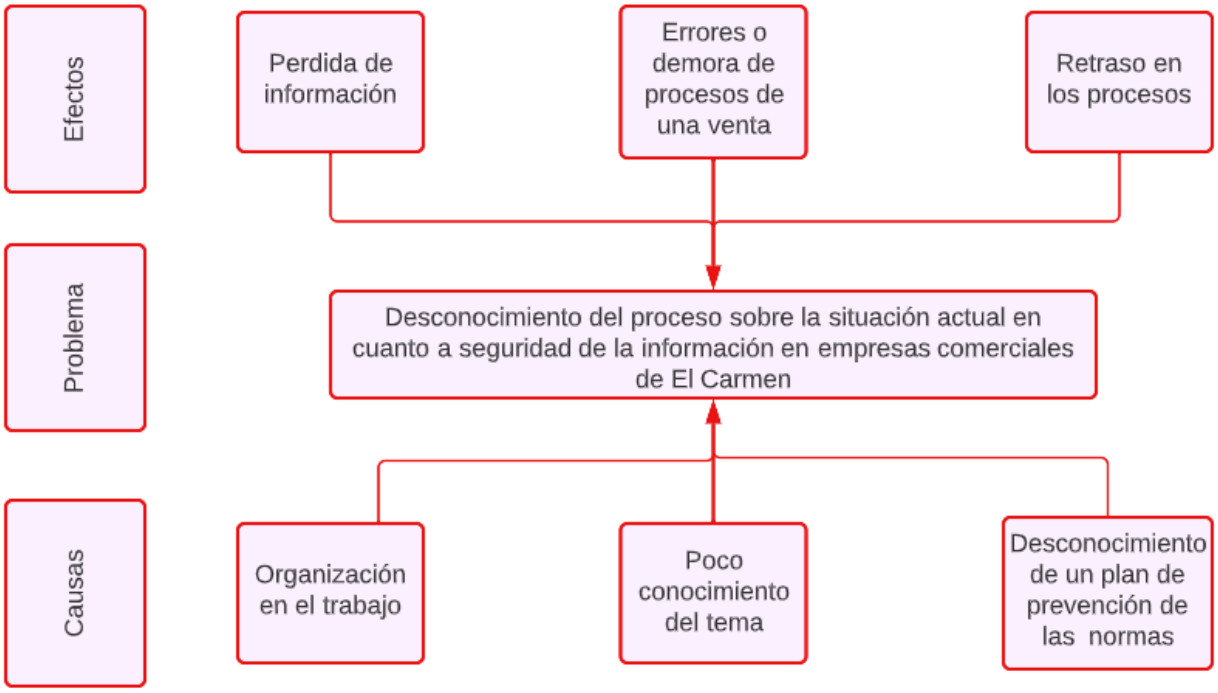


Ilustración 1 Diagrama causa - efecto del problema

1.6 Objetivos

1.6.1 Objetivo General

Realizar una auditoría informática en la seguridad de la información según la ISO 27001 en empresas comerciales de El Carmen.

1.6.2 Objetivos Específicos

1. Fundamentar bibliográficamente las variables del estudio, auditoría informática y seguridad de la información
2. Realizar un diagnóstico sobre la problemática en la seguridad de la información en 3 empresas comerciales.
3. Ejecutar una auditoria informática inicial para la gestión de seguridad según la ISO 27001.
4. Elaborar un manual para la gestión de seguridad de la información en empresas comerciales.
5. Redactar conclusiones que brinden información final a la investigación.

1.7 Justificación

Según Ferro Velga (2020), una auditoría informática, tanto externa como interna, debe ser una actividad libre de cualquier contenido o matiz "político" que quede fuera de la estrategia y las políticas generales de la empresa. La función de auditoría puede actuar de forma dura, ya sea por iniciativa propia de la organización o a petición de una parte, es decir, a instancias de la dirección o de un cliente.

Según Romero Castro, y otros (2018), la seguridad siempre busca administrar el riesgo, esto significa que siempre hay manera de evitarlo o prevenirlo y se pueden tomar ciertas acciones para evitar mejor estas situaciones. Se han definido que la seguridad puede clasificarse como libre de riesgo, cuya definición se refiere a cuatro acciones que siempre están inmersas en cualquier tema de seguridad, tales como:

- Prevención del riesgo
- Transferir el riesgo
- Mitigar el riesgo
- Aceptar el riesgo

En términos generales, uno de los principales beneficios de realizar auditorías internas de gestión de seguridad es permitir que el personal de alta dirección de la organización tome decisiones basadas en la situación de gestión de calidad revelada por dichas auditorías, para hacer algún reposicionamiento si es necesario lograr los objetivos establecidos según Escuela Europea de Excelencia (2016) los principales beneficios de auditoría de gestión de seguridad son:

- Permiten la comparación de los procedimientos de gestión de calidad documentados de la organización con la práctica observada.
- Identificar los errores existentes en los diversos procesos de gestión de la calidad de la organización.
- Mejora la comunicación interna.
- Detectar problemas que pueden llegar a ser graves.

1.8 Impactos esperados

1.8.1 Impacto tecnológico

Aspectos que conducen a la necesidad de cambiar la función de auditoría dinámica del mercado, en la automatización de procesos, el número cada vez menor de documentos impresos y tratar con una terminología cada vez más compleja (Mendz, 2016).

Garantizar el mejor rendimiento de las empresas, con los siguientes beneficios:

- Rentabilidad
- Detección de vulnerabilidades
- Anticipación a accidentes.

1.8.2 Impacto social

Según Davalos (2017) las actividades de la organización afectan a cierto sector de la sociedad, así como los eventos y actividades fuera de la organización lo afectan en alguna medida. Estos hechos o factores externos pueden ser:

- Económica
- Político
- Cultural
- Tecnología
- Social

Aporta el análisis de los riesgos y fallos de seguridad, control de los programas y sistemas instalados, seguridad de información, datos y programas.

1.8.3 Impacto ecológico

La auditoría informática aporta a que se consuma menos papel y que hay menos desechos informáticos porque brinda que se pueda prolongar más el tiempo de vida a los equipos informáticos porque esto ayuda al medio ambiente.

CAPÍTULO II

2 MARCO TEÓRICO

2.1 Antecedentes históricos

¿Qué es una auditoría? La palabra proviene del latín auditorius, de donde proviene auditor, persona con virtud de oír, que el diccionario define como auditor de Cuentas Colegiado; pero presumiblemente el propósito de la audiencia y el examen de estos informes es evaluar la economía, la eficiencia y la eficacia del uso de los recursos (Sánchez & Pellicer, 2013).

La auditoría informática es el proceso de recopilar, agrupar y evaluar pruebas para determinar si los sistemas informáticos pueden proteger los activos, mantener la integridad de los datos, alcanzar de forma eficaz los objetivos de la organización y utilizar los recursos de manera eficiente.

En 50 años, las empresas introdujeron máquinas, las llamadas auditorías informáticas. En la década de 1960, el enfoque cambio debido a los resultados de baja calidad obtenidos de las auditorías de distrito, a menudo denominadas auditorías informáticas.

A fines de la década de 1970, se alcanzó un tercer paso: la revisión computarizada, en este enfoque también se estudia el procesamiento lógico de la información en los programas y aplicaciones que los integran.

A principios de la década de 1980, los técnicos de procesamiento de información comenzaron a usar computadoras para el respaldar el trabajo de los contadores. Hoy en día, las empresas confían cada vez más en el uso de la tecnología para lograr sus objetivos y estrategias comerciales (Villegas, 2014).

La seguridad de la información no necesariamente surgió en la moderna y actual era de la informática, ya que se refiere a la información de manera general, la cual siempre ha estado asociada al término “humanidad, sociedad y civilización”, por el contrario, de seguridad informática (Linux NET, 2020).

En cuanto al sistema de control en sí, existen varios modelos como es el de la empresa Duport, utilizando el modelo del mismo nombre de la empresa, después en 1994, el ejecutivo de salud y seguridad elaboro un documento que resumía elementos clave de la gestión de la seguridad y la salud, cuando se hicieron populares las normas ISO 9001:1994 e ISO 14001:1996

inician la necesidad de modelos de gestión en la salud y la seguridad en el trabajo definidas por estas normas se integran fácilmente (Cueva, 2018).

2.2 Antecedentes de investigaciones relacionadas al tema presentado

Dado que el uso de las tecnologías de la información está orientado apoyar la sistematización del área empresarial, se inició la implementación de aplicaciones de gestión como contabilidad, nómina, entre otros., lo que derivó en la denominada auditoria de sistemas de información.

Después de eso, el uso de la tecnología de la información se extendió a todas las áreas de negocios en todos los niveles, los productos y servicios fueron muy diversos, se extendieron las microcomputadoras o equipos departamentales, luego de las computadoras personales, las redes de área local y la integración de las telecomunicaciones y las grandes empresas. Tecnología de la información manufacturada, los auditores de sistemas tradicionales y con principios no pueden continuar evaluando el número de componentes técnicos en el campo con métodos y procedimientos convencionales.

Después de eso, se debe revisar el contenido y la forma de la auditoría de TI, y el objetivo que tiene la auditoría de TI una dimensión más realista y adecuada (Hernandez, 1993).

2.2.1 Análisis de seguridad de procesamiento de datos y gestión de información de empresas comerciales de El Carmen

Zevallos Hidalgo (2020), expresa que “Por los diagnósticos anteriores se ha detectado que las empresas carecen de conocimiento de seguridad de procesamiento de datos y gestión de información, el objetivo general es, determinar la seguridad de procesamiento de datos para mejorar la gestión de la información mediante la aplicación a las empresas comerciales del cantón El Carmen”.

2.2.2 Software de análisis de riesgos informáticos aplicando Magerit y normas ISO/IEC 17799 e ISO/IEC 27001 caso de aplicación en la facultad de ciencias informáticas.

Acosta Alvarado & Carrillo Morán (2018), nos dice que lo “Consiste en la realización de un análisis de riesgos de seguridad de la información de los activos de una organización, para poder definir los controles necesarios que se necesitan para cumplir todos los requerimientos de protección de sus activos. En el desarrollo de este proyecto se ha definido una metodología de trabajo acorde a las necesidades, cultura y estructura específica de la institución”.

2.2.3 Auditoría de seguridad informática ISO 27001 para la empresa de alimentos "ITALIMENTOS CIA. LTDA"

Cadme Ruiz & Duque Pozo (2012), expresa que "El objetivo primordial de esta auditoría de SGSI es averiguar si hay algo que se está realizando mal, de manera objetiva. En ITALIMENTOS se realizó una encuesta, de la que se tomó una muestra de veinte empleados, logrando sacar conclusiones de que existe un 15% de movimientos de recursos informáticos entre distintos empleados, los cambios o movimientos realizados de los recursos informáticos se dan por nuevas características tecnológicas".

2.2.4 Norma de seguridad informática ISO 27001 para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación en el departamento de sistemas de la cooperativa de ahorro y crédito san francisco LTDA.

Aucapiña (2012), manifiesta que "El presente proyecto reúne la información necesaria para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001, se ha concebido esta norma para garantizar la selección de controles de seguridad adecuados y proporcionales. La investigación se realizó mediante la aplicación de entrevistas al personal que labora en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito ―San Francisco‖ Ltda. Los resultados se realizarán desde el punto de vista descriptivo y estadístico, proceso que permite realizar la interpretación adecuada basada en el marco teórico".

2.2.5 Auditoría informática dirigida al Centro de Cómputo de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil con base en las Normas ISO 27001 y 27002

Naranjo Camacho & Reyes Lucas (2020) afirma que

Se analizaron los peligros de los activos y se evaluaron los controles según lo indicado por las reglas ISO 27001 e ISO 27002, además de una revisión de los requisitos obligatorios por la regla ISO 27001. Como consecuencia, no existe el 42% de los controles considerados importantes para una óptima estabilidad de la información, el 24% de controles se sitúan en un estado inicial, el 5% poseen un mejor estado, sin embargo, se hacen de modo informal y solo el 2% de controles poseen documentación formal, ninguno es hecho por un archivo aprobado por la Dirección, el 2% de los controles no fueron revisados y el 25% son considerados como no aplicables para el

centro de cómputo. En la actualidad se cumple con el 4% de los requisitos obligatorios por la Regla ISO 27001. Si se permiten y aplican de manera correcta las políticas de estabilidad de la información; se cree que el estado de utilización podría ser del 37% de los requisitos en una fase inicial, 41% de requisitos formalizados y documentados, quedando todavía sin consumar el 22%.

2.3 AUDITORÍA INFORMÁTICA

2.3.1 Definición de la auditoría informática

Una auditoría es un componente del sistema de control interno de una organización, cuya función principal es asesorar a la dirección general en la identificación, desarrollo, implementación y mantenimiento de los sistemas de control: gerencial, financiero, informático y gerencial para asegurar los resultados operativos esperados con objetivos preestablecidos (Arcentales-Fenández & Caycedo-Casas, 2017).

La auditoría es una técnica de evaluación. Cada auditoría tiene un objeto de trabajo. Cada auditoría tiene una meta o propósito. La evaluación se caracteriza por el hecho de que se basa en referencias acordadas. La evaluación tiene como objetivo determinar la conformidad de lo evaluado frente a un criterio, mientras la auditoría se enfoca sobre la conformidad de lo evaluado con respecto a un criterio, la evaluación ex post se limita a opinar sobre el cumplimiento de las metas planeadas (Sánchez Ch, 2021).

Definen la auditoría de TI como la dirección evaluada en el sistema administrativo, es decir, la estructura de la organización, los procesos administrativos, las operaciones y el ambiente de control aplicado (Albarracín Zambrano et al., 2021).

2.3.1.1 Objetivo de la auditoría informática

Según Quillupangui Toapanda (2019) la auditoría informática implica un examen crítico y sistemático de políticas, normas, prácticas y procedimientos para determinar la economía, eficiencia y eficacia de los sistemas de control interno relacionados con Tecnologías de la información. Este estudio presenta enfoques para evaluar un sistema de gestión de tecnología de la información, cuyo objetivo es identificar las mejores prácticas de gestión

2.3.2 Importancia de la auditoría informática

La auditoría informática es fundamental y tiene como objetivo orientar y asesorar sin restricciones a todos sus empleados para que puedan desempeñar a cabalidad sus funciones; pero es imposible aferrarse a tantos controles y medidas que paralizan la propia sensación de

seguridad. Demasiado grande, por lo que se debe realizar un análisis coste/ beneficio para valorar las posibles consecuencias de la pérdida de información y otros recursos informáticos, así como para analizar los factores que inciden negativamente en la productividad de la empresa (Jiménez Ortiz & Namuche Ayala, 2019).

Arcentales Fernández y Caycedo Casas (2017) explican la importancia de las auditorías de TI, es que pueden identificar las fortalezas y debilidades en la gestión de proyectos, el nivel de funcionalidad de los sistemas de información automatizados, la idoneidad de la configuración de la plataforma de TI y el grado de calidad del servicio. Proporcionando por la autoridad responsable y su estado contractual con los proveedores de bienes y servicios, entre otros, está dentro del uso y aplicación de las TIC de la organización.

2.3.3 Normas técnicas de ejecución de la auditoría

Según Pallerola Comamala(2015) un equipo de todos los auditores y sus empleados siempre debe tener en cuenta cuál es el marco de las normas de auditoría cuando participa en la participación profesional en la auditoría externa de TI.

Las normas técnicas para la realización de los trabajos relacionados con la preparación y ejecución del trabajo del auditor de cuentas regulan las técnicas de investigación e inspección aplicables a las partidas y hechos relacionados con la auditoría de documentos contables a su cargo. Juicio independiente, especialmente:

- Trabajos que requieran un conocimiento previo y completo del sistema de control interno del auditado o entidad. La evaluación sirve de base para determinar el alcance de las garantías objetivas realizadas.
- Planificación y programación del trabajo.

2.3.4 Tipos de auditoría informática

2.3.4.1 Los principios de la seguridad

Romero Castro y otros (2018) explican que los datos son valor, los números, las medidas, el texto, los documentos en bruto, la información es el valor de estos datos, es lo que da el conocimiento. Manual de procedimientos, datos de empleados, proveedores y clientes de la empresa, base de datos de pagos son datos estructurados de tal manera que se convierten en información, aumentando el valor de una empresa.

Los pilares de la seguridad de la información se basan en la necesidad de las personas de obtener información, su validez, integridad y disponibilidad para poder hacer el mejor uso de la información con el mínimo riesgo.

La seguridad se basa en 3 pilares, pero puede haber más pilares que puedan soportar la seguridad, en este caso, si un lado es débil, entonces se pierde la seguridad o la usabilidad, si falta un lado, la organización será atacada, ya que debe saberse concretamente la función de los pilares.

2.3.4.2 Confidencialidad

La confidencialidad de la información es la clave para el crecimiento y sostenibilidad de una empresa, por lo que es imperativo evitar la divulgación no autorizada de información comercial. Es importante si las empresas grandes, medianas o pequeñas aplican ISO 27001, 27002 según su alcance, porque el estándar indicará cómo se manejan los aspectos de seguridad de la información y evaluará dónde se encuentra ahora y cómo han evolucionado con el tiempo. Toda empresa tiene información confidencial y, por lo tanto, debe protegerla incluso de sus socios comerciales; necesitan ser conscientes de la importancia de manejar adecuadamente la información que generan en su trabajo diario. Muchas empresas grandes, medianas y pequeñas han adoptado estándares internacionales y, con base en ellos, han analizado su situación actual de lo que pueden esperar los pilares de la seguridad informática como la confidencialidad (Rodriguez Baca y otros, 2020).

2.3.4.2.1 Autenticación de usuarios

Se utiliza para determinar quién está accediendo a la información del y quién dice ser.

2.3.4.2.2 Gestión de privilegios

Los usuarios que acceden al sistema solo pueden operar con la información para la que han sido autorizados y solo en la forma en que están autorizados, por ejemplo, gestionando permisos de lectura o escritura según el usuario.

2.3.4.2.3 Cifrado de información

El cifrado, también conocido como encriptado, evita el acceso de personas no autorizadas, debido a esto, la información se transforma de forma comprensible a ilegible y también se aplica a la información con licencia para usted y solo mediante un sistema de contraseña se puede extraer la información de forma inteligible y esto se aplica tanto a la información transmitida como a la almacenada.

Los principios de confidencialidad no solo deben aplicarse para proteger la información, sino también todos los datos e información de los que es responsable. La información puede estar segura no solo porque es de gran valor para la organización, sino, por ejemplo, porque puede regirse por las leyes de protección de datos personales. Un ejemplo de una brecha de seguridad son los bancos, las grandes corporaciones y los gobiernos que filtran para hacer públicas algunas de sus actividades (Romero Castro y otros, 2018).

2.3.4.3 Integridad

Este es el segundo pilar de la seguridad, es la propiedad responsable de asegurar que la información no sea alterada por usuarios no autorizados para evitar la pérdida de consistencia cuando se almacene, procese o transmita. Una violación de la integridad ocurre cuando un empleado, programa o proceso (accidental o maliciosamente) altera o elimina datos críticos que forman parte de la información, dejando su contenido sin cambios a menos que sea modificado por personal autorizado, y documente estos cambios para garantizar su precisión y confiabilidad (Niño Morante, 2018).

2.3.4.4 Disponibilidad

Según Vega Briceño (2021) la disponibilidad se refiere a poder acceder a los datos cuando los necesitamos. La pérdida de disponibilidad puede referirse a diversas interrupciones en cualquier parte de la cadena de comunicación que nos permite acceder a nuestros datos. Dichos problemas pueden ser causados por cortes de energía, problemas con el sistema operativo o las aplicaciones, ataques a red de datos, sistemas comprometidos u otros problemas que impiden que los usuarios accedan a su información. Dichos problemas a menudo son causados por ataques avanzados de denegación de servicio (DoS).

2.3.5 Riesgos de seguridad informática

Chicano Tejada (2015) menciona que un riesgo es un evento o conjunto de eventos que pueden comprometer el proyecto de la organización o impedir su éxito. La definición misma de riesgo siempre es controvertida. Sin embargo, existe un acuerdo sobre las características comunes que deben tener todos los riesgos de TI:

- **Incertidumbre:** el evento que caracteriza el riesgo puede ocurrir o no, no existe certeza sobre su ocurrencia.
- **Perdida:** Si el riesgo se materializa, habrá una serie de consecuencias negativas para la organización. Si no hay efectos negativos, entonces no hay riesgo.

2.3.6 Vulnerabilidades

Según Acosta Molina(2019) el ejemplo, a medida es que más y más dispositivos inteligentes de Internet de las cosas(IoT) se conecten al mundo, habrá más vulnerabilidades en los dispositivos que deben repararse; autenticación de dispositivos, manejo de actualizaciones de dispositivos, comunicación segua, garantía de privacidad e integridad de datos, protección de redes, aplicaciones móviles y en la nube, garantía de alta disponibilidad, predicción y prevención de problemas de seguridad: desde la perspectiva de seguridad de los dispositivos IoT, un diseño de seguridad de múltiples capas se puede implementar un enfoque para administrar dispositivos, datos y aplicaciones IoT basados en la nube. Lo más importante es tomar todas las precauciones e información necesarias. A medida que aumenta el flujo de información digital, a menudo escuchamos y leemos sobre las infracciones de seguridad de Internet de las cosas (IoT).

2.3.6.1 Causas de las vulnerabilidades de los sistemas informáticos

Se puede señalar una cantidad de causas como las respuestas de las vulnerabilidades que afectan al sistema informático (Gómez Vieites, 2015).

2.3.6.2 Tipos de vulnerabilidades

Existen varios tipos de vulnerabilidades que son aprovechadas por los atacantes de interfaz de una red o hurtar información entre las que se mencionan son las siguientes:

2.3.6.2.1 Desbordamiento de buffer

Romero Castro y otros (2018) dicen que los desbordamientos de búfer ocurren cuando el programador no controla el espacio de memoria de un programa, por lo que, si alguien coloca su propio código en ese espacio de memoria, la máquina lo ejecutará antes que otras tareas. Por ejemplo, suele pasar mucho en payloads. Se inserta una cierta cantidad de memoria, o incluso dentro de una puerta trasera, se inserta una cierta cantidad o una cierta cantidad de código en la RAM, se inició previamente, cualquier parte del sistema operativo o dentro del mismo sistema Se utiliza para el inicio normal donde parte del se puede iniciar el archivo.

2.3.6.2.2 Errores de configuración

Otra de las principales vulnerabilidades, son los errores de configuración, se puede mencionar, por ejemplo, las contraseñas por default, contraseñas débiles, usuarios con demasiados privilegios e inclusive la utilización de protocolos de encriptación obsoletos, las configuraciones incorrectas de seguridad son los controles mal configurados o inseguros que ponen en riesgo sus sistemas y datos. Básicamente, cualquier cambio de configuración mal

documentado, configuración predeterminada o error en cualquier componente de punto final puede resultar en una configuración incorrecta (manageengine.com, 2018).

2.3.6.2.3 Errores web

Las grandes redes públicas como internet son muy vulnerables porque son abiertas casi todos. Internet es tan grande que puede usarse para abusar el gran impacto en cada situación en la que nos encontramos nosotros, los grandes robos en internet los realizan los hackers famosos.

Un hacker es alguien que intenta obtener acceso no autorizado a un sistema computacional. Estos piratas informáticos obtener este acceso al encontrar lagunas en las defensas de seguridad. Medidas de seguridad del sitio y del sistema informático; la suplantación de identidad también puede implicar la redirección de enlaces web a direcciones distintas sugeridas donde el sitio web pretende estar (Árevalo Cordovilla y otros, 2020).

2.3.6.2.4 Errores de protocolo

Finalmente, hay una serie de vulnerabilidades en los protocolos, hay una serie de otros protocolos que a menudo se identifican sin seguridad o se consideran rigurosamente, y muchas veces no se prevé su proliferación. Dado que internet no está preparado a esta escala, la seguridad no es una preocupación.

Un protocolo en computación es un conjunto formal de estándares y especificaciones, gobiernan el formato y el control de las interacciones entre diferentes entidades en una red o sistema de comunicación. El objetivo es que puedan transferir datos entre ellos, como consultores informáticos, vemos más detalles sobre este tema.

El acuerdo establece el estándar de seguridad informática en el proceso de comunicación y proporciona información detallada sobre el proceso de transmisión de datos, un proceso puede ser manejado por múltiples protocolos simultáneamente (Imagar, 2021).

2.3.6.2.5 Aprovechamiento de las vulnerabilidades

En general, hay dos formas de explotar las vulnerabilidades, como se muestra a continuación:

- Forma remota
- Ingeniería social

En la forma remota se llega mediante una computadora y se empieza a hacer análisis, ataques a un cierto servidor y tratar de vulnerarlo, si se logra el acceso, quiere decir que ya se hizo alguna explotación remota. En la parte de la ingeniería social, alguien puede ayudar de manera interna, una persona dentro de la organización puede ayudar a realizar un acceso no permitido. También

existen las partes de ataques directos, una vulnerabilidad de forma remota utilizando internet, se aprovecha de que algún software o servicio tiene un puerto abierto volviéndose vulnerable. Otra de las partes es engañando a un usuario, aplicando ingeniería social con alguna memoria o algún archivo infectado, se puede aprovechar de alguna vulnerabilidad que se encuentra dentro del mismo sistema (Romero Castro y otros, 2018).

2.3.7 Debilidad en diseño de los protocolos

Algunos protocolos utilizados para prestar determinados servicios en redes como Internet han sido diseñados sin un conocimiento previo de cómo reaccionar ante situaciones inusuales o el mal comportamiento de una de las partes en la comunicación hacia adelante, que puede intentar "confundir" a la otra parte, por ejemplo, provocando un ataque de Denegación de servicio (DoS (Denegación de servicio)) (Gómez Vieites, 2015).

2.3.8 Errores de programación

González (2022) menciona que otra causa de muchas vulnerabilidades del sistema informático es el diseño del programa o los errores de codificación.

Los errores de programación reaccionan de diferentes maneras y pueden clasificarse según la etapa en la que ocurren. Algunos tipos de errores son más difíciles de detectar y corregir que otros. Vamos a ver:

2.3.8.1 Errores de sintaxis

Estos son errores en el código fuente. Estos pueden ser causados por faltas de ortografía de palabras reservadas, expresiones incorrectas o incompletas, variables no declaradas, etc. Se encontró un error de sintaxis durante la fase de compilación. Además de generar código objeto, el compilador también nos dará una lista de errores de sintaxis. De hecho, solo nos dará uno u otro, ya que, si hay errores, no será posible generar el código objeto.

2.3.8.2 Errores de ejecución

Incluso si se obtiene el ejecutable, pueden ocurrir errores durante la ejecución del código. En el caso de un error de tiempo de ejecución, generalmente no recibimos un mensaje de error muy específico o incluso ningún error, sino que simplemente el programa se cierra inesperadamente. Estos errores son más difíciles de detectar y corregir (porque están en nuestra lógica de aplicación). Existen herramientas de utilidad para buscar estos errores, se llaman depuradores. Estos programas nos permiten detener la ejecución del programa, examinar variables y ejecutar nuestros programas paso a paso (instrucción por instrucción). Esto es útil para detectar

excepciones, errores sutiles y errores según las circunstancias. Los errores de tiempo de ejecución a menudo son causados por situaciones que la aplicación no ha considerado, p. el usuario ingresa letras que están fuera de control en lugar de números.

2.3.9 Metodologías cualitativas y cuantitativas de análisis de riesgo

Según Chicano Tejada (2015) el control de seguridad es una serie de medidas para mitigar las vulnerabilidades y mitigar los riesgos de los sistemas de información. Actualmente, existen cuatro tipos de controles, como se muestra en la siguiente tabla.

Tipos de controles de seguridad	
Control	**Descripción**
Disuasorio	Su objetivo principal es reducir la posibilidad de ataques.
Preventivo	Su objetivo es defender al sistema de informes vulnerables, intentando secuestrar el inicio de los atacantes o reduciendo los daños causados.
Correctivo	Su objetivo principal es reducir el impacto de las amenazas.
Detective	Es responsable de detectar y prevenir posibles ataques.

Tabla 1 Tipos de controles de seguridad

La gestión de riesgos debe ser capaz de determinar cuáles de estos controles son los más adecuados, eficientes y rentables. Por esta razón, existen dos formas de realizar un análisis de riesgo:

- Metodología cuantitativa
- Metodología cualitativa

2.3.10 Identificación de los activos involucrados en el análisis de riesgos y su valoración

De Freitas (2023) menciona que el proceso de análisis y gestión de riesgos consta de varias fases.

Fases del proceso de análisis y gestión de riesgos
Identificación de activos
Valoración de activos
Identificación de amenazas
Sentencia de impacto de amenaza
Evaluación de riesgo
Establecimiento (mitigación) de medidas de protección.
Compruebe el impacto y determine el impacto restante.
Evaluación de riesgos y determinación del riesgo residual.

Tabla 2 Fases del proceso de análisis y gestión de riesgos

ISO 27001:2007 recomienda que, para fines de gestión de riesgos, primero defina el alcance de los estándares de la empresa e identifique todos los activos de información basados en eso. Los activos de información deben evaluarse para determinar su impacto en la organización. Luego se debe realizar un análisis para determinar qué activos están en riesgo. Es en este punto que se deben tomar decisiones sobre qué riesgos asumirá la organización y qué controles se implementarán para mitigarlos.

2.3.11 Identificación de las amenazas que pueden afectar a los activos identificados previamente

Una amenaza es un conjunto de hechos y eventos que pueden ocurrir y afectar adversamente los activos del sistema de información. Por lo tanto, proteger los activos de tales amenazas es una prioridad.

Al identificar amenazas, debe tener en cuenta que pueden activarse accidentalmente o viceversa.

Ejemplos de amenazas aleatorias son amenazas naturales (terremotos, inundaciones, etc.), amenazas industriales (cortes de energía, fallas de comunicación, etc.) o amenazas humanas (errores imprudentes y omisiones de acciones esenciales para la operación del sistema).

Por otro lado, las amenazas intencionales son intencionales y la mayoría son sancionadas por la ley. Los ejemplos incluyen intrusiones, espionaje, robo de información y fraude (Chicano Tejada, 2015).

2.3.12 La comunicación en la empresa

Antes de comenzar a auditar, es útil considerar cómo funciona su sistema de comunicación interno y cómo funciona. De esta manera, los problemas que los auditores encuentran y entienden si pueden resolver se entienden mucho mejor. La comunicación de la empresa se compone de muchos elementos internos y externos que deben ser analizados a fondo, así que los casos se enfrentan para hacer su trabajo correctamente.

La comunicación es generalmente la capacidad de todos los seres vivos para transmitir información, emociones y experiencias a los demás. Por lo tanto, todas las comunicaciones requieren remitentes, mensajes y destinatarios (Pallerola Comamala, 2015).

2.4 SEGURIDAD DE LA INFORMACIÓN SEGÚN LA ISO 27001

2.4.1 Definición de la seguridad informática

En el caso de estudiantes o empleados corporativos cuyas PC están llenas de datos personales, al decidir no prestar su PC a nadie, ha eliminado en gran medida el riesgo de perder su información; sin embargo, necesita intercambiar información con otros, tanto dentro de la empresa como con otros, directamente o a través de los servicios disponibles en Internet, lo que lo deja vulnerable a ataques o controles electrónicos.

Sin embargo, las empresas aún enfrentan un riesgo mayor: es el personal de la empresa quien roba, daña o elimina información importante; Aun cuando la selección y promoción del personal y otras políticas sean adecuadas dentro de la empresa, siempre existe el riesgo de que los propios empleados, sobre todo, puedan sustraer información importante, dársela al público de otra empresa o revenderla al mejor postor. Si la empresa atrapa a un empleado robando información, puede ser denunciado y procesado por las autoridades correspondientes y enfrentar un juicio que lo lleve a la cárcel; sin embargo, esto no dará como resultado que se recupere la información o que alguien fuera de la organización se aproveche de ella. Así que es mejor evitar que esto suceda tanto como sea posible.

La seguridad informática es la disciplina, basada en políticas y normas internas y externas de la empresa, encargada de proteger la integridad y confidencialidad de la información almacenada

en los sistemas informáticos, contra cualquier tipo de amenaza, minimizando el riesgo físico y lógico al que está expuesta (Baca Urbina, 2016).

2.4.2 Objetivos de la seguridad informática

Kiligann (2022) menciona que el propósito de la seguridad informática es mantener la integridad, disponibilidad, confidencialidad, control y autenticidad de la información procesada en las computadoras. Reduzca el riesgo y detecte posibles problemas y amenazas de seguridad. Garantizar el uso adecuado de los recursos del sistema y las aplicaciones. Limite la pérdida del sistema y la recuperación asociada en caso de un incidente de seguridad. Cumplir con el marco legal.

Para que la cadena de suministro funcione a pleno rendimiento, ya se trate de una organización de fabricación o de servicios, es fundamental terminar los cuatro procesos o fases del proceso administrativo. La seguridad informática tiene sentido cuando uno entiende por qué quiere proteger las características de su información. La empresa tendrá más posibilidades de sobrevivir en un mercado cada vez más competitivo.

2.4.3 Normas ISO 27001

Es un estándar desarrollado como modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) para cualquier tipo de organización. Permite el diseño y la implementación de un SGSI, en función de las necesidades, los objetivos, los requisitos de seguridad, los procesos, el personal, el tamaño, los sistemas de soporte y la estructura de una organización.

Esta Norma Internacional se ha estructurado metodológicamente para dar cabida al modelo "Plan Do Check Act", que se aplica para estructurar todos los procesos del SGSI y tiene como objetivo: establecer, gestionar y documentar el SGSI, tener la Responsabilidad de la Gestión, incluido el seguimiento, la auditoría y la mejora. La norma ISO 27001 trabaja sobre el enfoque de procesos, cuya aplicación detallada y oportuna requiere de un manual de procesos, establecido, definido, documentado y validado. El diseño, la implementación y el funcionamiento adecuados del SGSI permiten que una organización lleve a cabo sus actividades de manera más eficiente; sin embargo, si una organización no rediseña el proceso antes de implementar la Cumbre Mundial sobre la Sociedad de la Información (CMSI), el rendimiento de la organización se ralentizará (Mantilla Guerra, 2018).

2.4.4 Sistema de gestión de la seguridad de la información

Según Fernández Rivero y Gómez Fernández (2018) que, si bien se podría pensar que un sistema de gestión está dirigido a las grandes empresas, son precisamente las organizaciones pequeñas las que más se pueden beneficiar de él, ya que les proporciona un hormiguero, el conocimiento y los estándares no están a su alcance. Sin embargo, es importante conocer la organización y su contexto, para que la definición del sistema de gestión tenga en cuenta los objetivos de negocio específicos de la organización, para los cuales la gestión de la seguridad de la información debe ser adecuada.

Cuando una organización desea cumplir con los requisitos de la norma UNE-EN ISO/IEC 27001, debe demostrar la implementación efectiva de las secciones a 10, que conforman el cuerpo principal de la norma:

- Contexto organizacional.
- Liderazgo.
- Planificación.
- Soporte.
- Operación.
- Evaluación del desempeño.
- Mejora

El sistema incluirá información documentada a diferentes niveles:

- Política proporcionando líneas generales de actuación en cada caso.
- Información documentada del proceso (comúnmente conocida como procedimientos), que proporciona una descripción de las actividades a realizar.
- Información documentada sobre evidencia (anteriormente conocida como registros), que demuestra que se han llevado a cabo las actividades planificadas.

2.4.5 El valor de la información

Según Baca Urbina (2016) en los negocios, ya sea de manufactura o de servicios, los sistemas de información son como los sistemas nerviosos. Si alguna parte de su sistema nervioso está obstruida o no puede funcionar, provocará un mal funcionamiento de los músculos de sus dedos, brazos o piernas e incluso puede afectar el funcionamiento de todo el sistema fisiológico y posiblemente de todo el organismo.

Lo mismo sucede en los negocios; todos los sistemas comerciales están interconectados por información y se han separado en diferentes ramas solo con fines de investigación. La información es necesaria para la vida de cualquier ser, para cualquier tipo de negocio, así como para la sociedad en general.

Pero ¿por qué los actores maliciosos buscarían sabotear, robar o destruir la información de empresas o usuarios de una computadora personal común (computadora)? Se ha tomado, en varios casos, para demostrar que socialmente son mucho más ingeniosos y creativos que los "chicos buenos" del otro lado de la mesa. Por supuesto que habrá gente malvada que realizará estas acciones por dinero; ej., robar tecnología confidencial de otras empresas para venderla al mejor postor o competir, o acceder a computadoras personales para extraer números de cuentas bancarias y contraseñas de cuentas de ahorro personales “vacías” o del sistema bancario para realizar transferencias de dinero a su favor, además de miles de otras acciones maliciosas.

2.4.6 Principios de la seguridad física

Es muy importante señalar que, aunque nuestra empresa sea la más segura desde el punto de vista de ataques externos, hackers, virus, etc., su seguridad será nula si no cuenta con un plan contra incendios.

La seguridad física es uno de los aspectos que más se pasa por alto al diseñar un sistema informático. Si bien se esperan algunos aspectos que se analizan a continuación, otros, como la detección de un atacante dentro de la empresa que intenta obtener acceso físico a la sala de operaciones corporativas, no lo son.

Así, la seguridad física incluye la aplicación de barreras físicas y procedimientos de control, como medidas para prevenir y contrarrestar las amenazas a la información y los activos clasificados. Se ocupa de los controles y mecanismos de seguridad en y alrededor de la ubicación física del sistema informático, así como los medios de acceso remoto hacia y desde él; implementado para proteger el hardware y los medios de almacenamiento de datos.

La seguridad física se centra en proteger las amenazas creadas por el hombre y la naturaleza del entorno físico en el que se encuentra el centro (Costas Santos, 2015).

2.4.7 Principios de la seguridad lógica

Navarro(2021) menciona que, en la seguridad de la información, la seguridad lógica se refiere a la seguridad del uso de sistemas y software. También significa asegurar los datos, procesos y procedimientos, así como el acceso ordenado y autorizado a la información para los usuarios.

En general, la seguridad lógica tiene los siguientes objetivos:

- Restrinja el acceso a programas y archivos solo a usuarios autorizados.
- Los operadores pueden trabajar sin una estrecha supervisión, pero no pueden cambiar programas o archivos que no cumplan.
- Verifique que se estén utilizando los datos, archivos y programas correctos en y con los programas correctos.
- Se garantiza que la información transmitida será recibida solo por el destinatario y nadie más.
- Asegúrese de que el destinatario reciba la misma información que se envió.

2.4.8 Plan de mejoramiento

El plan de mejora se basa en los resultados del análisis de no conformidades, acciones correctivas y preventivas y procesos de evaluación. Su propósito u objetivo es orientar las acciones necesarias para eliminar las debilidades identificadas y sus causas, sin alterar las fortalezas ya alcanzadas. En otras palabras, un plan de mejora es un medio conceptual y una guía para actuar sobre lo que se requiere, con el fin de modificar el estado actual del sistema para asegurar un futuro de mejor calidad, manteniendo sus fortalezas. Define los objetivos del plan de mejora, establece las acciones a seguir, su plazo de desarrollo e identifica a los responsables.

Una vez que se implementa un sistema de seguros en la instalación, es hora de observar la alineación de las organizaciones. Para ello, se deberá estandarizar el proceso de suministro o transferencia de datos, el cual dependerá del medio en que se realice, ya sea en soporte físico o electrónico. Este proceso deberá estar respaldado por un documento que, como en el caso anterior, describa todas las actividades que se deben considerar para brindar, incorporar o compartir datos de calidad. El documento será elaborado por la entidad donde confluyen los datos de las distintas fuentes de información y tendrá en cuenta la estructura descrita en los puntos anteriores: objetivos, alcance, responsabilidades, conceptos estandarizados relacionados con los datos compartidos o transferidos, el marco legal que sustenta la proceso, el producto o resultado esperado, insumos disponibles (es decir, hardware, software), recursos humanos, formato metodológico (Salcedo Cifuentes y otros, 2018).

2.4.9 Tendencias en el área de la “gestión de seguridad de información”

La Gestión de la Seguridad de la Información ha evolucionado desde sus inicios como norma ISO-17799 en el año 2000, para convertirse en la familia ISO 27000 desde el año

2005, pretendiendo ser una norma internacional que brinda recomendaciones para su implementación. Actualmente, gestiona la seguridad de la información. Este estándar está destinado a las personas responsables de iniciar, implementar o mantener la seguridad de la información en miembro.

ISO 27001:2005 tiene como objetivo establecer, implementar, operar, monitorear, analizar, mantener y mejorar un sistema de gestión de seguridad de la información, ISMS, y cumplir con ISO 9001 para respaldar la implementación y operar, ser consistente e integración con sistemas de gestión relacionados. es decir, fusionar diferentes sistemas de gestión organizacional en un solo sistema integrada, optimizando sus procesos y facilitando el flujo de información entre ellos.

La versión 2013 de ISO27001 proporciona un enfoque y una estructura comunes a los estándares de sistemas de gestión para facilitar la integración con otros estándares de sistemas de gestión. El estándar ISO-27001 actualizado tiene 114 controles en 14 categoría o sector, a diferencia de los 133 controles y 11 categorías contenidos en la edición de 2005. Los requisitos de análisis de riesgos están de acuerdo con la norma ISO 31000 para la gestión de riesgos (Silva Coelho y otros, 2018).

2.4.10 Los controles de seguridad de la información

Casal(2022) menciona que los controles de seguridad internos están diseñados para garantizar que todos los activos, sistemas, equipos, datos y documentos relacionados con el uso de la tecnología de la información estén protegidos contra accesos no autorizados, posibles daños y usos indebidos o ilegales, y siempre sean funcionales, seguros y protegidos.

El objetivo de la seguridad informática es proteger la información de una variedad de amenazas para garantizar la continuidad del negocio, minimizar el costo del daño potencial para el negocio y maximizar el retorno de la inversión sin dejar de ser competitivo a través de un mejor posicionamiento competitivo para aprovechar la oportunidad.

En este sentido, se puede decir que se debe proteger la seguridad de la información:

- Asegura que la información sea accesible solo para personal autorizado con derechos de revisión o modificación, según sea el caso.
- **Integridad:** mantener la integridad y exactitud de la información y el procesamiento relacionado.

- **Disponibilidad:** Garantizar que aquellos que tienen el derecho legal de acceder a la información puedan usarla cuando la necesiten.

2.4.11 Análisis de brechas

Espinoza Vanegas(2018) menciona que se realiza un análisis de brechas (GAP) para iniciar la configuración del sistema gestión de la seguridad de la información (SGSI), y permite conocer directamente el nivel de madurez de la entidad relacionada con controles requeridos por la norma. Se ha aplicado GAP al proceso de liquidación dependiente del consejo de administración general, consultorio urbanístico, consultorio comunicación y control interno.

La información de soporte debe ser de fundamental importancia para la operación e incluso para el logro de la Unidad en el corto, mediano y largo plazo. limita la realización de tareas y también asegura su supervivencia en un entorno cada vez más dinámico y arriesgado. Existe una gama de controles para reducir el riesgo de acuerdo con la NTC/ISO 27001:2013 que ayudan a administrar y proteger los activos de información críticos para la operación y funcionamiento de los procesos organizacionales.

Dominios ISO 27001	Objetivos de Control
Política de seguridad	Objetivo de control A.5
Organización de la seguridad de la información	Objetivo de control A.6
Seguridad de los RRHH	Objetivo de control A.7
Gestión de activos	Objetivo de control A.8
Gestión de acceso	Objetivo de control A.9
Criptografía	Objetivo de control A.10
Seguridad física y ambiental	Objetivo de control A.11
Seguridad en las operaciones	Objetivo de control A.12
Seguridad en las comunicaciones	Objetivo de control A.13
Adquisición de sistemas, desarrollo y mantenimiento	Objetivo de control A.14
Relación con proveedores	Objetivo de control A.15
Gestión de los incidentes de seguridad	Objetivo de control A.16
Continuidad de negocio	Objetivo de control A.17
Cumplimiento con requerimientos legales y contractuales	Objetivo de control A.18

Tabla 3 Dominios de la norma NTC-ISO 27001:2013

2.5 Conclusiones

- La planificación de la auditoría informática es esencial para el funcionamiento óptimo de los sistemas de información, de modo que estos sistemas sean suficientes y confiables para brindar recomendaciones a los contratistas de auditoría, propietarios, gerentes o la alta gerencia al realizar una evaluación final.
- La auditoría informática ayuda con el proceso de recopilar, agrupar y evaluar las pruebas de los sistemas informáticos y ver si se pueden proteger los activos y mantener la integridad de los datos.
- La seguridad informática para las empresas es cada vez más compleja y, como se ve en la investigación de seguridad informática para organizaciones o empresas, los riesgos asociados con las amenazas a la seguridad de las empresas son reales. Las pérdidas se registran cada año y millones de empresas sufren los innumerables ataques de virus y las brechas de seguridad informática que sufren estas empresas.
- La serie ISO 27001 define los requisitos para la creación, implementación, mantenimiento y mejora de SGSI basándonos en a los siguientes estándares: integridad, disponibilidad y confiabilidad de la información en la organización. Por otro lado, la norma ISO 27005 brinda orientación para el análisis de riesgos, pero no para la implementación.

CAPÍTULO III

3 MARCO INVESTIGATIVO

3.1 Introducción

El presente capítulo se muestra la información de los tipos de investigación que se realizaran en la Auditoría informática. Con estos tipos de investigación, se conocerá cómo definir la investigación.

Utilizar métodos de investigación para lograr resultados con la ayuda de herramientas de recopilación de datos obtenidos en encuestas y entrevistas.

3.2 Tipo de investigación

3.2.1 Investigación cualitativa

La investigación cualitativa implica la recopilación y el análisis de datos cuantitativos para comprender conceptos, opiniones o experiencias, así como datos sobre experiencias vividas, sentimientos o comportamientos y los significados que las personas les atribuyen. Por lo tanto, los resultados se expresan en palabras. También puede ser útil explorar cómo o por qué ocurrió un incidente, explicar el incidente y ayudar a describir qué hacer (Santander Becas, 2021).

La investigación cualitativa es utilizada para explicar y recopilar actividades relacionadas con el problema.

3.2.2 Investigación cuantitativa

El diseño del estudio cuantitativo es método empírico común a la mayoría de las ramas de la ciencia, propósito de la investigación cuantitativa es obtener conocimientos básicos y elección, el modelo más adecuado que permite conocer la realidad más justa, ya que se recopilan y analizan datos a través de conceptos y variables medibles.

La investigación cuantitativa sirve para recopilar y evaluar datos procedentes de diversas fuentes, la investigación cuantitativa utiliza técnicas informáticas, estadísticas y matemáticas para obtener resultados. Se trata de cuantificar el problema y comprender su importancia buscando resultados que se puedan predecir para una población más grande (Alan Neill & Cortez Suárez, 2018).

La investigación cuantitativa ayudó con el análisis de datos obtenidos de diversas fuentes con herramientas informáticas y obtener los resultados estadísticos de la investigación.

3.2.3 Investigación descriptiva

Se utilizan para analizar cómo se ve un fenómeno, y sus componentes y como se manifiestan. Permiten el detalle del fenómeno se estudia básicamente midiendo una o más de sus propiedades.

Identificar las características del universo estudiado, mostrar patrones de comportamiento y actitudes del universo estudiado, establecido comportamientos específicos, descubierto y verificado asociaciones entre variables de a la investigación. De acuerdo con los objetivos planteados, el investigador indica el tipo de descripción propuesto fundar (Vásquez Hidalgo, 2005).

La investigación descriptiva se utilizó para la recopilación de información con la entrevista y encuesta y a la vez con la tabulación y análisis estadísticos de la auditoría.

3.3 Métodos de investigación

3.3.1 Método inductivo

Es el método científico de sacar conclusiones generales basadas en suposiciones o antecedentes específicos. A menudo se basa en observar y experimentar eventos y acciones específicas para llegar a una solución o conclusión general sobre ellos; es decir, en este proceso se parte de datos y se termina con una teoría, por lo que se puede decir que va de lo particular a lo general. La inferencia va de lo particular a lo general (Carbajal Suárez, 2019).

Desde la revisión el estudio se divide en pequeñas unidades de aprendizaje, siendo estas partes más detalladas para la revisión y luego su reorganización, con este método se combina, de manera armoniosa, no excluyente, las fases generales para seguir en una auditoría.

3.3.2 Método deductivo

El tipo de razonamiento lógico caracterizado por el hecho de que la conclusión se sigue necesariamente de varias premisas se denomina método o razonamiento deductivo.

La deducción puede entenderse como la obtención de una conclusión válida, comprobable y transferible a partir de una o más premisas de tipo general (Uriarte, 2022).

El método deducción incluye la derivación de aspectos específicos de leyes generales, donde se aplicará en la formación de los objetivos generales y específicos, a declarar las normas de la auditoría y la aplicación de normas generales a situaciones específicas.

3.3.3 Método analítico

El método analítico es un método de investigación que consiste en clasificar el todo, descomponiéndolo en partes o factores para observar sus causas, naturaleza y efectos. El análisis es la observación y el examen de un hecho particular

Para comprender su naturaleza, es necesario conocer la naturaleza del fenómeno y el objeto de estudio. Este método nos posibilita conocer más sobre el objeto de estudio, que a su vez puede: explicar, hacer analogías, comprender mejor su comportamiento y establecer nuevas teorías (Ruiz Limón, 2006).

Los procedimientos analíticos se utilizaron en una auditoría para obtener evidencia adecuada y fiable en la valoración final precisa de la aportación de recursos humanos a través de las actividades.

3.3.4 Método sintético

El enfoque sintético es un proceso de análisis inferencial que busca una forma de reconstruir eventos de manera generalizada utilizando los diversos bloques de construcción presentes en el desarrollo de eventos. Este enfoque permite a las personas resumir lo que ya saben. La síntesis es un proceso mental que comprime la información en la memoria. Este proceso muestra la capacidad humana para reconocer todas las cosas conocidas y extraer de ellas las propiedades más importantes (Reyqui, 2019).

Este método ayudó a ejecutar los resultados analizados de la de auditoría en las propiedades de los elementos.

3.4 Fuentes de información de datos

Dentro de las empresas comerciales de El Carmen se puedo identificar que cuentan políticas de seguridad de la información que son manejadas por sus empleados y administrativos.

3.4.1 Fuentes primarias – Fuentes secundarias

3.4.1.1 Fuentes secundaria - Encuesta

Las encuestas por muestreo son la técnica más utilizada en la investigación en ciencias sociales. Se utiliza para recopilar información de las personas sobre características, creencias, opiniones, expectativas, conocimientos, comportamiento actual o comportamiento pasado (Ocampo, 2020).

La encuesta se aplicó a los empleados de las empresas comerciales de El Carmen con la finalidad de conocer si las empresas cuentan con políticas de seguridad de la información.

3.4.1.2 Fuente primaria - Entrevista

Las entrevistas son conversaciones con un propósito. Es un proceso interactivo que involucra muchos aspectos de la comunicación más allá de hablar o escuchar, como gestos, posturas, expresiones faciales y otros comportamientos comunicativos (Grados & Sánchez, 2018).

La entrevista se aplicó a los administrativos de cada una de las empresas comerciales de El Carmen con fin de tener de primera mano la información de que se cumplan las políticas de seguridad de la información.

3.5 Estrategia operacional para la recolección de datos

3.5.1 Población – Segmentación – Técnica de muestreo

3.5.1.1 Población

La población se trata de un conjunto de elementos los cuales contienen características en la cual se lleva a cabo una investigación sobre lo que se pretende estudiar. En ocasiones la población puede ser accesible, es decir donde el número de elementos sea menor y esté delimitado, en otros casos la población es demasiado grande y el investigador no tiene acceso a ella (Ventura León, 2017).

La población a que se aplicó los instrumentos de investigación es a nueve empleados de tres empresas comerciales de El Carmen.

3.5.1.2 Muestra

Es un subconjunto o parte del universo o población en la que se llevara a cabo la investigación. Hay procesos para el número de componentes de muestreo, como fórmulas, lógicas y otros componentes que se verán a continuación. Las muestras son parte del representante de la población (Lopéz, 2004).

No se utilizó muestra porque la población no es representativa para el muestreo a comerciales de El Carmen y se han elegido a empleados y directivos de las empresas para realizarles las encuestas.

Se seleccionó a los trabajadores del área de informática para la realización de las encuestas y para la entrevista se obtuvo la información del principal jefe del departamento de informática.

3.5.2 Análisis de las herramientas de recolección de datos

3.5.2.1 Encuesta – Entrevista

Encuesta Dirigida a: Empleados de tres empresas comerciales de El Carmen.

Objetivo: Identificar nivel de conocimiento del proceso sobre la situación actual en cuanto a seguridad de la información en empresas comerciales de El Carmen.

Nombre de la empresa: Translatin S.A.

1. **¿Conoce usted en que consiste la seguridad de la información?**
   SI () NO ()
2. **¿Conoce usted sobre las políticas de seguridad de la información?**
   SI () NO ()
3. **Conoce usted si la empresa cuenta con políticas de seguridad de la información**
   SI () NO ()
4. **La empresa ha socializado con usted las políticas de seguridad de la información**
   SI () NO ()
5. **¿Sabe usted si la empresa ha sido víctima de ataques informáticos en sus datos en los últimos 3 años?**
   SI () NO ()
6. **¿Sabe usted si la empresa ha sido víctima de ataques informáticos en su infraestructura tecnológica en los últimos 3 años?**
   SI () NO ()
7. **¿La empresa cuenta con un Sistema de Gestión de la Seguridad de la Información (SGSI)?**
   SI () NO ()
8. **¿Existe tecnología para el etiquetado de la información (pública, privada o confidencial)?**
   SI () NO ()
9. **¿Se cuenta con Tecnología para el respaldo y recuperación de la Información?**
   SI () NO ()
10. **Usted actualiza sus contraseñas con frecuencia**
    SI () NO ()
11. **Sus contraseñas cumplen con las políticas de contraseña segura**
    SI () NO ()
    NO CONOCE SOBRE EL TEMA ()

Entrevista dirigida a: Responsables de la seguridad de la información en la empresa

Objetivo: Identificar el nivel de conocimiento del proceso sobre la situación actual en cuanto a seguridad de la información en empresas comerciales de El Carmen.

Nombre de la Empresa: Translatin S.A.

Cargo que ocupa en la empresa: Administrador

1. **La empresa cuenta con políticas de seguridad de la información**

   _____

   _____

2. **La empresa ha socializado con sus empleados las políticas de seguridad de la información**

   _____

   _____

3. **¿Por qué medios ha realizado la socialización?**

   _____

   _____

4. **La empresa cuenta con un control sobre el acceso fisco a las copias de seguridad**

   _____

   _____

5. **¿Los empleados tienen la formación que necesitan para prevenir errores de seguridad informática?**

   _____

   _____

6. **La empresa invierte en ciberseguridad**

   _____

   _____

7. **Los empleados hacen un uso adecuado de las contraseñas y datos personales**

   _____

   _____

8. **La empresa cuenta con tecnología para el respaldo de la información**

   _____

   _____

9. **La empresa cuenta con controladores de seguridad para todos los usuarios empresariales**

   _____

   _____

10. **La empresa cuenta con un plan de prevención de riesgos informáticos**

    _____

    _____

11. **Ha tenido usted algún incidente de seguridad de la información**

_____

_____

12. Sabe usted cuál es el proceso que se debe seguir con un incidente de seguridad

_____

_____

13. En los últimos tres años los empleados han reportado problemas de seguridad de la información

_____

_____

14. Conoce usted las responsabilidades que tiene sobre la información que tiene a su manejo

_____

_____

3.5.3 Estructura de los instrumentos de recolección de datos aplicados

La encuesta consta de 11 preguntas donde se propone una lista de dos respuestas. Donde existe una pregunta pilota que es la número 3 que es para verificar la información existente en las repuestas emitidas por los encuestados. Además, existen preguntas para identificar si las empresas cuentan con seguridad de la información.

Se plantea una entrevista estructurada de 14 preguntas con el fin de recolectar información sobre que si las empresas comerciales cumplen con las políticas de seguridad de la información. Las preguntas están dirigidas a los administrativos de cada una de las empresas considerando abarcar la información necesaria.

3.5.4 Plan de recolección de datos

El plan se diseñó con la ayuda del administrador con el siguiente detalle:

Día	Hora	Personal	Tipo de instrumento
12/09/2022	11:19	Empleados del área informática de la Empacadora Translatin	Encuesta
12/09/2022	12:05	Administrador de la empresa Translatin	Entrevista
13/09/2022	11:00	Empleados del área informática de la Empacadora Hermanos Loor	Encuesta
13/09/2022	12:00	Empleados del área informática de la Empacadora Hermanos Loor	Entrevista
14/09/2022	10:00	Empleados del área	Encuesta

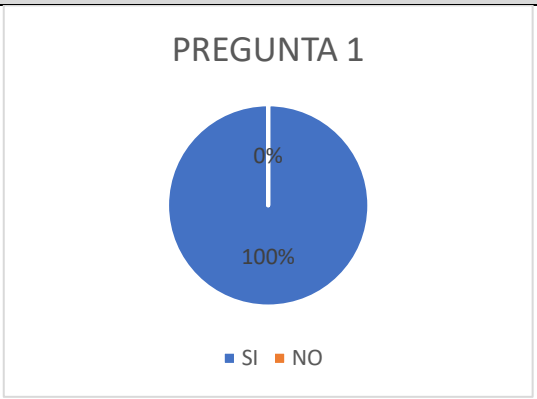
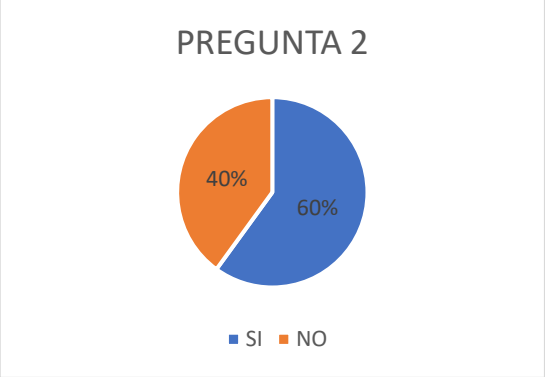
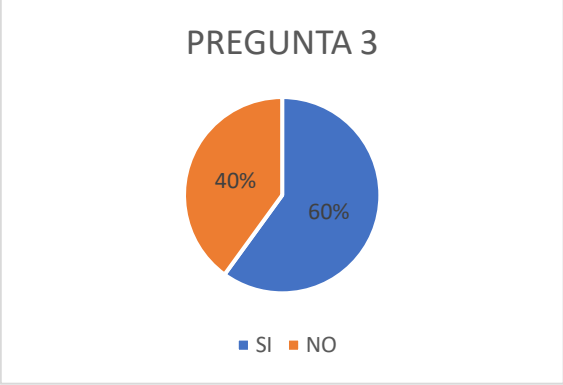
		informática de la Empacadora Alcívar	
14/09/2022	11:00	Empleados del área informática de la Empacadora Alcívar	Entrevista

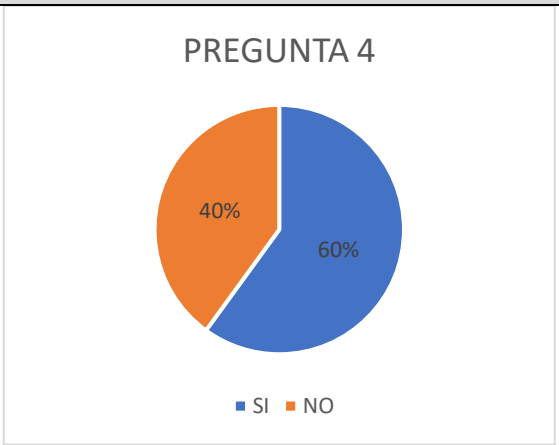
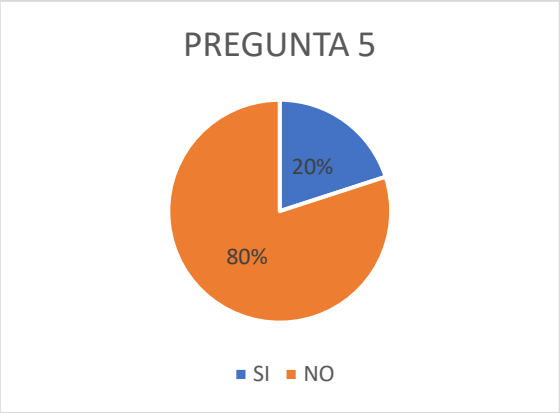
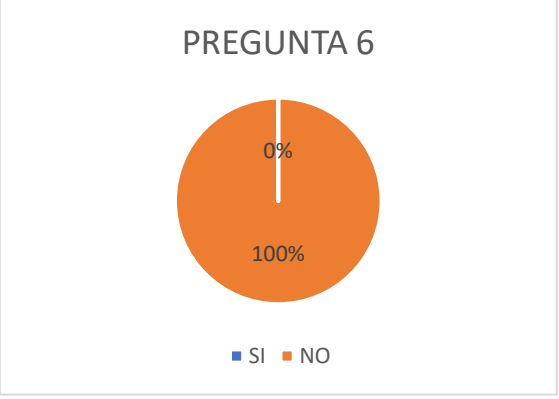
Tabla 4 Plan de recolección de datos

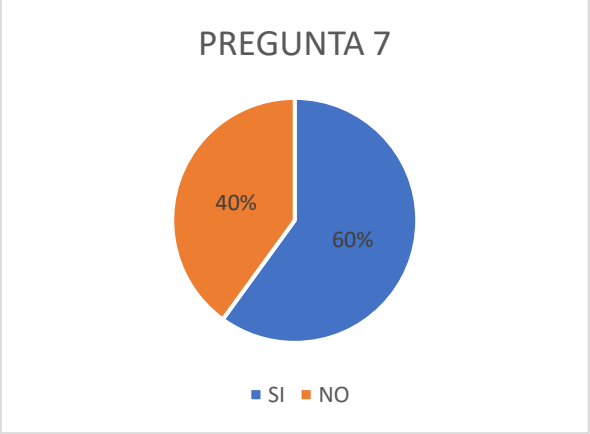
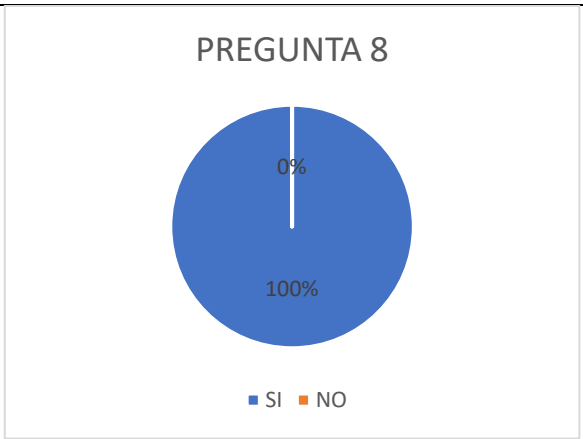
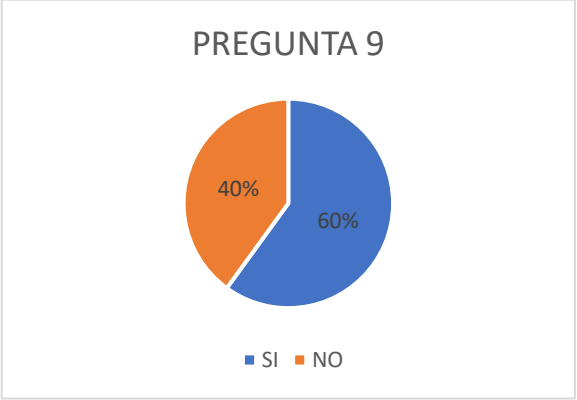
3.6 Análisis y presentación de resultados

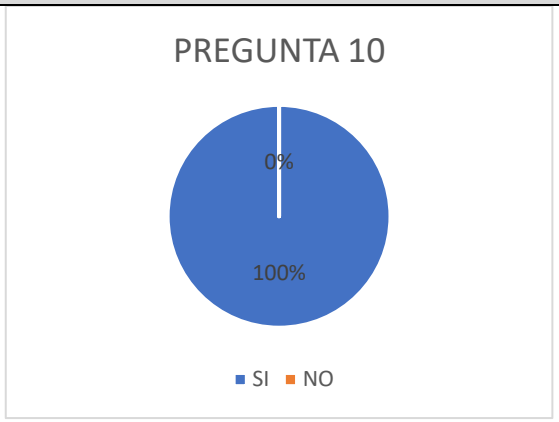
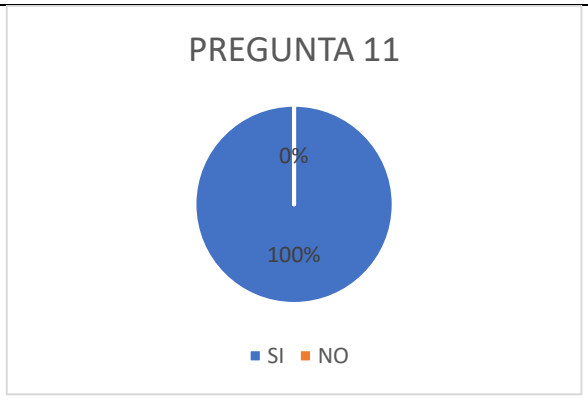
3.6.1 Tabulación y análisis de los datos

3.6.1.1 Encuesta aplicada a empleados de empresas comerciales de El Carmen

PREGUNTA	GRÁFICO	INTERPRETACIÓN
¿Conoce usted en que consiste la seguridad de la información?		La totalidad del personal encuestado conoce en que consiste la seguridad de la información
¿Conoce usted sobre las políticas de seguridad de la información?		Más de la mitad del personal conoce sobre las políticas y el restante no conoce las políticas de seguridad
Conoce usted si la empresa cuenta con políticas de seguridad de la información		Más de la mitad conoce que la empresa cuenta con políticas de seguridad de la información

PREGUNTA	GRÁFICO	INTERPRETACIÓN
La empresa ha socializado con usted las políticas de seguridad de la información		Más de la mitad del personal confirma que si se han socializado las políticas de seguridad
¿Sabe usted si la empresa ha sido víctima de ataques informáticos en sus datos en los últimos tres años?		La mayoría desconoce que la empresa haya sido víctima de ataques informáticos
¿Sabe usted si la empresa ha sido víctima de ataques informáticos en su infraestructura tecnológica en los últimos 3 años?		La totalidad de los encuestados no conoce que la empresa haya sufrido ataque informático en su infraestructura

PREGUNTA	GRÁFICO	INTERPRETACIÓN
¿La empresa cuenta con un Sistema de Gestión de la Seguridad de la información (SGSI)?		La mayor parte del personal afirma que la empresa cuenta con un Sistema de Gestión de Seguridad de la Información
¿Existe tecnología para el etiquetado de la información (pública, privada o confidencial)?		La totalidad de los encuestados conoce que de la tecnología del etiquetado de la información
¿Se cuenta con Tecnología para el respaldo y recuperación de la información?		La mayor parte del personal confirma que si cuentan con tecnología para el respaldo y recuperación de la información

PREGUNTA	GRÁFICO	INTERPRETACIÓN
Usted actualiza sus contraseñas con frecuencia		La totalidad de los encuestados confirman que actualizan sus contraseñas con frecuencia
Sus contraseñas cumplen con las políticas de contraseña		La totalidad de los encuestados confirman que cumplen con las políticas de contraseñas

3.6.1.2 Entrevista aplicada a los administradores de las empresas comerciales de El Carmen

N.º	PREGUNTAS	RESPUESTAS	CONCLUSIÓN
1	La empresa cuenta con políticas de seguridad de la información	Sí misma que está en constante mantenimiento	Se observó que si cuentan con políticas de seguridad de la información
2	La empresa ha socializado con sus empleados las políticas de seguridad de la información	Sí, se realizan capacitaciones virtuales sobre el uso y seguridad de este	Se puede ver que si realizan la socialización de las políticas
3	¿Por qué medios ha realizado la socialización?	Vía ZOOM, de manera virtual	Un medio que abarca a que todos los empleados para la socialización de las políticas
4	La empresa cuenta con un control sobre el acceso físico a las copias de seguridad	Si	Se puede ver que si cuentan con un control de acceso físico a las copias de seguridad
5	¿Los empleados tienen la formación que necesitan para prevenir errores de seguridad	Si	Los empleados si tienen la formación que necesitan para prevenir errores de seguridad

	informática?		
6	La empresa invierte en ciberseguridad	Si	Se observó que la empresa invierte en ciberseguridad
7	Los empleados hacen un uso adecuado de las contraseñas y datos personales	Si, se siguen las instrucciones según nos indican	Hacen el adecuado uso de las contraseñas y siguen las instrucciones indicadas
8	La empresa cuenta con tecnología para el respaldo de la información	Si	Se observó que la empresa cuenta con respaldo de la información
9	La empresa cuenta con controladores de seguridad para todos los usuarios empresariales	Si	Se puede ver que la empresa si cuenta con controladores de seguridad
10	La empresa cuenta con un plan de prevención de riesgos informáticos	Si	La empresa si cuenta con un plan de prevención de riesgos informáticos
11	Ha tenido usted algún incidente de seguridad de la información	Si de inicio cuando se implementó el sistema	La empresa si tuvo incidentes de seguridad de la información cuando se implementó el sistema
12	Sabe usted cuál es el proceso que se debe seguir con un incidente de seguridad	Si llamar al Sr. Encargado en el desarrollo del sistema	Se observó que saben cuál es proceso que hay que seguir con incidente de seguridad
13	En los últimos tres años los empleados han reportado problemas de seguridad de la información	No	La empresa no ha reportado problemas de seguridad en los últimos tres años
14	Conoce usted las responsabilidades que tiene sobre la información que tiene a su manejo	Si existen en el sistema diferentes áreas laborales que hacen uso de este y a las que se actualizan con capacitaciones.	Se puede ver que, si sabe sobre la responsabilidad que tiene, sobre la información que tiene a su manejo

3.6.2 Presentación y descripción de los resultados obtenidos

La pregunta 2 de la encuesta dirigida a los empleados de las empresas comerciales de El Carmen, determina que más de la mitad del personal conoce sobre las políticas de seguridad de la información. En base en la información obtenida, se puede concluir que las empresas tienen políticas de seguridad específicas.

En relación con la pregunta 4 de la encuesta, la mayoría del personal confirma que han socializado las políticas de seguridad de la información. Basándose en la información obtenida, se tiene que si se han socializado ciertas políticas de seguridad de la información.

En la pregunta 5 de la encuesta, la mayoría no sabe si las empresas han sido víctimas de ataques informáticos en los últimos tres años. En lo obtenido se afirma que las empresas comerciales no saben si han sido víctimas de ataques informáticos.

En la pregunta 6 la totalidad del personal no saben si la empresa ha sido víctima de ataques informáticos a la infraestructura. Donde los administradores también confirman que no saben si han sido víctimas de ataques informáticos en su infraestructura.

En relación a si las empresas cuentan con un sistema de gestión de seguridad, la mayoría del personal sabe que existe un SGSI según la pregunta 7 de la encuesta a los empleados de estas.

Basándose en la pregunta 9 de la encuesta, se puede afirmar que más de la mitad del personal sabe si cuenta con tecnologías de respaldo y recuperación de la información.

3.6.3 Informe final del análisis de los datos

Considerando los resultados obtenidos en el numeral anterior, se puedo concluir que las causas del problema es el poco conocimiento del tema y muestra que las empresas comerciales que tienen poco presente en que consiste la seguridad de la información.

La mitad de las empresas comerciales de El Carmen no cuentan con un sistema de gestión de seguridad, ya que el desconocimiento de estas empresas es el mayor problema de pérdida de información de la empresa.

CAPÍTULO IV

4 MARCO PROPOSITIVO

4.1 Introducción

El presente capítulo contiene el análisis de la auditoría inicial en empresas comerciales de El Carmen utilizando la Norma ISO 27001, a las cuales se aplicó un análisis de la brecha GAP.

4.2 Descripción de la propuesta

Se aplicó la norma ISO 27001 y es un estándar desarrollado por ISO (Organización Internacional de Normalización) para ayudar a gestionar la seguridad de la información en las empresas, que es una revisión de la primera edición de esta norma publicada en 2005 y es una adaptación ISO de la norma británica BS 7799-2.

Por lo tanto, un análisis de brechas o análisis de defectos GAP incluye un análisis de la conformidad con los requisitos de ISO 27001 y sus controles. Entonces parece una auditoría inicial a través de la cual se puede ver que tan bien se implementa el estándar ISO 27001 en la organización.

4.3 Determinación de recursos

4.3.1 Humanos

Los recursos humanos que utilizará para la auditoría son los empleados, los administradores de las empresas y la auditora para llevar a cabo la auditoría.

4.3.2 Tecnológicos y Económico

Recurso	Descripción	Valor	Total
Equipo Informático	1 computadora Core i3-3220 de 6 GB de RAM de 148 GB de disco duro HHD para procesamiento de datos	$800	$800
Conexión a internet	8 horas de internet	$0.036	$0.288

Recurso	Descripción	Valor	Total
	para investigar sobre el tema		
Transporte	Para poder movilizarse a las empresas	$0.40	$70
Impresiones	Hojas para las encuestas, entrevista y tesis	$0.05	$10
		TOTAL	$880.28

Tabla 5 Tecnológicos y Económico

4.4 Etapas de acción para el desarrollo de la propuesta

4.4.1 Planificación

4.4.1.1 Programa de auditoría

Programa de auditoría Inicial para gestión de seguridad de la información en empresas comerciales de El Carmen		
Objetivos **1. Evaluar el nivel de cumplimiento de requisitos de seguridad de ISO 27001 en empresas comerciales de El Carmen** **2. Identificar nivel de madurez de seguridad de la información en empresas comerciales de El Carmen**		
Técnicas y procedimientos		
1. Revisar la norma ISO 27001 **2. Diseño de instrumentos según ISO 27001** **3. Entrevista a informantes en empresas para llenar instrumentos de auditoría**	Referencia a papel de trabajo	Fecha:
	4.4.1.2	05/09/2022
	4.4.1.3	12/09/2022
		12/09/2022
	4.4.2.1	17/10/2022

4. Tabulación de datos **5. Análisis de Resultados**	4.4.2.2	14/11/2022
6. Elaboración de Informe de auditoría	5.2	22/12/2022

Tabla 6 Programa de auditoría

4.4.1.2 Revisión de ISO 27001

¿Qué es un análisis de brechas GAP en ISO 27001?

El análisis GAP es un método para evaluar las brechas de rendimiento entre los sistemas de información o las aplicaciones de software de una empresa para determinar si se están satisfaciendo las necesidades comerciales y, de no ser así, qué pasos deben tomarse para garantizar una implementación exitosa. La brecha es el espacio entre "dónde estamos" (ahora) y "dónde queremos estar" (lo que necesitamos lograr). El análisis de brechas permite identificar lo que falta y los recursos que necesarios para lograr los objetivos.

Objetivos

- Establecer el punto de partida para implementar la norma y evaluar el esfuerzo necesario, así como tener una herramienta fiable para elaborar un plan de implementación de ISO 27001
- Mantener una herramienta de evaluación del grado de implantación de la norma durante el proceso de implantación y evaluar el grado de avance del proyecto

Descripción de la fase I

Se recomienda un modelo de madurez de evaluación de cumplimiento para el análisis de brechas de GAP. Los modelos de madurez más comunes, como NIST, CITI-ISEM, COBOT, SSE/CM y CERT/CSO, ofrecen modelos con 5-6 niveles de madurez o cumplimiento. Estos modelos de madurez se utilizan a menudo como herramientas de gestión de servicios de TI y para medir qué tan bien funcionan los procesos de gestión con respecto a los controles internos. Este modelo es ideal para crear un modelo de auditoría que permita medir su nivel actual de madurez frente a los requisitos de un estándar específico (en este caso, ISO27001). Por lo tanto, el análisis de brechas GAP revelará mejoras reales en los controles internos del SGSI. El nivel de madurez no es una meta, sino un medio para evaluar la adecuación del control interno con respecto a los objetivos del sistema de gestión.

Descripción de los Ítems

Ítem	Requisito	Descripción
4	La Organización y su Contexto	Este ítem permite identificar los objetivos del SGSI y determinar el alcance del SGSI identificando las cuestiones internas y externas relacionadas con la seguridad de información
5	Liderazgo	Es ítem permite identificar los objetivos establecidos de la seguridad de la información acorde con los negocios y se han definido las políticas de seguridad, los roles y responsabilidades
6	Planificación	El tratamiento de riesgos y oportunidades consideradas en las partes interesadas en la seguridad de la información y con la planificación, saber si se han establecido los objetivos de seguridad de la información
7	Soporte	Identificar los recursos necesarios para el SGSI, la competencia, la concienciación, la comunicación e información documentada requerida por la organización
8	Operación	Un control operacional de los procesos de seguridad de la información con el análisis de riesgos de la seguridad de la información y el tratamiento de riesgos de la seguridad de la información
9	Evaluación del desempeño	Permite establecer un monitoreo continuo de los aspectos claves de seguridad de la información en las auditorías internas y el informe de revisión por la dirección
10	Mejora	Permite identificar los procedimientos documentados, no conformidades y acciones correctivas y la mejora continua del SGSI

Tabla 7 Descripción de Ítems Evaluados

4.4.1.3 Diseño de Instrumentos

En el instrumento de cumplimiento de requisitos se realizó un análisis de deficiencias mediante el modelo de niveles de madurez que se enumeraron desde el nivel 0 hasta el nivel 5.

REQUISITOS		PREGUNTA	CUMPLIMIENTO	OBSERVACIÓN
4 La Organización y su Contex	4.1 Entendiendo la Organ	1.- ¿Están identificados los objetivos del SGS Sistema de Gestión de la Seguridad de la		
		2.- ¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?		
		3.- ¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la Información?		
	4.2 Expectativas de las pa	1.- ¿Se han identificado las partes interesadas?		
		2.- ¿Existe un listado de requisitos sobre Seguridad de la Información de las partes		
		3.- ¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales?		
	4.3 Alcance del SGSI	1.- ¿Se ha determinado el alcance del SGS y se conserva información documentada?		
	4.4 SGS Sistema de Gesti	1.- ¿El sistema de Gestión de Seguridad de la información SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora?		
5 Liderazgo	5.1 Liderazgo y compromi	1.- ¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio?		
		2.- ¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?		
		3.- ¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?		
	5.2 Política de la Seguridad	1.- ¿Se ha definido una Política de la Seguridad de la Información?		
		2.- ¿Se ha establecido un marco que permita el establecimiento de objetivos?		
		3.- ¿Se ha comunicado la política de la Seguridad de la información a las partes interesadas y a toda la empresa?		
		4.- ¿Se mantiene información documentada de la política del SGSI y de sus objetivos?		
	5.3 Roles y Responsabilid	1.- ¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la		
		2.- ¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información?		

Ilustración 2 Instrumentos de cumplimientos de requisitos

Anexo A

Numeral	Clausula		Requisito	CUMPLE	OBSERVACIÓN
A5	Políticas de Seguridad de la Información	A5.1 Dirección de gestión para la seguridad de la información	1.- ¿La dirección ha publicado y aprobado las políticas sobre la Seguridad de la Información acordar con los requisitos del negocio?		
			2.- ¿Existe un proceso planificado y verificable de revisión de las políticas de Seguridad de la información?		
A6	Organización de la Seguridad de la Información	A6.1.	1.- ¿Se han asignado y definido las responsabilidades sobre la seguridad de la Información en las distintas tareas o actividades de la organización?		
			2.- ¿Se han segregado las diversas áreas de responsabilidad sobre la Seguridad de la Información para evitar usos o accesos indebidos?		
			3.- ¿Existe un proceso definido para contactar con las autoridades competentes ante incidentes relacionados con la Seguridad de la Información?		
			4.- ¿Existen medios y se han establecido contactos con grupos de interés y asociaciones relacionadas con la seguridad de la información para mantenerse actualizado en noticias e información sobre Seguridad?		
			5.- ¿Existen requisitos para afrontar cuestiones sobre la seguridad de la información en la gestión de proyectos de la organización?		
			1.- ¿Se consideran requisitos especiales para la Seguridad de la Información en la utilización		

Ilustración 3 Instrumentos de cumplimientos de controles

En el instrumento de cumplimiento de controles se realizó un análisis de los controles de la norma ISO 27001 con el SI o NO.

4.4.2 Ejecución

Los datos se tomaron en cuenta con los niveles de madurez que son los siguientes:

- No existencia (Nivel 0): no hay reconocimiento de la necesidad del control o requisito.
- Ad-hoc (Nivel 1): existe cierto reconocimiento de la necesidad de control interno o requisito. Se aplica para algún problema o tarea específica, no generalizable.
- Ejecutado (Nivel 2): los controles existen, pero no están documentados.
- Definido (Nivel 3): los controles están en su lugar y están documentados adecuadamente.
- Manipulable y medible (Nivel 4): Existe un control interno sobre la aplicación de controles y cumplimiento de requisito.
- Optimizado (5): Existe un control interno y continúo sobre la aplicación de controles y cumplimiento de requisitos. Se mide la eficacia de los controles estableciendo objetivos de mejora.

Fotografía de las entrevistas

Ilustración 4 Fotografía de entrevista

4.4.2.1 Tabulación de datos

Ilustración 5 Datos de la empresa Translatin S.A

En la empresa Translatin S.A cumple con la mayoría de los requisitos establecidos por la norma ISO 27001 teniendo un estado de madurez que CUMPLE.

REQUISITOS		PREGUNTA	CUMPLIMIENTO	PROMEDIO	Estado GAP	Brecha	ESTADO DE MADUREZ
4 La Organización y su Contex	4.1 Entendiendo la Organización y s	1.- ¿Están identificados los objetivos del SGS Sistema de Gestión de la Seguridad de la	2	1,625	33%	68%	CUMPLE PARCIALMENTE
		2.- ¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?	1				
		3.- ¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la Información?	1				
	4.2 Expectativas de las partes inter	1.- ¿Se han identificado las partes interesadas?	2				
		2.- ¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas?	2				
		3.- ¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales?	2				
	4.3 Alcance del SGSI	1.- ¿Se ha determinado el alcance del SGS y se conserva información documentada?	2				
	4.4 SGS Sistema de Gestión de la S	1.- ¿El sistema de Gestión de Seguridad de la información SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora?	1				
5 Liderazgo	5.1 Liderazgo y compromiso	1.- ¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio?	2	1,88888889	38%	62%	CUMPLE PARCIALMENTE
		2.- ¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?	2				
		3.- ¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?	2				
	5.2 Política de la Seguridad de la In	1.- ¿Se ha definido una Política de la Seguridad de la Información?	2				
		2.- ¿Se ha establecido un marco que permita el establecimiento de objetivos?	2				
		3.- ¿Se ha comunicado la política de la Seguridad de la información a las partes interesadas y a toda la empresa?	2				
		4.- ¿Se mantiene información documentada de la política del SGSI y de sus objetivos?	1				
	5.3 Roles y Responsabilidades	1.- ¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información?	2				
		2.- ¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información?	2				

Ilustración 6 Datos de la empresa Hermanos Loor

La empresa Hermanos Loor cumple parcialmente con los requisitos establecidos por la norma ISO 27001.

REQUISITOS		PREGUNTA	CUMPLIMIENTO	PROMEDIO	Estado GAP	Brecha	ESTADO DE MADUREZ
4 La Organización y su Contex	4.1 Entendiendo la Organiz	1.- ¿Están identificados los objetivos del SGS Sistema de Gestión de la Seguridad de la Información?	1	1,625	33%	68%	CUMPLE PARCIALMENTE
		2.- ¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?	1				
		3.- ¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la Información?	2				
	4.2 Expectativas de las pa	1.- ¿Se han identificado las partes interesadas?	2				
		2.- ¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas?	2				
		3.- ¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales?	1				
	4.3 Alcance del SGSI	1.- ¿Se ha determinado el alcance del SGS y se conserva información documentada?	2				
	4.4 SGS Sistema de Gesti	1.- ¿El sistema de Gestión de Seguridad de la información SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora?	2				
5 Liderazgo	5.1 Liderazgo y compromis	1.- ¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio?	2	1,8888889	38%	62%	CUMPLE PARCIALMENTE
		2.- ¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?	1				
		3.- ¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?	2				
	5.2 Política de la Seguridad	1.- ¿Se ha definido una Política de la Seguridad de la Información?	2				
		2.- ¿Se ha establecido un marco que permita el establecimiento de objetivos?	2				
		3.- ¿Se ha comunicado la política de la Seguridad de la información a las partes interesadas y a toda la empresa?	2				
		4.- ¿Se mantiene información documentada de la política del SGSI y de sus objetivos?	2				
	5.3 Roles y Responsabilid	1.- ¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información?	2				
		2.- ¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información?	2				

Ilustración 7 Datos de la empresa Alcívar

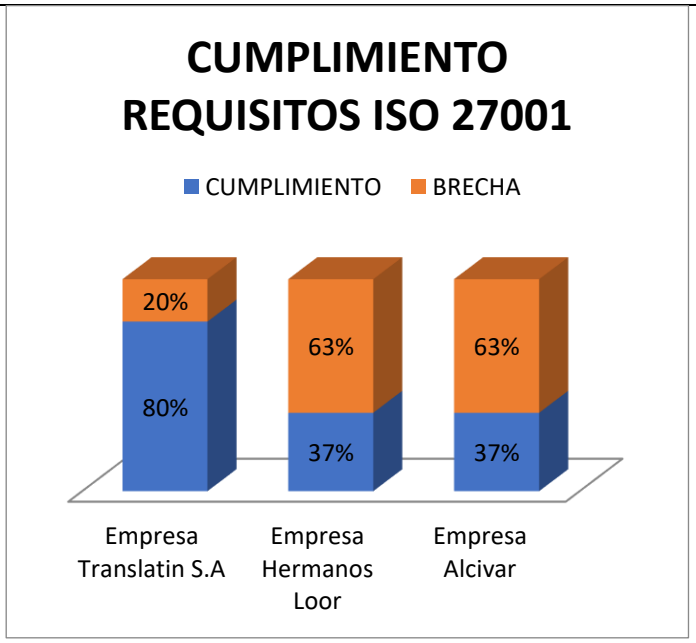
La empresa Alcívar cumple parcialmente con los requisitos establecidos por la norma ISO 27001.

4.4.2.2 Análisis de resultados

	EMPRESA TRANSLATIN S.A		EMPRESA HERMANOS LOOR		EMPRESA ALCIVAR	
REQUISITO DE ISO 27001	Cumple la Norma	BRECHA	Cumple la Norma	BRECHA	Cumple la Norma	BRECHA
4. Organización y Contexto	80%	20%	33%	68%	33%	68%
5. Liderazgo	80%	20%	38%	62%	38%	62%
6. Planificación	80%	20%	35%	65%	35%	65%
7. Soporte	80%	20%	40%	60%	40%	60%
8. Operación	80%	20%	37%	63%	35%	65%
9. Evaluación y desempeño	80%	20%	40%	60%	37%	63%
10. Mejora	80%	20%	40%	60%	40%	60%
PROMEDIO CUMPLIMIENTO	80%	20%	37%	63%	37%	63%

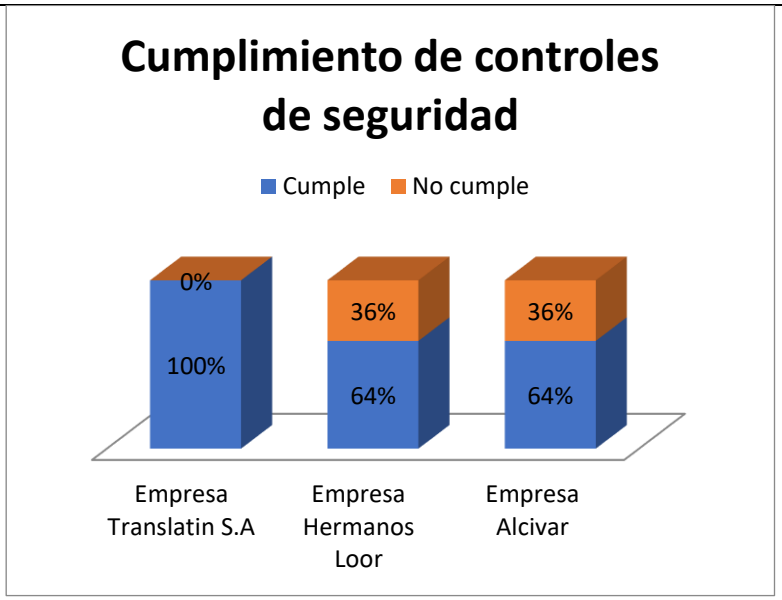
Ilustración 8 Análisis de resultados

Tabla de cumplimiento con porcentajes y gráficos



Interpretación: Se interpreta que la empresa Translatin S.A tiene un mayor cumplimiento de los requisitos de la ISO 27001 teniendo está un nivel de madurez alto y las otras dos empresas teniendo un nivel de brecha alto haciendo que estas no cumplan con todos los requisitos que determina la Norma ISO 27001.

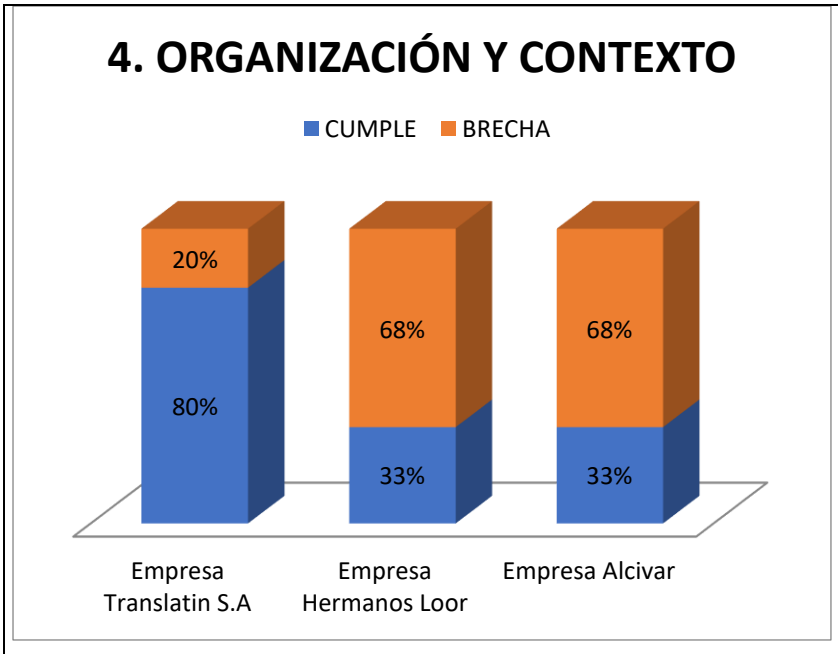
Tabla 8 Cumplimiento de requisitos ISO 27001



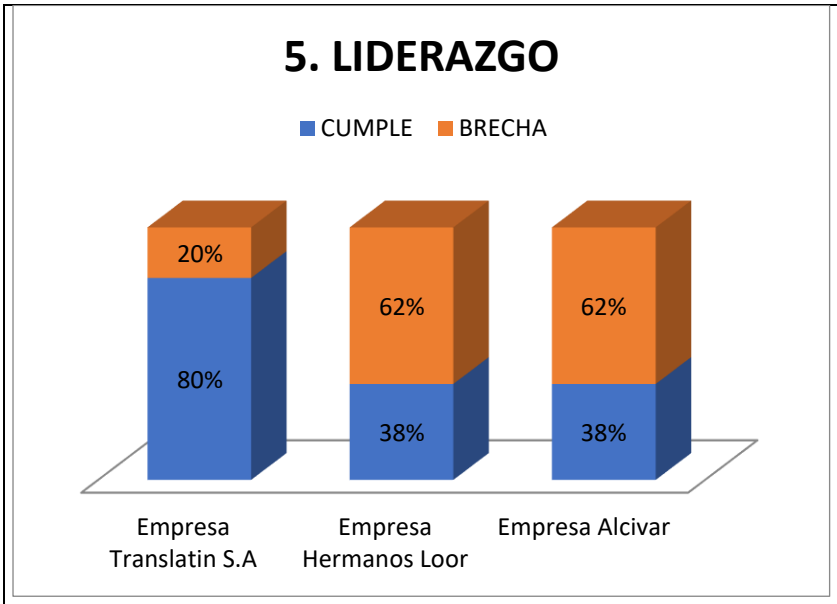
Interpretación: Las empresas Hermanos Loor y Alcívar tiene parcialmente con los controles de seguridad que establece la Norma ISO 27001, teniendo que menos cumplen con la manipulación de soporte y a su vez la empresa Translatin S.A es la que cumple con la mayoría de los requisitos.

Tabla 9 Cumplimiento de controles de seguridad

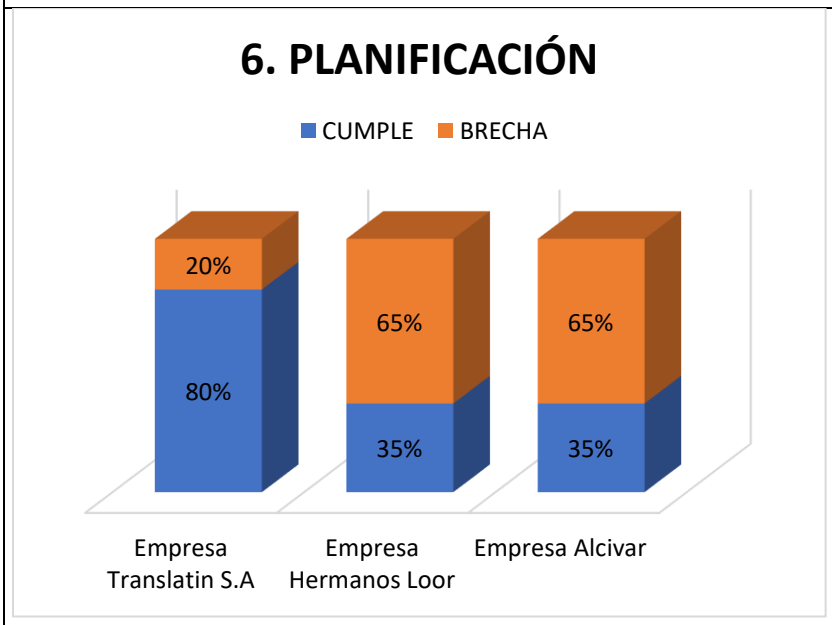
Análisis por cumplimiento de requisitos



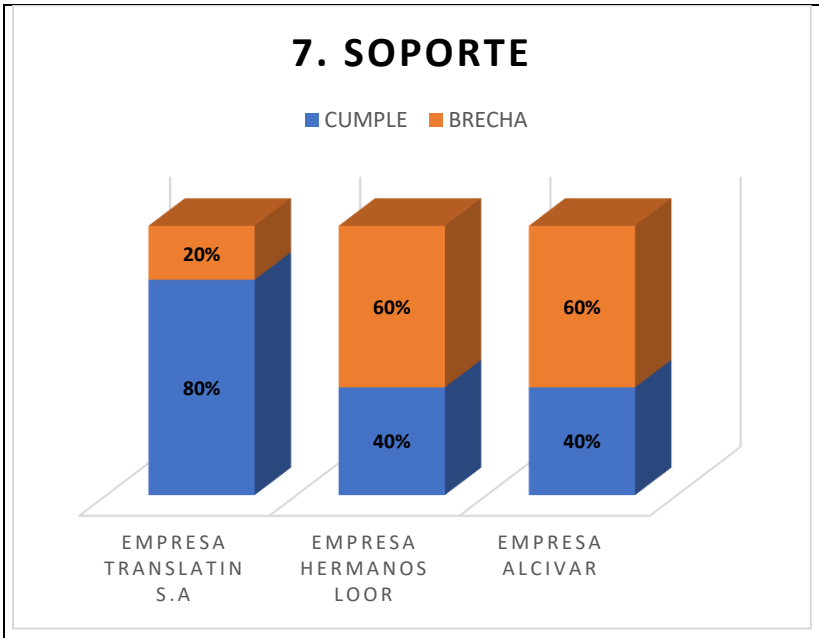
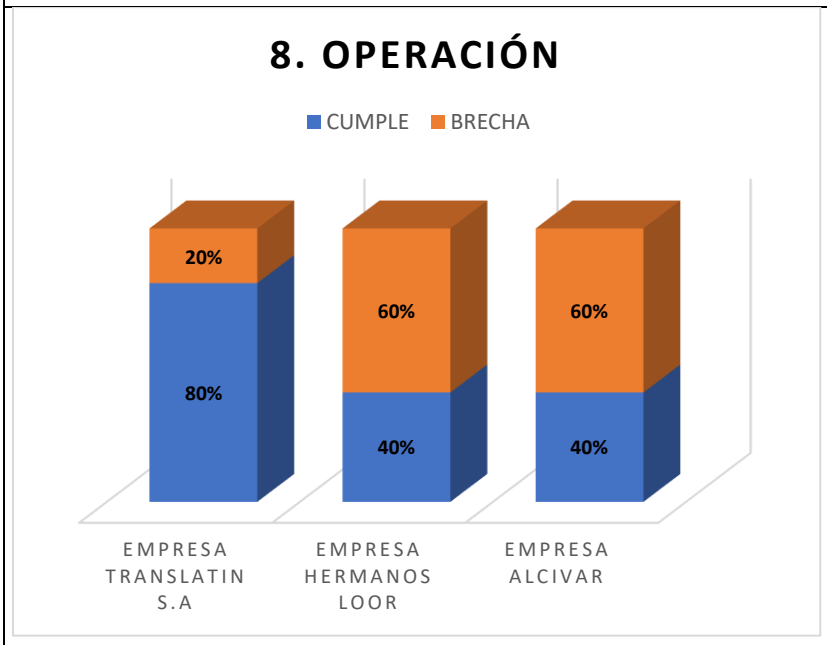
Interpretación: Entre las tres empresas hay una de ellas que destaca más con el cumplimiento de la organización, dos de ellas tiene una brecha alta haciendo que tengan muy poco cumplimiento de los requisitos.



Interpretación: La empresa Translatin S.A cumple con la mayoría de los requisitos de liderazgo y teniendo una brecha baja, las otras empresas tienen un porcentaje alto de brecha haciendo que casi no cumplan con el requisito de liderazgo.



Interpretación: En los requisitos de planificación la empresa Translatin S.A es la que cumple con la mayor parte de los requisitos, las empresas Hermanos Loor y Alcívar tienen un bajo cumplimiento

	**Interpretación:** Las empresas de los Hermanos Loor y Alcívar tienen un bajo cumplimiento en los requisitos de soporte que establece la ISO 27001 teniendo una brecha alta y a su vez la empresa Translatin S.A. cumple con la mayoría de los requisitos de soporte.
	**Interpretación: E**n el requisito operación, las empresas Hermanos Loor y Alcívar tienen un mayor porcentaje de brecha, a la vez la empresa Translatin S.A. cumple con la mayor parte de requisitos de operación.

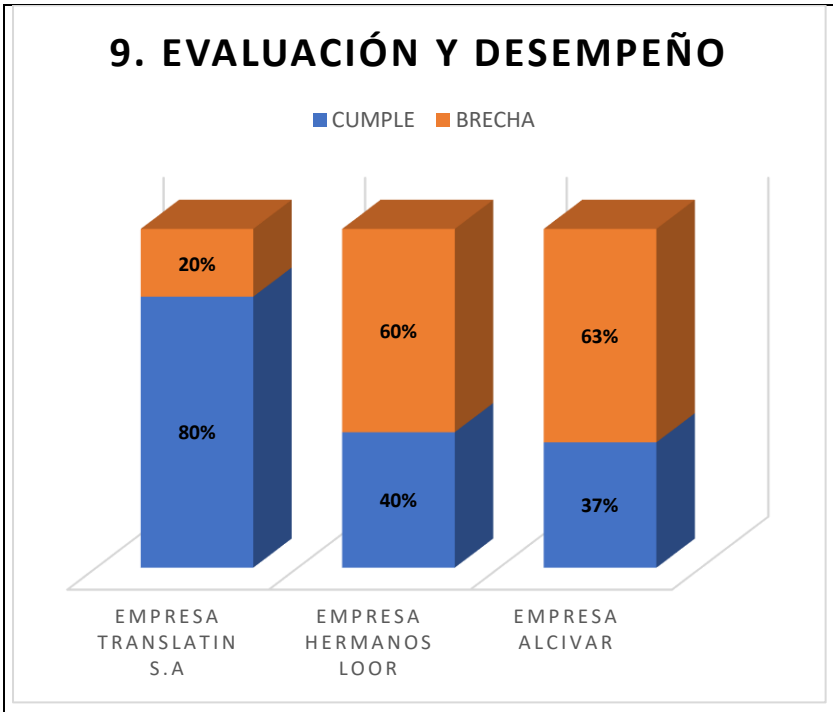
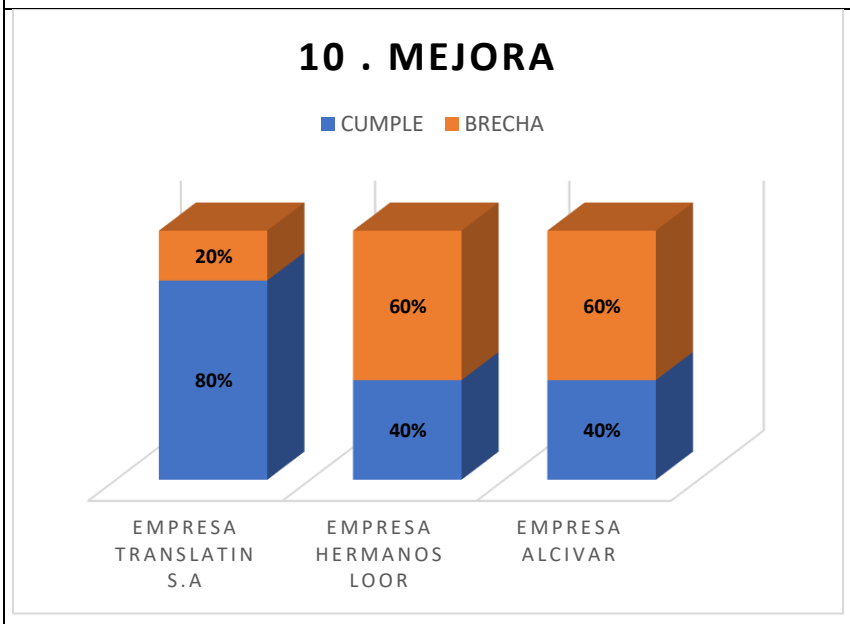
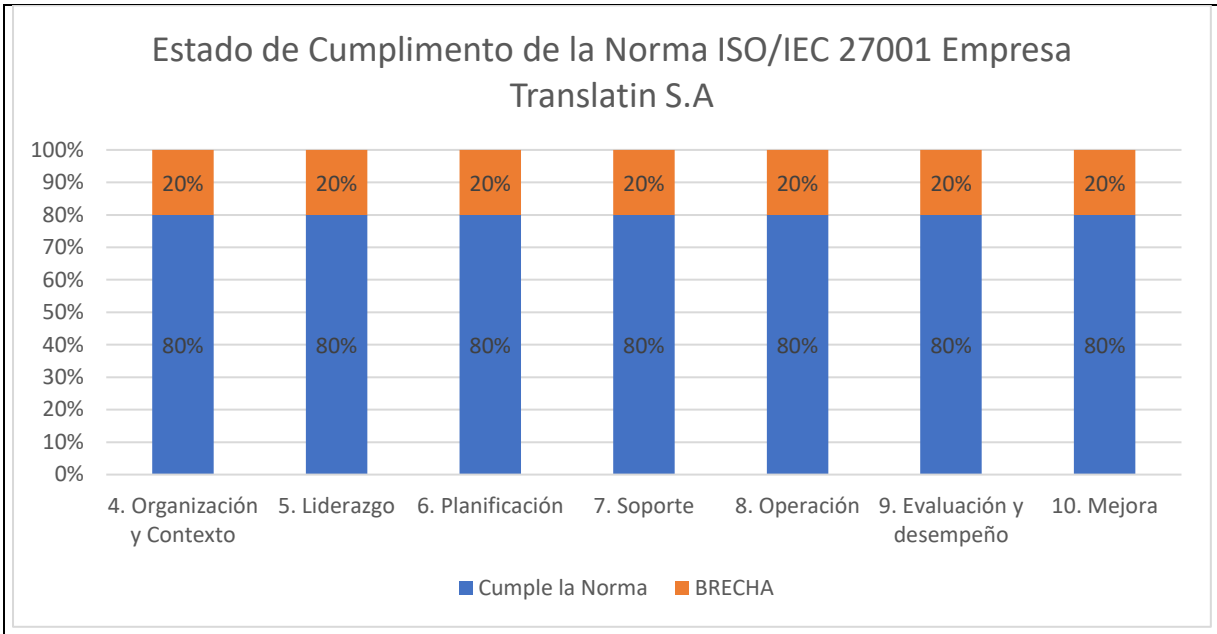
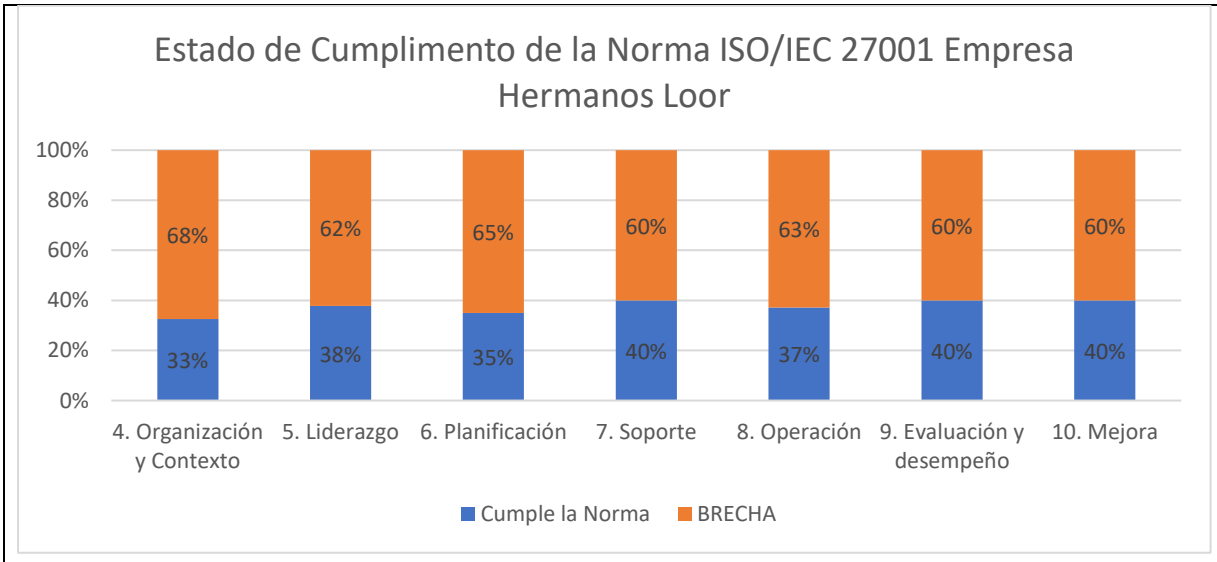
	**Interpretación:** La empresa Alcívar es la que menos cumple con los requisitos teniendo un mayor porcentaje de brecha siendo la parte de organización y contexto su menor cumplimiento, la empresa Translatin S.A. es la que mayor cumple con los requisitos.
	**Interpretación:** La empresa que más cumple con los requisitos de mejora es Translatin S.A. teniendo mayor nivel de madurez en el cumplimiento de los requisitos, a la vez las otras dos empresas cumplen parcialmente con el requisito de mejora.

Tabla 10 Análisis por cumplimiento de requisitos



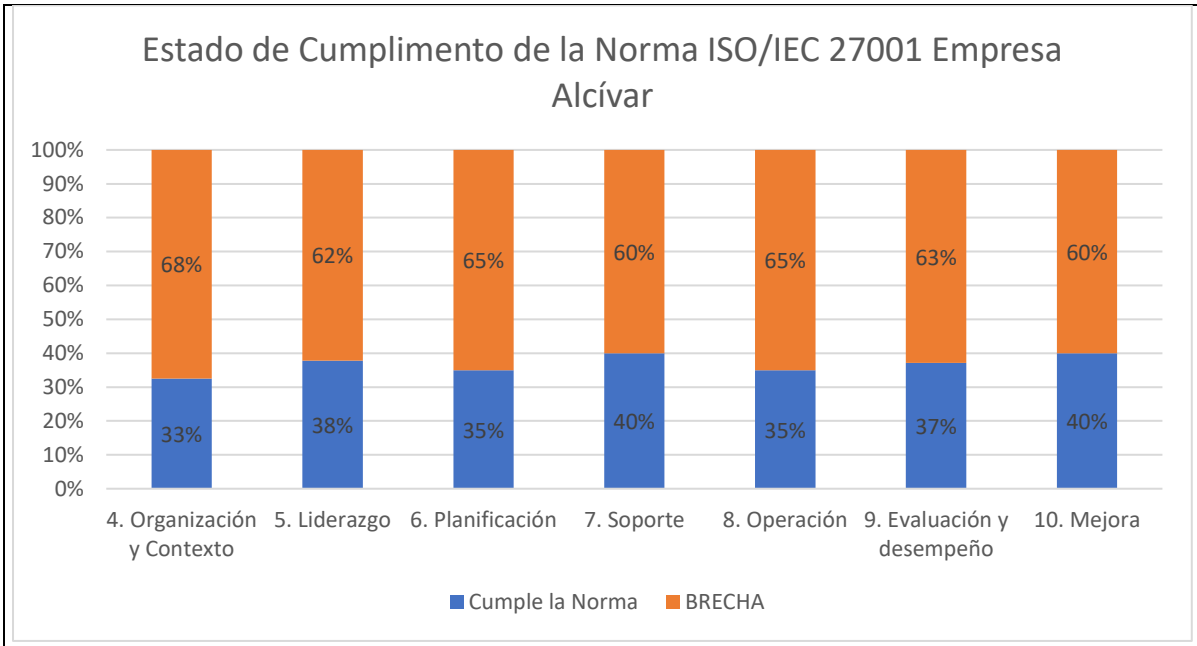
Interpretación: Translatin S.A. cumple la mayoría de los requisitos de la norma ISO 27001 haciendo que esta tenga un nivel de madurez alto, al tener una brecha baja hace que exista un control interno de la norma.

Tabla 11 Estado de cumplimiento de la Norma ISO 27001 Empresa Translatin S.A



Interpretación: La empresa Hermanos Loor cumple parcialmente con los requisitos de la norma ISO 27001, siendo la organización y contexto su menor cumplimiento de la norma teniendo un nivel madurez parcial y existe ciertos reconocimientos de los controles.

Tabla 12 Estado de cumplimiento de la Norma ISO 27001 Empresa Hermanos Loor



Interpretación: La empresa Alcívar cumple parcialmente con los requisitos que establece la norma ISO 27001, siendo la organización y contexto, planificación y operación sus menores cumplimientos y teniendo un nivel de madurez parcial.

Tabla 13 Estado de cumplimiento de la Norma ISO 27001 Empresa Alcívar

CAPÍTULO V

5 Evaluación de resultados

5.1 Introducción

La auditoría es una de las aplicaciones que juegan un papel importante en los parámetros y principios científicos basados en principios contables, comprobando registros, observando su corrección, pero no es el único propósito. Su importancia ha sido reconocida desde la antigüedad. Antiguamente, era la profesión de censor jurado de cuentas, pero sigue siendo la parte más aislada de su trabajo, aunque hoy en día se utiliza para otros servicios relacionados con la contabilidad y otros campos.

5.2 Informe detallado

El presente informe corresponde a la auditoría inicial de seguridad de la información realizada a empresas comerciales de El Carmen, que son la Empresa Translatin S.A., Empresa Hermanos Loor y Empresa Alcívar, mediante la verificación del cumplimiento de los requisitos de seguridad y del anexo A ISO 27001.

5.2.1 Dirigido a

A los administradores de las empresas comerciales las cuales son:

- Empresa Translatin S.A., administrador el Ingeniero Celó Giler
- Empresa Hermanos Loor, administrador el Señor Alfredo Loor
- Empresa Alcívar administrador el Señor Wilson Alcívar

5.2.2 Motivo

Cumplir con los requisitos para el trabajo de titulación aplicando el área de auditoría informática y seguridad de la información.

5.2.3 Objetivo

- Evaluar el nivel de cumplimiento de requisitos de ISO 27001 en empresas comerciales de El Carmen.
- Identificar nivel de madurez de seguridad de la información en empresas comerciales de El Carmen.

5.2.4 Alcance

Para el desarrollo del presente trabajo de investigación se aplicaron diferentes técnicas y procedimientos que permitieron obtener la información necesaria para respaldar el informe:

- Revisar la norma ISO 27001
- Diseño de instrumentos según la ISO 27001
- Entrevistas a informantes en empresas para llenar instrumentos de auditoría
- Tabulación de datos
- Análisis de resultados
- Elaboración de informe de auditoría

5.2.5 Personal relacionado

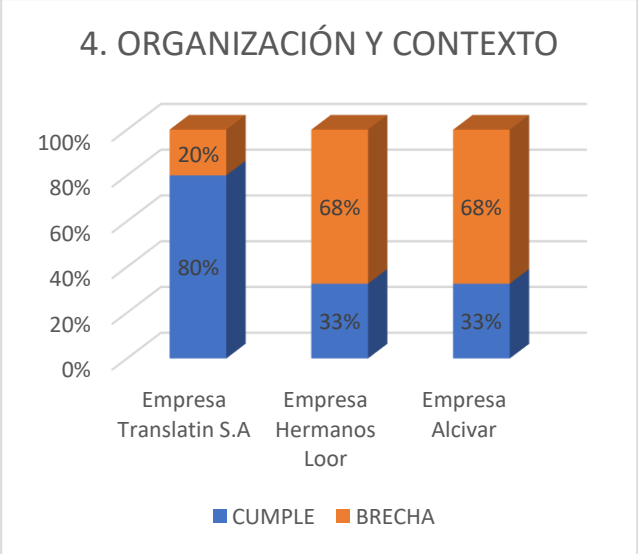
Empresa	Administrador	Área informática
Empresa Translatin S. A	Ingeniero Celó Giler	Secretarias
Empresa Hermanos Loor	Señor Alfredo Loor	Secretaria
Empresa Alcívar	Señor Wilson Alcívar	Secretaria

Tabla 14 Personal Relacionado

5.2.6 Hallazgos

Al realizar la auditoría se puede encontrar que los requisitos que mayor se cumplen con los de soporte y mejora, teniendo estos la mayor parte de cumplimiento.

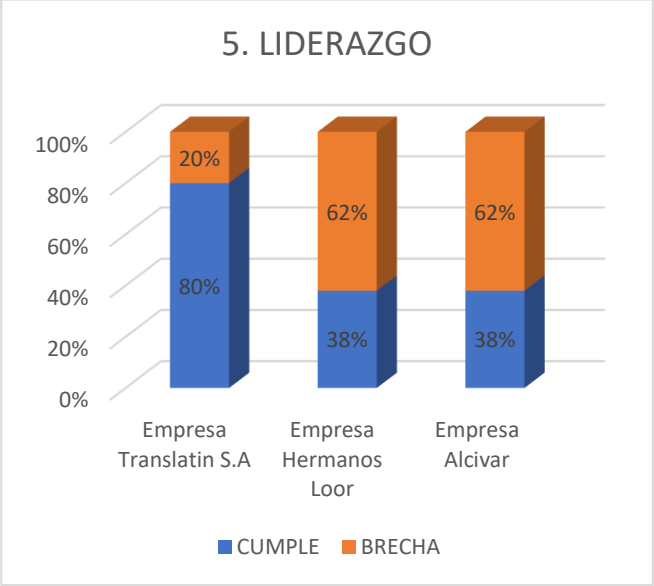
Requisitos



Interpretación: La empresa Translatin S.A. cumple con la mayoría de los requisitos de

organización y contexto, las empresas Alcívar y Hermanos Loor tiene un cumplimiento parcial, entre los requisitos que obtuvieron menor valoración de cumplimiento están:

- No existe un listado de requisitos de seguridad de la información de las partes interesadas
- No se cumple con la identificación de los objetivos del SGSI
- No se han identificado las cuestiones internas y externas relacionadas con la seguridad y su vez
- No existe un listado de requisitos de seguridad de la información referente a los reglamentos.
- No se han identificado las cuestiones internas y externas relacionadas con la seguridad,
- No se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad
- No cuentan con sistema de gestión de seguridad de la información establecido, implementado y se revisa la planificación considerada.

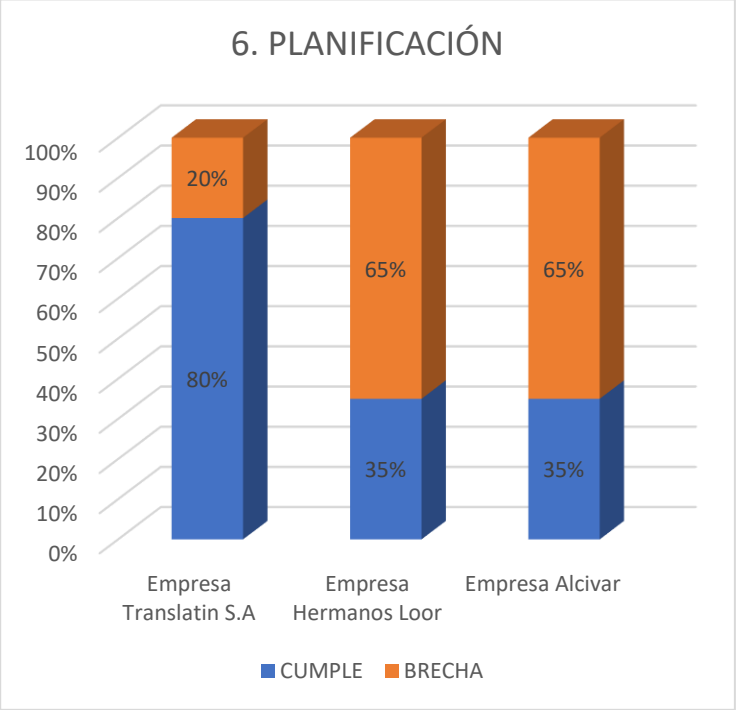


Interpretación: La empresa Translatin S.A. cumple con la mayoría de los requisitos de liderazgo, las empresas Alcívar y Hermanos Loor tiene un cumplimiento parcial, entre los requisitos que obtuvieron menor valoración de cumplimiento están:

- No se han asignado las responsabilidades y autoridades sobre la seguridad de la información.
- No cumple con la dirección, provee los recursos materiales y humanos necesarios para el

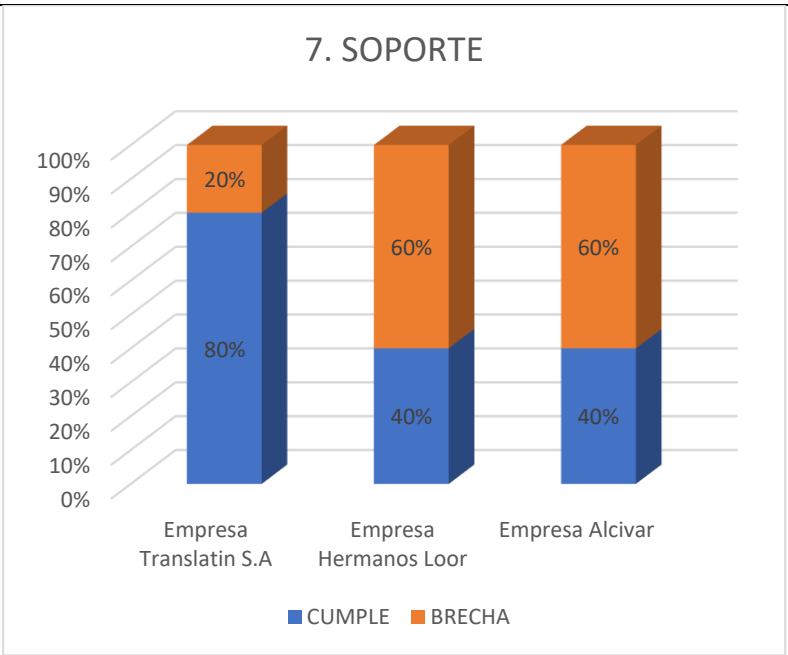
cumplimiento de los objetivos SGSI.

- No mantiene información documentada de la política del SGSI y de sus objetivos.



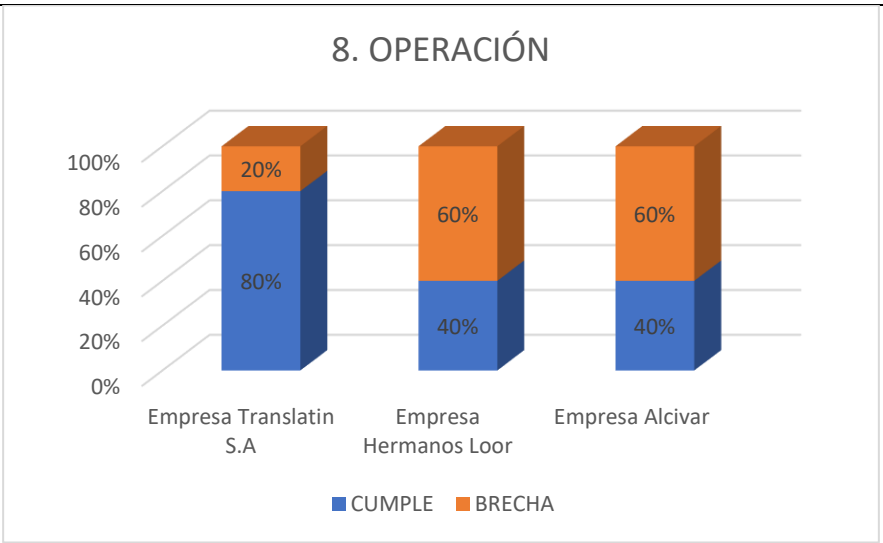
Interpretación: La empresa Translatin S.A. cumple con la mayoría de los requisitos de planificación, las empresas Alcívar y Hermanos Loor tiene un cumplimiento parcial, entre los requisitos que obtuvieron menor valoración de cumplimiento están:

- No se han definido un proceso de tratamiento de riesgo.
- No cumplen con los objetivos de la seguridad de la información planificada mediante, la asignación de responsabilidades - cronograma de ejecución temporal.
- No se han integrado los objetivos de seguridad de la información en los procesos de organización, teniendo en cuenta las funciones principales dentro la organización.
- No se han identificado y analizado los riesgos mediante un método de evaluación y aceptación, a su vez no cumple con los objetivos de la seguridad de la información planificados mediante, la asignación de responsabilidades - cronograma de ejecución temporal.



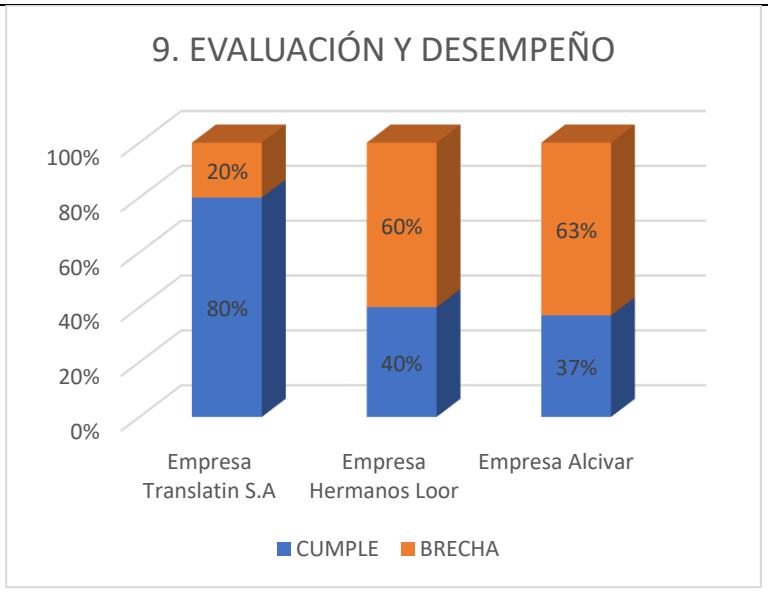
Interpretación: La empresa Translatin S.A. cumple con la mayoría de los requisitos de soporte, las empresas Alcívar y Hermanos Loor tiene un cumplimiento parcial, entre los requisitos que obtuvieron menor valoración de cumplimiento están:

- No existe un proceso para comunicar las deficiencias o malas prácticas en la seguridad de la información.
- No cumple con el control de documentos de origen externos.
- No se evalúa la competencia en materias de seguridad de la información para personas que afectan tareas que pueden afectar a la seguridad.
- No cumple con control de documentos de origen externo.



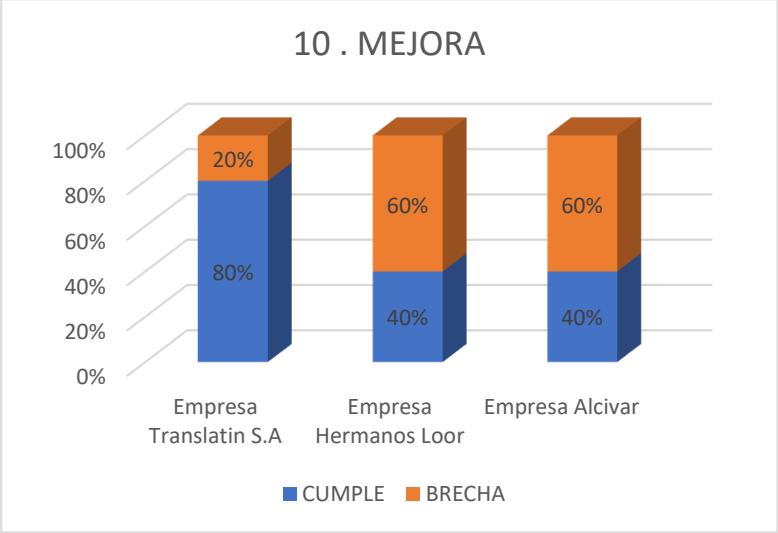
Interpretación: La empresa Translatin S.A. cumple con la mayoría de los requisitos de operación, las empresas Alcívar y Hermanos Loor tiene un cumplimiento parcial, entre los requisitos que obtuvieron menor valoración de cumplimiento están:

- No se han implementado un plan de tratamiento de riegos donde – los propietarios de riesgos están informados y han aprobado el plan – se documentan los resultados.
- No existe un proceso para evaluar los riesgos en la seguridad de la información antes de realizar cambios en sistema de gestión o procesos de seguridad.
- No se documenta el nivel de aplicación de todos los controles aplicar.
- No se establecen medidas y planes para mitigar los riesgos en la seguridad de la información ante cambios realizados.



Interpretación: La empresa Translatin S.A. cumple con la mayoría de los requisitos de evaluación y desempeño, las empresas Alcívar y Hermanos Loor tiene un cumplimiento parcial, entre los requisitos que obtuvieron menor valoración de cumplimiento están:

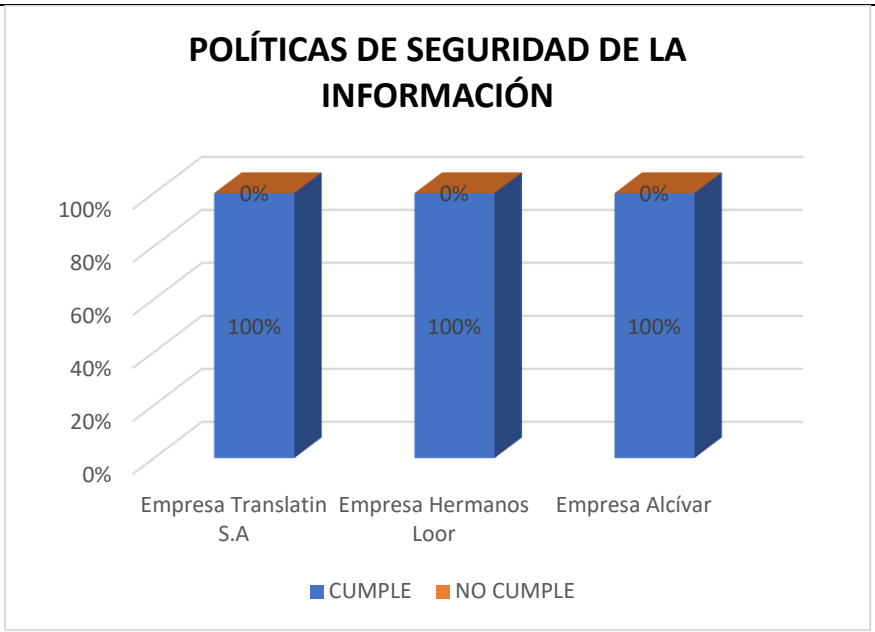
- No existe una programación para los informes de la dirección y registrar las no conformidades y su tratamiento.
- No se han establecido una programación de auditorías internas y asignado responsable.
- No se han considerado acciones correctivas y propuestas de cambio en los informes de auditoría.



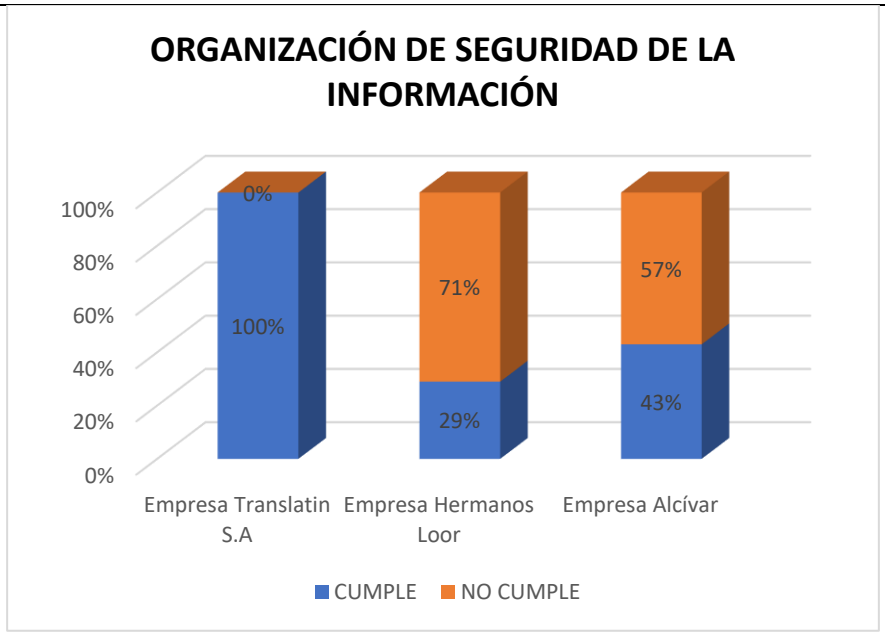
Interpretación: La empresa Translatin S.A. cumple con la mayoría de los requisitos de mejora, las empresas Alcívar y Hermanos Loor tiene un cumplimiento parcial, entre los requisitos que obtuvieron menor valoración de cumplimiento están:

- No cumple con el procesamiento documentado para identificar y registrar las no conformidades y su tratamiento.
- No existe un procedimiento documentado para identificar y registrar las no conformidades y su tratamiento.
- No cumplen dentro de las acciones correctivas, existe una diferenciación entre las acciones correctivas sobre la no conformidad y sobre las causas de estas.

CONTROLES



Interpretación: Las empresas Translatin S.A., Hermanos Loor y Alcívar cumplen con la totalidad de controles de seguridad de las políticas de seguridad de la información.

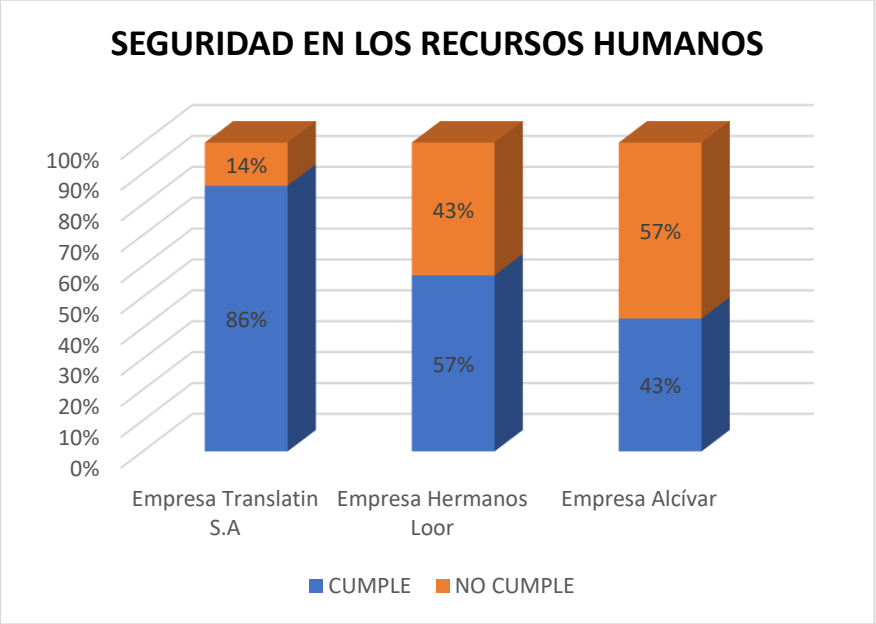


Interpretación: La empresa Translatin S.A. cumple con la totalidad de los controles de la organización de seguridad de la información, las empresas Hermanos Loor y Alcívar no cumplen con todos los controles, entre los que obtuvieron menor valoración están:

- No se han asignado y definido las responsabilidades sobre la seguridad de la información

en las distintas tareas o actividades de la organización.

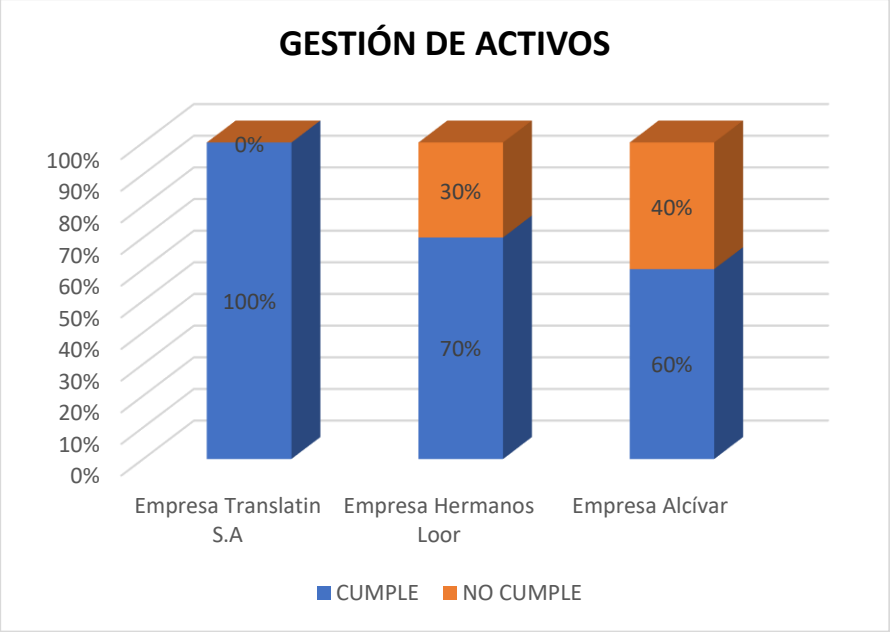
- No se han agregado las diversas áreas de responsabilidad sobre la seguridad de la información para evitar uso o accesos indebidos.
- No existe un proceso definido para contactar con las autoridades competentes ante incidentes relacionados con seguridad de la información.
- No existen requisitos para afrontar cuestiones sobre la seguridad de la información en la gestión de proyectos de la organización.
- No se consideran requisitos especiales para la seguridad de la información en la utilización de dispositivos móviles.



Interpretación: La empresa Translatin S.A. cumple con la mayoría de los controles de seguridad en los recursos, las empresas Hermanos Loor y Alcívar no cumplen con todos los controles, entre los que obtuvieron menor valoración están:

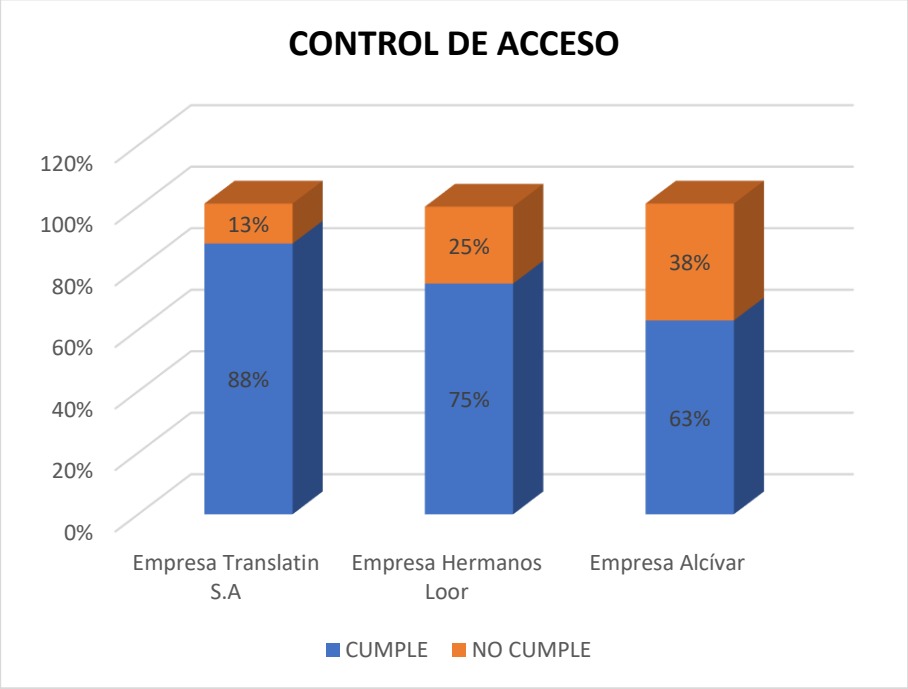
- No se cumple con las responsabilidades sobre la seguridad de la información, es exigida de forma activa a empleados y contratistas.
- No existen procesos de información, formación y sensibilidades sobre las responsabilidades sobre seguridad de la información.
- No existe un plan disciplinario donde se comunica a los empleados y contratistas las consecuencias de los incumplimientos sobre las políticas de seguridad.
- No se definen responsabilidades sobre la seguridad de la información que se extiendan

más allá de la finalización de un contrato, como por ejemplo cuestiones relativas a la confidencialidad de la información.



Interpretación: La empresa Translatin S.A. cumple con la totalidad de los controles de la gestión de activos, las empresas Hermanos Loor y Alcívar no cumplen con todos los controles, entre los que obtuvieron menor valoración están:

- No existen controles establecidos para aplicar a soportes extraíbles.
- No existen procedimientos establecidos para la eliminación de soporte.
- No existen procedimientos para el traslado de soportes de información para proteger su seguridad.
- No cumple con los activos de información fácilmente identificable en cuanto a su grado de confidencialidad o su nivel de clasificación.
- No existe procedimientos para el traslado de soportes de información para proteger su seguridad – control de salidas – cifrados, etc.



Interpretación: La empresa Translatin S.A. cumple con la mayoría de los controles de acceso, las empresas Hermanos Loor y Alcívar no cumplen con todos los controles, entre los que obtuvieron menor valoración están:

- No existe un proceso definido para la revocación de permisos cuando se finalice una actividad, puesto de trabajo o cese de contratos.
- No existen procesos formales para asignación de perfiles de acceso.
- No se ha establecido una política específica para el manejo de información clasificada cono secreto en cuanto a: Autenticación – Compromisos.
- No se establecen accesos limitados a los recursos y necesidades de la red según perfiles determinados
- No existen procesos formales para asignación de perfiles de acceso.
- No existe un proceso definido para la revocación de permisos cundo se finalice una actividad, puesto de trabajo o cese de contratos.

5.2.7 Opinión

Él cumplimiento de los requisitos de seguridad de la ISO 27001 en empresas comerciales de El Carmen es llevado a cabo por la empresa Translatin S.A., la cual cuenta con un alto nivel de

cumplimiento. Por otro lado, las empresas Hermanos Loor y Alcívar presentan un bajo nivel de cumplimiento.

Empresa	% de cumplimiento Requisitos de seguridad	% de cumplimiento controles anexo
Empresa Translatin S. A	80% (ALTO)	100%(ALTO)
Empresa Hermanos Loor	37%(BAJO)	64%(MEDIO)
Empresa Alcívar	37%(BAJO)	64%(MEDIO)

Tabla 15 Porcentaje de cumplimiento de requisitos de seguridad por empresa

El Nivel de madurez en gestión de seguridad de las empresas evaluadas es el siguiente: La empresa Translatin S.A. tiene un nivel de madurez alto, mientras que las empresas Hermanos Loor y Alcívar tienen un nivel de madurez medio.

Nivel de madurez en gestión de seguridad

Empresa	Nivel de madurez
Empresa Translatin S. A.	Alto
Empresa Hermanos Loor	Medio
Empresa Alcívar	Medio

Tabla 16 Nivel de madurez de seguridad

5.2.8 Conclusiones y recomendaciones

Se concluyó que las empresas comerciales de El Carmen siguen ciertos requisitos y controles de seguridad de la información que les otorga un nivel medio de madurez en la gestión de la seguridad.

Se recomienda un plan de seguridad que es el siguiente:

5.2.8.1 Plan de seguridad

1. **Alcance**

   Las políticas de seguridad informática están orientadas a toda la información almacenada, procesada y transmitida en medios electrónicos, estas políticas deben ser conocidas y cumplidas tanto a administradores como por los empleados que utilizan información generada y hagan uso de los servicios tecnológicos de la empresa.

2. **Definiciones**

   Acceso físico: La posibilidad de acceder físicamente a un computador o dispositivos, manipularlo tanto interna como externa.

Acceso lógico: Ingresar al sistema operativo o aplicaciones de los equipos y operarlos, ya sea directamente, a través de la red de datos interna o de internet.

Aplicaciones o aplicativos: Son herramientas informáticas que permiten a los usuarios comunicarse, realizar trámites, entretenerse, orientarse, aprender, trabajar, informarse y realizar una serie de tareas de manera práctica desde distintos tipos de terminales como computadoras, tabletas o celulares.

Cableado estructurado: Cableado de un edificio o una serie de edificios que permite interconectar equipos activos, de diferentes o igual tecnología, permitiendo la integración de los diferentes servicios que dependen del tendido de cable de datos, telefonía, control, entre otros.

Cifrado de datos: Proceso por el que una información legible se transforma mediante un algoritmo (llamado cifra) en información ilegible, llamada criptograma o secreto.

Configuración lógica: Conjunto de datos que determina el valor de algunas variables de un programa o de un sistema operativo, elegir entre distintas opciones con el fin de obtener un programa o sistema informático personalizado o para poder ejecutar dicho programa correctamente.

Copia de respaldo o Backus: Operación que consiste en duplicar y asegurar datos e información contenida en un sistema informático. Es una copia de seguridad.

Contenido: Todos los tipos de información o datos que se divulgan a través de los diferentes servicios informáticos, entre los que se encuentran: textos, imágenes, video, diseños, software, animaciones, entre otros.

Contraseña: Clave criptográfica utilizada para la autenticación de usuarios y que se utiliza para acceder a los recursos informáticos.

Cuenta de acceso: Colección de información que permite a un usuario identificarse en un sistema informático o servicio, mediante un usuario y una contraseña, para que pueda obtener seguridad, acceso al sistema, administración, entre otros.

Dispositivos/ Periféricos: Aparatos auxiliares e independiente conectados al computador o la red.

Dominio: Es un conjunto de computadoras, conectadas en una red, que confían a uno de los equipos de dicha red la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en la red.

Información confidencial: Se trata de una propiedad de la información que pretende garantizar el acceso solo a personas autorizadas.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Plataformas web: Sistema que permite la ejecución de diversas aplicaciones bajo un mismo entorno, dando al usuario la posibilidad de acceder a ellas a través de internet.

Software antivirus: Son programas que buscan prevenir, detectar y eliminar virus informáticos.

3. Políticas orientadas a los usuarios internos

3.1 Gestión de la Información

3.1.1 Todo funcionario de la empresa que esté relacionado con el uso de equipos de cómputo, software de gestión, aplicativos, plataformas web y servicios informáticos, debe aceptar las condiciones de confidencialidad y de uso adecuado de los recursos informáticos, así como cumplir y respetar las directrices impartidas en el Manual de políticas de Seguridad Informática.

3.1.2 Los empleados que culminen su vínculo contractual con la Empresa deberán hacer: entrega formal de los equipos asignados, así como de la totalidad de la información electrónica que se produjo y se recibió con motivo de sus funciones y actividades, como requisito para expendición de paz y salvo o liquidación de contrato

3.1.3 Toda la información recibida y producida en el ejercicio de las funciones y cumplimiento de obligaciones contractuales, que se encuentre almacenada en los equipos de cómputo, pertenece a la Empresa, por lo tanto, no se hará divulgación ni extracción de esta sin previa autorización de las directivas de la Entidad.

3.1.4 No se realizará por parte de los empleados copia no autorizada de información de la Empresa.

3.1.5 Ningún funcionario o contratista podrá visualizar, copiar, alterar o destruir información que no se encuentre bajo su custodia.

3.1.6 Todo contrato o convenio relacionado con servicios de tecnología o acceso a información, debe contener una obligación o cláusula donde el contratista o tercero acepte el conocimiento de las políticas de seguridad y

acuerde mantener confidencialidad de la información, el cual se hará extensivo a todos sus colaboradores.

3.2 Hardware y Software:

3.2.1 La instalación y desinstalación de software, la configuración lógica, conexión a red, instalación y desinstalación de dispositivos, la manipulación interna y reubicación de equipos de cómputo y periféricos, será realizada únicamente por personal del área de TIC'S.

3.2.2 El espacio en disco duro de los equipos de cómputo pertenecientes a la Empresa será ocupado únicamente con información institucional, no se hará uso de ellos para almacenar información de tipo personal (documentos, imágenes, música, video).

3.2.3 Ningún empleado podrá acceder a equipos de cómputo diferentes al suyo sin el consentimiento explícito de la persona responsable.

3.2.4 Ningún empleado podrá interceptar datos informáticos en su origen, destino o en el interior de un sistema informático protegido o no con una medida de seguridad, sin autorización.

3.2.5 Ningún empleado podrá impedir u obstaculizar el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos del área de TIC'S en aplicación de las políticas o medidas de seguridad.

3.2.6 No se permite el uso de la plataforma y servicios informáticos (equipos de cómputo, periféricos, dispositivos, internet, red de datos, correo electrónico institucional) de la Empresa para actividades que no estén relacionadas con lo laboral.

3.2.7 Los empleados serán responsables de contar con conocimientos actualizados en informática básica y el uso de herramientas ofimáticas.

3.3 Correo electrónico:

3.3.1 El correo electrónico institucional es exclusivo para el envío y recepción de mensajes de datos relacionados con las actividades de la Empresa, no se hará uso de él para fines personales como registros en redes sociales, registros en sitios web con actividades particulares o comerciales o en

general entablar comunicaciones en asuntos no relacionados con las funciones y actividades de la Entidad.

3.3.2 La información transmitida a través de las cuentas de correo electrónico institucional no se considera correspondencia privada, ya que estas tienen como fin primordial la transmisión de información relacionada con las actividades ordinarias de la empresa.

3.3.3 Es prohibido utilizar el correo electrónico institucional para divulgar información confidencial, reenviar mensajes que falten al respecto o atenten contra la dignidad e intimidad de las personas, difundir propaganda política, comercial, religiosa, racista, sexista o similares, reenviar contenido y anexos que atenten contra la propiedad intelectual.

3.3.4 Es responsabilidad del empleado depurar su cuenta de correo periódicamente, en todo caso se debe hacer copia de seguridad completa de los correos tanto recibidos como enviados.

3.4 Internet:

3.4.1 No se harán descargas de archivos por internet que no provengan de páginas conocidas o relacionadas con las funciones y actividades en la Empresa.

3.4.2 El servicio de internet de la Empresa no podrá ser usado para fines diferentes a los requeridos en el desarrollo de las actividades propias de la Entidad. Esta restricción incluye el acceso a páginas con contenido pornográfico, terrorismo, juegos en línea, redes sociales y demás cuyo contenido no sea obligatorio para desarrollar las labores encomendadas al cargo.

3.4.3 No es permitido el uso de internet para las actividades ilegibles o que atenten contra la ética y el buen nombre de la Empresa.

3.4.4 La empresa se reserva el derecho a registrar los accesos y monitorear el contenido al que el usuario puede acceder a través de internet desde los recursos y servicios de internet de la Entidad.

3.5 Cuentas de Acceso:

3.5.1 Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles, cada empleado es responsable por las cuentas de acceso asignadas y las transacciones que con ella se realicen.

3.5.2 Las contraseñas de acceso deben poseer un mínimo de ocho (8) caracteres y debe contener al menos una letra mayúscula, una letra minúscula, un número y un carácter especial (+-*/@#$%&). No debe contener vocales tildadas, ni eñes, ni espacios.

3.5.3 La contraseña inicial de acceso a la red que le sea asignada debe ser cambiada la primera vez que acceda al sistema, además, debe ser cambiada mínima cada 4 meses, o cuando se considere necesario debido a alguna vulnerabilidad en criterios de seguridad.

3.5.4 Solamente puede solicitar cambio o restablecimiento de contraseñas desde el servidor, el empleado al cual pertenece dicho usuario, o el jefe inmediato mediante solicitud motiva al correo electrónico del área de TIC'S.

3.5.5 Todo empleado que se retire de la Entidad de forma definitiva o temporal (superior a 1 semana), deberá hacer entrega formal a quien lo reemplace en sus funciones o a su superior inmediato de las claves de acceso de las cuentas asignadas, con el fin de garantizar la continuidad de las operaciones a su cargo.

3.6 Seguridad física:

3.6.1 Es responsabilidad de los empleados velar por la conservación física de los equipos a ellos asignados, haciendo uso adecuado de ellos y en el caso de los equipos portátiles, estos podrán ser retirados de las instalaciones de la Entidad única y exclusivamente por el usuario a cargo y estrictamente para ejercer labores que estén relacionadas con la Empresa.

3.6.2 Los empleados deberán reportar de forma inmediata a los directivos la detección de riesgos reales o potenciales sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes, peligro de incendio, peligro de robo, entre otros. Así como reportar

algún problema o violación de la seguridad de la información, del cual fueren testigos.

3.6.3 Mientras se operan equipos de cómputo, no se deberá consumir alimentos ni ingerir bebidas.

3.6.4 Se debe evitar colocar objetos encima de los equipos de cómputo que obstruyan las salidas de ventilación del monitor o de la CPU.

3.7 Personal de sistemas:

3.7.1 El control de los equipos tecnológicos deberá estar bajo la responsabilidad del área de TIC'S, así como la asignación de usuarios y la ubicación física.

3.7.2 En el área de TIC'S se deberá llevar el control total y sistematizado de los recursos tanto de hardware como de software.

3.7.3 El área de TIC'S será la encargada de velar por qué se cumpla con la normatividad vigente sobre propiedad intelectual de soporte lógico (software).

3.7.4 Las licencias de uso de software estarán bajo custodia del área de TIC'S. Así mismo, los manuales y los medios de almacenamiento (CD, cintas magnéticas u otros medios) que acompañen a las versiones originales de software.

3.7.5 El área de TIC'S es la única dependencia autorizada para realizar copia de seguridad del software original, aplicando los respectivos controles. Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.

3.7.6 Todas las publicaciones que se realicen en el sitio WEB de la entidad deberán atender el cumplimiento de las normas en materia de propiedad intelectual.

3.7.7 El acceso a los sistemas de información y red de datos sea controlado por medio de nombres de usuario personales y contraseñas. El área de TIC'S será la encargada de crear y asignar las cuentas de acceso y sus permisos a dominio de red, sistemas de información y correo electrónico, previo cumplimiento del procedimiento establecido para tal fin.

3.7.8 Se deben asignar usuarios unificados para todos y cada uno de los sistemas, servicios y aplicaciones, garantizando la estandarización por cada usuario, es decir, que cada usuario debe tener el mismo nombre de usuario para todos los sistemas y aplicaciones de la Entidad La estandarización de los nombres de usuario estará compuesta de la siguiente forma (Primera letra del primer nombre + punto () + primer apellido, en caso de existir duplicidad, Primeras dos letras del primer nombre + punto () + primer apellido).

3.7.9 Las cuentas de acceso a sistemas, servicios y aplicaciones no podrán ser eliminadas al retiro de los funcionarios o contratistas, debe aplicarse la inactivación del usuario.

3.7.10 Se realizará Backup a la información institucional y bases de datos, conforme a lo establecido en la política de Backup y cronograma, así como en los casos extraordinarios desvinculación de funcionario o contratista, envío de equipo para garantía, mantenimiento correctivo de equipo.

3.7.11 Las contraseñas de los usuarios administradores de las plataformas tecnológicas y sistemas de información de la Entidad deberán ser salvaguardadas por el área de TIC'S en un archivo protegido a través de técnicas de cifrado de datos u otro mecanismo seguro.

4. Políticas de administración de Backup

4.1 Objetivo:

Establecer las directrices para la ejecución y control de las copias de seguridad de la información digital de la Empresa.

4.2 Alcance:

Estas directrices son aplicadas a la información institucional, bases de datos y archivos de restauración de los equipos pertenecientes a la Empresa.

4.3 Clasificación de la Información:

Información Institucional:

Entiéndase como información institucional aquella relativa a las operaciones realizadas por cada una de las dependencias de la Empresa, su producción,

almacenamiento y gestión está a cargo de cada uno de los empleados. Información que se encuentra alojada en los equipos de cómputo.

Bases de Datos

Las bases de datos son el conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso, la Empresa cuenta con la base de datos del software de gestión de usuarios RED GERENCIADA.

Archivos de Restauración del Sistema:

Los archivos de restauración son la copia de las unidades necesarias para que se ejecute el Sistema Operativo, son la herramienta para recuperar el Sistema Operativo de un error grave o restaurar el equipo si la unidad de disco duro o el equipo dejan de funcionar.

4.4 Periodicidad del Backup

Tipo de información	Frecuencia de copia
Información de Usuarios	Diaria
Bases de datos	Diaria

Tabla 17 Periodicidad del Backup

4.5 Medios de almacenamiento

Las copias de seguridad son almacenadas en un ¡Cloud en la nube asegurado por un correo exclusivo para tal fin y copia en un Disco Duro Extraíble dispuesto exclusivamente para este fin. Este debe ser resguardado por el responsable del área de TIC'S.

4.6 Tipos de Backup

- Las copias de seguridad se realizarán bajo el método de Backup completo y Backup incremental.
- Backup completo se hace un respaldo completo de todos archivos del equipo. El Backup abarca el 100% de los datos.
- En una copia de seguridad incremental se copian todos los archivos modificados desde la última copia de seguridad completa.

CAPÍTULO VI

6 Conclusiones y recomendaciones

CONCLUSIONES

Existe bibliografía actualizada que permitió fundamentar los referentes bibliográficos que fueron de gran utilidad para la investigación de las variables independiente y dependiente, facilitando el desarrollo de la tesis.

Se determina que los representantes de las empresas comerciales de El Carmen participaron activamente en el estudio de los requisitos y controles de seguridad de la información y esto permitió obtener información importante para la investigación.

Para terminar, se comprueba que en las empresas comerciales existen ciertas normas, políticas y estados de seguridad de la información, el principal objetivo es de verificar si se cumplen las mismas. Se puede decir que en algunas de las empresas comerciales de El Carmen se cumplen con algunos de los requisitos y controles de la Norma ISO 27001 y en otras no se cumplen.

RECOMENDACIONES

Tras la finalización de la auditoría informática, se proponen que se implementen mejoras claras, que abarcan los niveles estratégicos, tácticos y operativo, con base en el apoyo de dirección general y el compromiso de todos los involucrados.

Se sugiere que las empresas en evaluación implementen sus políticas de seguridad de la información y las den a conocer a todos los involucrados para obtener resultados válidos, así como a la Universidad que realicen este tipo de investigaciones en otros tipos de empresas.

Establecer políticas y procedimientos adecuados relacionados con la seguridad de los activos, teniendo en cuenta que la información debe clasificarse de acuerdo con las necesidades de acceso. Los controles de información de autenticación garantizan que solo el personal autorizado pueda acceder a la información y utilizarla.

Este tipo de investigación se recomienda para los estudiantes de la Universidad en la carrera de Tecnologías de la Información.

BIBLIOGRAFÍA

Acosta Alvarado, N., & Carrillo Morán, F. (2018). *Repositorio Uleam.* Obtenido de https://repositorio.uleam.edu.ec/handle/123456789/2668

Acosta Molina, C. (2019). *El estado del arte sobre el internet de las cosas. Amenazas y vulnerabilidades de seguridad informática evidenciadas desde la domotica.* Escuela de Ciencias Básicas, Ingeniería, Tecnología e Ingeniería - ECBTI. Obtenido de https://repository.unad.edu.co/handle/10596/28446

Alan Neill, D., & Cortez Suárez, L. (2018). Procesos y fundamentos de la investigación científica. En D. Alan Neill, C. Quezada Abad, & J. Arce Rodríguez, *Procesos y fundamentos de la investigación científica* (pág. 68). Editorial UTMACH. Obtenido de http://repositorio.utmachala.edu.ec/bitstream/48000/14232/1/Cap.4-Investigaci%C3%B3n%20cuantitativa%20y%20cualitativa.pdf

Albarracín Zambrano, L., Marín Vilela, C., Lozada Calle, J., & Martínez Matute, J. (2021). Auditoría informática dentro de la empresa "Promaelec" de la ciudad de Quevedo, en tiempo de Covid-19. *Revista Universidad y Sociedad*, 345-354. Obtenido de http://scielo.sld.cu/pdf/rus/v13n5/2218-3620-rus-13-05-345.pdf

Arcentales-Fenández, D., & Caycedo-Casas, X. (2017). Auditoría informática: un enfoque efectivo. *Revista científica Dominio de las Ciencias*, 157-173. Obtenido de https://dialnet.unirioja.es/descarga/articulo/6102836.pdf

Árevalo Cordovilla, F., Ordoñez Sigcho, I., Peñaherrera Larenas, M., & Suárez Matamoros, V. (2020). Importancia de la seguridad de los sistemas de información frente el abuso, error. *Dominio de las Ciencias, 6*(2), 835-846. doi:https://dominiodelasciencias.com/index.php/es/article/view/1197

Aucapiña, T. V. (2012). *NORMA DE SEGURIDAD INFORMÁTICA ISO 27001 PARA MEJORAR LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN EN EL DEPARTAMENTO DE SISTEMAS DE LA COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCO LTDA.* Obtenido de https://repositorio.uta.edu.ec/bitstream/123456789/2361/1/Tesis_t715si.pdf

Aucapiña, T. V. (2012). *Repositorio UTA.* Obtenido de https://repositorio.uta.edu.ec/bitstream/123456789/2361/1/Tesis_t715si.pdf

Baca Urbina, G. (2016). *Introducción a la seguridad informática.* Grupo Editorial Patricia. Obtenido de https://elibro.net/es/ereader/uleam/40458

Basaldúa, L. D. (2005). *bib.* Obtenido de http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

Blanco Encinosa , L. (2008). *Auditoría y sistemas informáticos.* Editorial Félix Varela. Obtenido de https://elibro.net/es/ereader/uleam/71229

Cadme Ruiz, C., & Duque Pozo, D. (2012). *DSPACE UPS.* Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/2644/16/UPS-CT002441.pdf

Carbajal Suárez, Y. (2019). *Paradigma, revolución científica y métodos deductivo e inductivo.* Obtenido de http://ri.uaemex.mx/bitstream/handle/20.500.11799/108420/secme-22923_1.pdf?sequence=1

Casal, G. (10 de Febrero de 2022). *Auditool*. Obtenido de https://www.auditool.org/blog/auditoria-de-ti/8317-que-son-los-controles-de-seguridad-de-ti

Chicano Tejada, E. (2015). *Auditoría de seguridad informática (MF0487_3).* IC Editorial. Obtenido de https://elibro.net/es/ereader/uleam/44136

Costas Santos, J. (2015). *Seguridad informática.* RA-MA Editorial. Obtenido de https://elibro.net/es/ereader/uleam/62452

Costas Santos, J. (2015). *Seguridad Informática.* RA-MA. Obtenido de https://elibro.net/es/ereader/uleam/62452?page=16

Cueva, M. (2018). *SCRIBD.* Obtenido de https://es.scribd.com/document/380525985/Historia-Del-Sistema-de-Gestion-de-La-Seguridad

Davalos, S. (2017). *SlidePlayer.* Obtenido de https://slideplayer.es/slide/143212/

De Freitas, V. (2023). Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. *Scielo Venezuela*, *6*(1), 43-45. Obtenido de http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1690-75152009000100004&lng=es&tlng=es.

Escuela Europea de Excelencia. (20 de Octubre de 2016). *Escuela Europea de Excelencia*. Obtenido de https://acortar.link/NCrBJP

Espinosa Vanegas, D. (2018). *ANÁLISIS DE BRECHA, IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS DE LOS ACTIVOS DE INFORMACIÓN DEL PROCESO DE DIRECCIONAMIENTO DEL INSTITUTO COLOMBIANO AGROPECUARIO ICA*

BASADO EN LA NORMA NTC-ISO/IEC 27001:2013. Bogotá D.C. Obtenido de http://polux.unipiloto.edu.co:8080/00004753.pdf

Fernández Rivero, P., & Gómez Fernández, L. (2018). *Cómo implementar un SGSI según UNE-EN 27001 y su aplicación en el Esquema Nacional de Seguridad.* AENOR - Asociación Española de Normalización y Certificación. Obtenido de https://elibro.net/es/ereader/uleam/53624

Ferro Velga, J. M. (2020). *Perito Judicial en Auditoría Informática* (Ilustrada ed.). Lulu. Obtenido de https://books.google.com.ec/books?id=w9HMDwAAQBAJ&lpg=PT8&dq=area%20de%20la%20auditoria%20informatica&pg=PT6#v=onepage&q&f=false

Gómez Vieites, Á. (2015). *Auditoría de seguridad informática.* Madrid: RA-MA Editorial. Obtenido de https://elibro.net/es/ereader/uleam/62464

González, J. D. (2022). *ProgramarYa*. Obtenido de https://www.programarya.com/Cursos/Fundamentacion/Errores

Grados, J., & Sánchez, E. (2018). *La entrevista en las organizaciones.* Manual Moderno. Obtenido de http://biblio3.url.edu.gt/Libros/la_entrevista/4.pdf

Hernandez, E. H. (1993). *Master en Informática Administrativa.* Monterrey. Obtenido de https://repository.ucc.edu.co/bitstream/20.500.12494/304/1/AUDITORIA%20DE%20SEGURIDAD%20DE%20LA%20INFORMACI%C3%93N.pdf

Imagar. (9 de Octubre de 2021). *Imagar*. Obtenido de https://www.imagar.com/blog-desarrollo-web/que-es-el-protocolo-en-informatica/

Jiménez Ortiz, D., & Namuche Ayala, J. (2019). *Estado del arte de la auditoría informática y su importancia para las empresas.* Linea de Investigación. Obtenido de https://repositorio.unp.edu.pe/handle/UNP/1971

Kiligann, A. (21 de Junio de 2022). *El Consejo Salvador*. Obtenido de https://elconsejosalvador.com/faq/cual-es-el-objetivo-de-la-seguridad-informatica.html

Laprieda Alcamí, R., Devece Carañana, C., & Guiral Herrando, J. (2016). *Introducción a la gestión de sistemas de información en la empresa.* D - Universitat Jaume I. Servei de Comunicació i Publucaciones. Obtenido de https://elibro.net/es/ereader/uleam/51689

Linux NET. (12 de Diciembre de 2020). *Linux NET*. Obtenido de https://blog.desdelinux.net/seguridad-informacion-historia-terminologia-campo/#Historia

Lopéz, P. L. (2004). Población, muestra y muestreo . *SciELO Analytics*. Obtenido de http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S1815-02762004000100012#:~:text=Es%20un%20subconjunto%20o%20parte,parte%20representativa%20de%20la%20poblaci%C3%B3n.

manageengine.com. (2018). *Manage Engine* . Obtenido de https://manageengine.com.mx/vmp/mala-configuracion

Mantilla Guerra, A. (2018). Gestión de seguridad de la información con la norma ISO 27001:2013. *Revista Espacios, 39*, 5. Obtenido de https://www.revistaespacios.com/a18v39n18/a18v39n18p05.pdf

Mendz, L. (21 de Agosto de 2016). *Slideshare.* Obtenido de https://es.slideshare.net/LionMendz/impacto-de-la-tecnologa-informtica-sobre-la-funcin-de-la-auditora

Naranjo Camacho, J., & Reyes Lucas, J. (Junio de 2020). *Repositorio UG.* Obtenido de http://repositorio.ug.edu.ec/handle/redug/48923

Navarro, F. (14 de Diciembre de 2021). *INESEM Escuela de líderes*. Obtenido de https://www.inesem.es/revistadigital/gestion-integrada/seguridad-logica-informatica/#:~:text=A%20grandes%20rasgos%20con%20la,ni%20archivos%20que%20no%20correspondan.

Niño Morante, N. (2018). *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.* Obtenido de https://repositorio.unprg.edu.pe/handle/20.500.12893/5935

Ocampo, D. S. (23 de Junio de 2020). *Investigalia.* Obtenido de https://investigaliacr.com/investigacion/la-encuesta-y-el-cuestionario/

Pallerola Comamala, J. (2015). *Auditoría.* Madrid: RA-MA Editorial. Obtenido de https://elibro.net/es/ereader/uleam/62443

Quillupangui Toapanda, D. A. (2019). *Auditoría informática mediante COBIT 5 para el área informática en la empresa ROSAS DEL CORAZÓN.* U.T.C. Latacunga. Obtenido de http://repositorio.utc.edu.ec/handle/27000/5703

Reyqui. (21 de Agosto de 2019). *La UPEA.* Obtenido de https://upea.reyqui.com/2019/08/metodo-sintetico-en-que-

consiste.html#:~:text=El%20m%C3%A9todo%20sint%C3%A9tico%20es%20un,en%20el%20desarrollo%20del%20acontecimiento.

Rodriguez Baca, L., Cruzado Puente de la Vega, C., Mejia Corredor, C., & Diaz Mitchell, A. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. *Propósitos y Representaciones, vol. 8*. Obtenido de http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S2307-79992020000400011&lng=es&nrm=iso&tlng=es

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., . . . Castillo Merino, M. A. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Área de Innovación y Desarrollo. Obtenido de https://books.google.com.ec/books?id=5Z9yDwAAQBAJ&lpg=PA1&pg=PA1#v=onepage&q&f=false

Ruiz Limón, R. (2006). *Historia y evolución del pensamiento científico.* Obtenido de http://www.eumed.net/libros-gratis/2007a/257/7.1.htm#:~:text=El%20M%C3%A9todo%20anal%C3%ADtico%20es%20aquel,de%20un%20hecho%20en%20particular.

Salcedo Cifuentes, M., Ortíz Gómez, Y., & Hincapie Saldarriaga, Á. F. (2018). *La calidad del dato en los sistemas de información de convivencia y seguridad ciudadana.* Programa Editorial Universidad del Valle. Obtenido de https://elibro.net/es/ereader/uleam/131607

Sánchez , A., & Pellicer, Y. (2013). *La auditoría a las tecnologías de la informática. Relación del derecho y la informática jurídica.* Derecho y Cambio Social. doi:10(32)

Sánchez Ch, W. (2021). *Teoría de la auditoría.* Grupo Editorial Nueva Legislación. Obtenido de https://elibro.net/es/ereader/uleam/188499

Santander Becas. (10 de Diciembre de 2021). *Santander Becas*. Obtenido de https://www.becas-santander.com/es/blog/cualitativa-y-cuantitativa.html

Silva Coelho, F., Segadas de Araújo, L., & Kowask Bezerra, E. (2018). *Gestión de la seguridad de la información.* Bogotá D.C.: Escuela superior de Redes RED CEDIA. doi:https://www.cedia.edu.ec/assets/docs/publicaciones/libros/GTI8.pdf

Uriarte, J. (27 de Julio de 2022). *Humanidades.com*. Obtenido de https://humanidades.com/metodo-deductivo/

Vásquez Hidalgo, I. (2005). *Tipos de estudio y métodos de investigación* (Vol. 20). Recuperado el Noviembre de. Obtenido de http://nodo.ugto.mx/wp-content/uploads/2016/05/Tipos-de-estudio-y-m%C3%A9todos-de-investigaci%C3%B3n.pdf

Vega Briceño, E. (2021). *Seguridad de la Información.* Alzamora. doi:https://doi.org/10.17993/tics.2021.4

Ventura León, J. (2017). Population or sample?: A necessary difference. *Revista Cubana de Salud Pública*. Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0864-34662017000400014&lng=es&tlng=en.

Villegas, A. S. (14 de Julio de 2014). *Prezi.* Obtenido de https://prezi.com/kfxqvkl2f-h6/auditoria-informatica-evolucion-y-conceptos/

Zevallos Hidalgo , E. (Enero de 2020). *Repositorio Uleam.* Obtenido de https://repositorio.uleam.edu.ec/handle/123456789/2067

ANEXOS

Anexo A

Document Information

Analyzed document	TesisNathalyRamirez.pdf (D156564992)
Submitted	2023-01-22 03:16:00
Submitted by	
Submitter email	e2350998049@live.uleam.edu.ec
Similarity	2%
Analysis address	clara.pozo.uleam@analysis.urkund.com

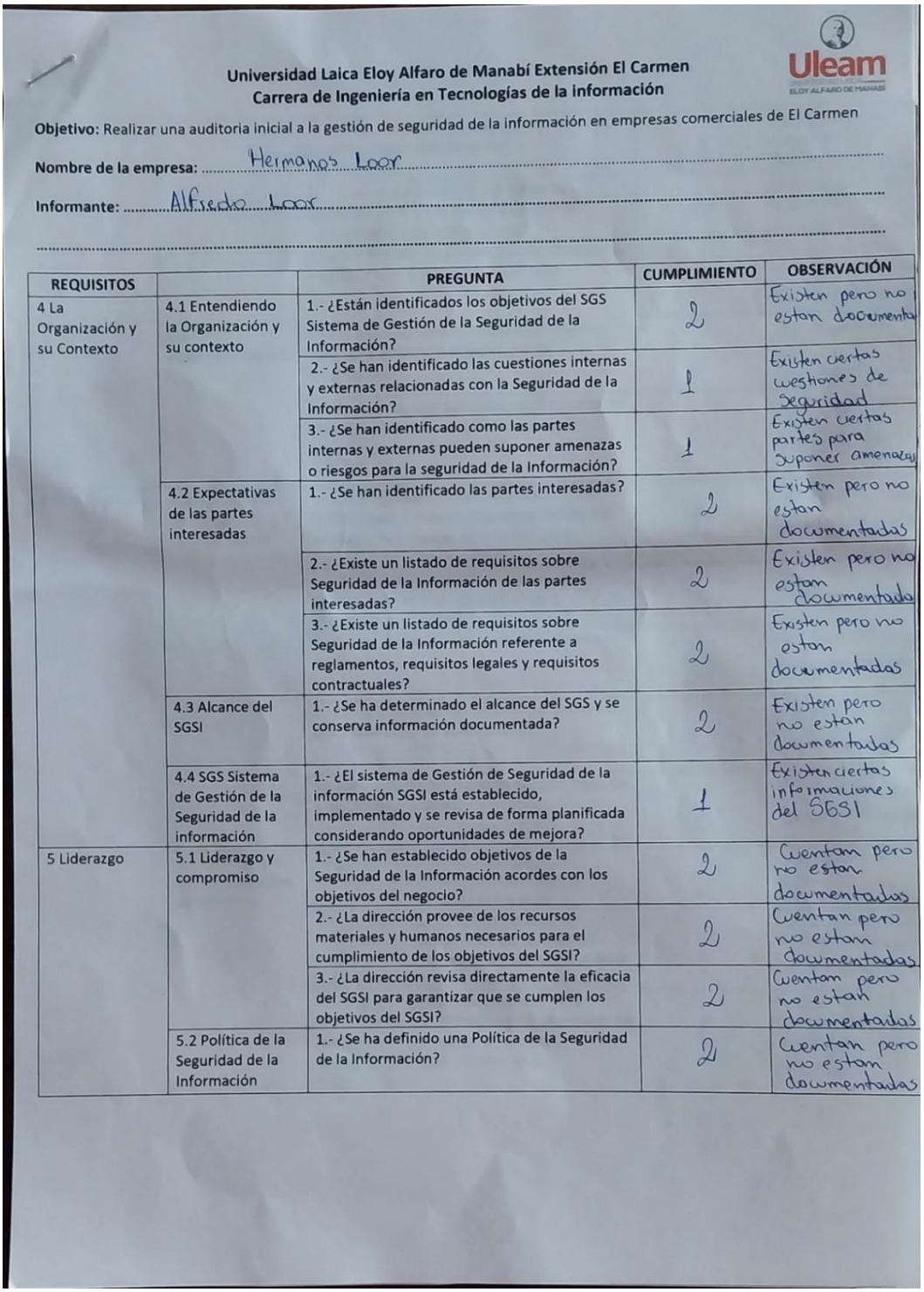
Sources included in the report

W	URL: http://repositorio.unesum.edu.ec/bitstream/53000/2581/1/MAYANQUER%20ANDINO%20JAVIER%20ANIBAL.pdf Fetched: 2021 06-26 10:27:20	5
SA	**1430541842_Borrador_Tesis_VARGAS_LUIS_v1.docx** Document 1430541842_Borrador_Tesis_VARGAS_LUIS_v1.docx (D14169328)	2
W	URL: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/10320/IMPLEMENTACIO%CC%81N%20... Fetched: 2022 09-06 17:15:25	1
SA	**M1.880_20221_PEC6_19018864.txt** Document M1.880_20221_PEC6_19018864.txt (D155225204)	1
SA	**M1.809_20201_PEC1_12864557.txt** Document M1.809_20201_PEC1_12864557.txt (D81485562)	1
SA	**DAQUI DAISY.docx** Document DAQUI DAISY.docx (D64895085)	1
SA	**M1.887_20202_PEC 4. Memoria final_15169886.txt** Document M1.887_20202_PEC 4. Memoria final_15169886.txt (D107359366)	1

Entire Document

I Tesis Nathaly Ramirez Coello RESUMEN El presente trabajo de titulación tuvo por objetivo realizar una auditoría informática a la gestión de seguridad de la información según la ISO 27001 a 3 empresas comerciales de El Carmen, se empezó por identificar la problemática realizando una entrevista y encuesta a los empleados de dichas empresas para justificar la presente investigación, llegando a determinar que no existía un conocimiento sobre Gestión de seguridad de la información y su importancia, por ello como propuesta se aplicó una auditoría de seguridad inicial para determinar la brecha GAP que consiste en encontrar el porcentaje de incumplimiento según el estándar de los requisitos y controles de seguridad, que contiene un conjunto de 7 ítems que deberían cumplir las organizaciones para considerar que la gestión de seguridad garantiza la integridad, confidencialidad y disponibilidad de su información. Como resultados relevantes se obtuvo que, la empresa Translatin tiene un nivel de madurez alto y las empresas Hermanos Loor y Alcívar tienen un nivel de madurez medio, finalmente se propone un manual para la gestión de seguridad de la información para las empresas ya mencionadas.

Anexos B



Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen
Carrera de Ingeniería en Tecnologías de la Información

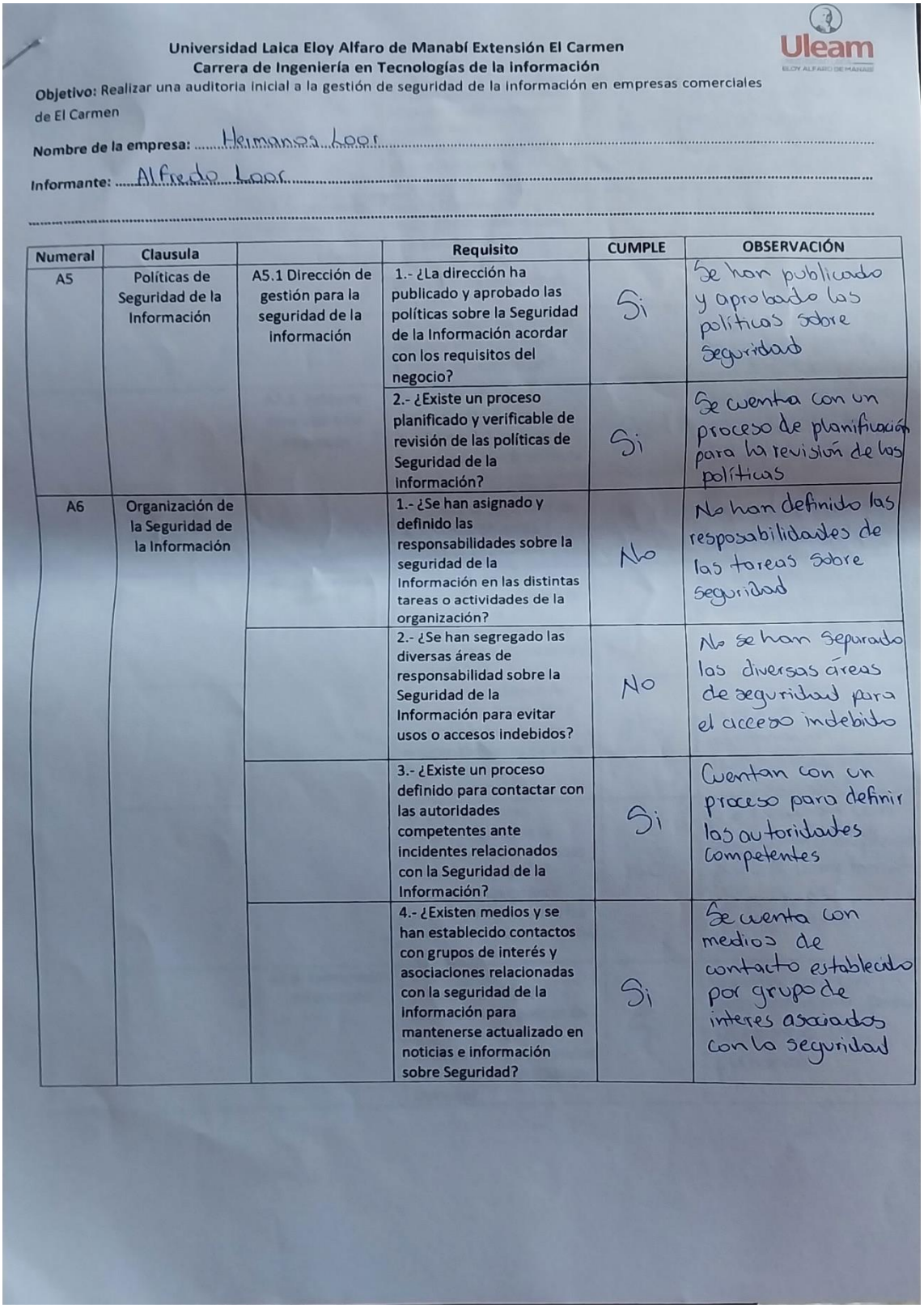
Objetivo: Realizar una auditoria inicial a la gestión de seguridad de la información en empresas comerciales de El Carmen

Nombre de la empresa: Hermanos Loor

Informante: Alfredo Loor

REQUISITOS		PREGUNTA	CUMPLIMIENTO	OBSERVACIÓN
4 La Organización y su Contexto	4.1 Entendiendo la Organización y su contexto	1.- ¿Están identificados los objetivos del SGS Sistema de Gestión de la Seguridad de la Información?	2	Existen pero no estan documenta
		2.- ¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?	1	Existen ciertas cuestiones de seguridad
		3.- ¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la Información?	1	Existen ciertas partes para suponer amenaza
	4.2 Expectativas de las partes interesadas	1.- ¿Se han identificado las partes interesadas?	2	Existen pero no estan documentadas
		2.- ¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas?	2	Existen pero no estan documentadas
		3.- ¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales?	2	Existen pero no estan documentadas
	4.3 Alcance del SGSI	1.- ¿Se ha determinado el alcance del SGS y se conserva información documentada?	2	Existen pero no estan documentadas
	4.4 SGS Sistema de Gestión de la Seguridad de la información	1.- ¿El sistema de Gestión de Seguridad de la información SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora?	1	Existen ciertas informaciones del SGSI
5 Liderazgo	5.1 Liderazgo y compromiso	1.- ¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio?	2	Cuentan pero no estan documentadas
		2.- ¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?	2	Cuentan pero no estan documentadas
		3.- ¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?	2	Cuentan pero no estan documentadas
	5.2 Política de la Seguridad de la Información	1.- ¿Se ha definido una Política de la Seguridad de la Información?	2	Cuentan pero no estan documentadas

Instrumentos de cumplimiento de requisitos de la ISO 27001



Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen
Carrera de Ingeniería en Tecnologías de la Información

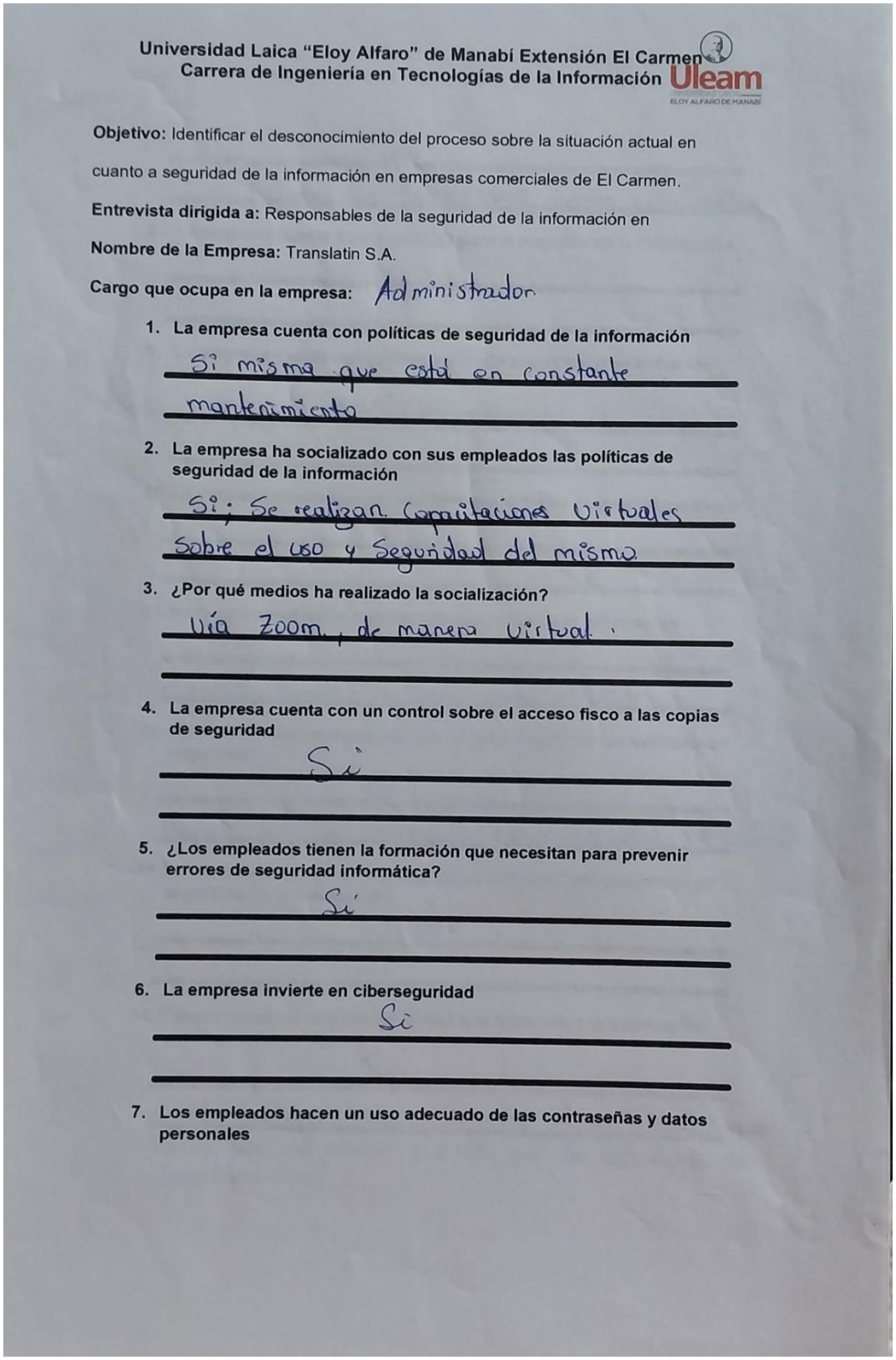
Objetivo: Realizar una auditoria inicial a la gestión de seguridad de la información en empresas comerciales de El Carmen

Nombre de la empresa: Hermanos Loor

Informante: Alfredo Loor

Numeral	Clausula		Requisito	CUMPLE	OBSERVACIÓN
A5	Políticas de Seguridad de la Información	A5.1 Dirección de gestión para la seguridad de la información	1.- ¿La dirección ha publicado y aprobado las políticas sobre la Seguridad de la Información acordar con los requisitos del negocio?	Si	Se han publicado y aprobado las políticas sobre seguridad
			2.- ¿Existe un proceso planificado y verificable de revisión de las políticas de Seguridad de la información?	Si	Se cuenta con un proceso de planificación para la revisión de las políticas
A6	Organización de la Seguridad de la Información		1.- ¿Se han asignado y definido las responsabilidades sobre la seguridad de la Información en las distintas tareas o actividades de la organización?	No	No han definido las responsabilidades de las tareas sobre seguridad
			2.- ¿Se han segregado las diversas áreas de responsabilidad sobre la Seguridad de la Información para evitar usos o accesos indebidos?	No	No se han separado las diversas áreas de seguridad para el acceso indebido
			3.- ¿Existe un proceso definido para contactar con las autoridades competentes ante incidentes relacionados con la Seguridad de la Información?	Si	Cuentan con un proceso para definir las autoridades competentes
			4.- ¿Existen medios y se han establecido contactos con grupos de interés y asociaciones relacionadas con la seguridad de la información para mantenerse actualizado en noticias e información sobre Seguridad?	Si	Se cuenta con medios de contacto establecido por grupo de interes asociados con la seguridad

Instrumentos de control de seguridad de la ISO 27001



Universidad Laica "Eloy Alfaro" de Manabí Extensión El Carmen
Carrera de Ingeniería en Tecnologías de la Información

Objetivo: Identificar el desconocimiento del proceso sobre la situación actual en cuanto a seguridad de la información en empresas comerciales de El Carmen.

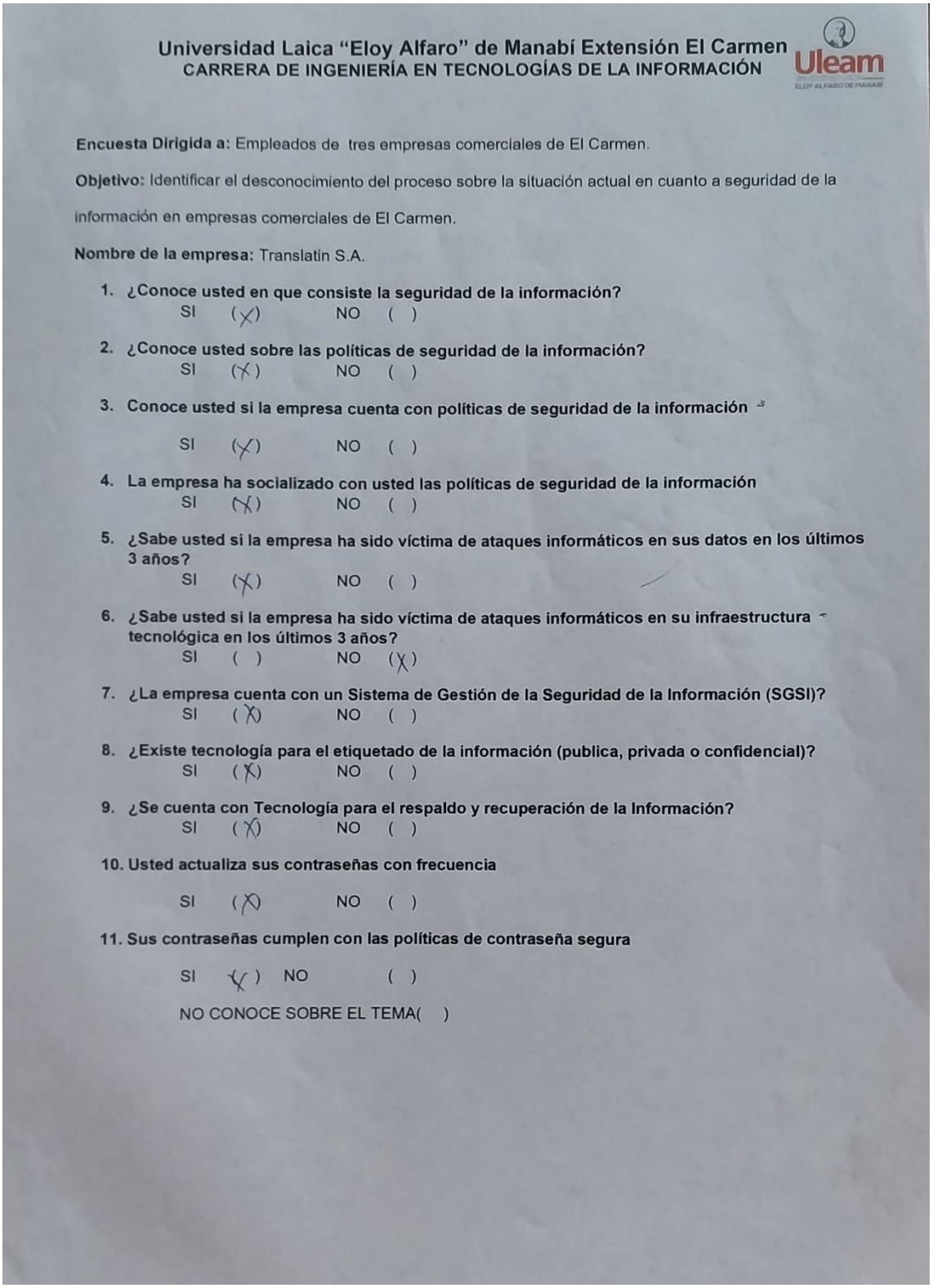
Entrevista dirigida a: Responsables de la seguridad de la información en

Nombre de la Empresa: Translatin S.A.

Cargo que ocupa en la empresa: Administrador

1. **La empresa cuenta con políticas de seguridad de la información**
   Si misma que está en constante mantenimiento
2. **La empresa ha socializado con sus empleados las políticas de seguridad de la información**
   Si; Se realizan Capacitaciones Virtuales sobre el uso y Seguridad del mismo
3. **¿Por qué medios ha realizado la socialización?**
   Vía Zoom, de manera virtual.
4. **La empresa cuenta con un control sobre el acceso fisco a las copias de seguridad**
   Si
5. **¿Los empleados tienen la formación que necesitan para prevenir errores de seguridad informática?**
   Si
6. **La empresa invierte en ciberseguridad**
   Si
7. **Los empleados hacen un uso adecuado de las contraseñas y datos personales**

Instrumento de entrevista a las empresas comerciales de El Carmen.



Universidad Laica "Eloy Alfaro" de Manabí Extensión El Carmen
CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

Encuesta Dirigida a: Empleados de tres empresas comerciales de El Carmen.

Objetivo: Identificar el desconocimiento del proceso sobre la situación actual en cuanto a seguridad de la información en empresas comerciales de El Carmen.

Nombre de la empresa: Translatin S.A.

1. **¿Conoce usted en que consiste la seguridad de la información?**
   SI (X) NO ( )
2. **¿Conoce usted sobre las políticas de seguridad de la información?**
   SI (X) NO ( )
3. **Conoce usted si la empresa cuenta con políticas de seguridad de la información**
   SI (X) NO ( )
4. **La empresa ha socializado con usted las políticas de seguridad de la información**
   SI (X) NO ( )
5. **¿Sabe usted si la empresa ha sido víctima de ataques informáticos en sus datos en los últimos 3 años?**
   SI (X) NO ( )
6. **¿Sabe usted si la empresa ha sido víctima de ataques informáticos en su infraestructura tecnológica en los últimos 3 años?**
   SI ( ) NO (X)
7. **¿La empresa cuenta con un Sistema de Gestión de la Seguridad de la Información (SGSI)?**
   SI (X) NO ( )
8. **¿Existe tecnología para el etiquetado de la información (publica, privada o confidencial)?**
   SI (X) NO ( )
9. **¿Se cuenta con Tecnología para el respaldo y recuperación de la Información?**
   SI (X) NO ( )
10. **Usted actualiza sus contraseñas con frecuencia**
    SI (X) NO ( )
11. **Sus contraseñas cumplen con las políticas de contraseña segura**
    SI (X) NO ( )
    NO CONOCE SOBRE EL TEMA( )

Instrumento de encuestas de las empresas comerciales de El Carmen

Entrevistando al personal encargado de informática de las empresas comerciales de El Carmen.

GLOSARIO

TIC'S: Tecnologías de la Información y Comunicación

ISO: Organización Internacional de Normalización

Denegación: Delito que se comete desobedeciendo de manera injustificada un requerimiento de la autoridad o elidiendo sin excusa legal una función o un cargo público.

Mitigar: Atenuar o suavizar una cosa negativa, especialmente una enfermedad.

Reposicionamiento: Es la modificación del enfoque estratégico de la marca para alcanzar territorios relevantes de significado. Un reposicionamiento de marca surge cuando la estrategia de marca no es la mejor y no genera buenos resultados para la empresa.

Terminología: Conjunto de términos o palabras propias utilizadas en una ciencia, técnica, o especialidad, o por un autor.

TI: Tecnologías de la Información

Magerit: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

SGSI: Sistema de seguridad de la Información

Usabilidad: Cualidad de la página web o del programa informático que son sencillos de usar porque facilita la lectura de los textos, descargan rápidamente la información y presentan funciones y menús sencillos, por lo que el usuario encuentra satisfechas sus consultas y cómodo su uso.

Encriptado: Es el proceso de codificar un mensaje o información de modo tal que solo los individuos autorizados sean capaces de acceder a esta, y aquellos que no estén autorizados no puedan hacerlo.

Inteligible: Que puede ser entendido.

DDoS: Ataque distribuido de denegación de servicio.

SLA: Acuerdo de Nivel de Servicio

Buffer: Memoria de almacenamiento temporal de información que permite transferir los datos entre unidades funcionales con características de transferencia diferentes.

Payloads: Es la carga maliciosa que ejecuta un hacker en el ordenador de una víctima durante un ciberataque.

Backdoor: Puerta trasera: la entrada secreta a tus dispositivos.

Default: Defecto que se produce cuando una empresa, una persona o un Estado no cuenta con dinero líquido (en efectivo) para hacer frente a su deuda.

Crackear: Es una técnica que vulnera software informático o todo un sistema de seguridad con intenciones maliciosas.

SSH: Cápsula segura, es un mecanismo de seguridad ofrecido por los servicios de hospedaje.

Password: Contraseña, clave o código de acceso.

XSS: (Cross Site Scripting) Vulnerabilidad de seguridad que permite a un atacante inyectar en un sitio web código malicioso del lado del cliente.

SQL: Lenguaje de consulta estructurado

Scripts: Fragmentos de código que tienen como objetivo realizar o añadir funciones dentro de una página web o e-commerce.

HTTP: Protocolo de transferencia de hipertextos, que se utiliza en algunas direcciones de internet.

TSL: Seguridad de la capa de transporte, es el protocolo sucesor de SSL.

Disuasorio: Que disuade o tiene la capacidad de hacer que alguien desista de una acción o decisión.