UNIVERSIDAD TÉCNICA DE BABAHOYO FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

PERIODO DICIEMBRE 2022 - MAYO 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERÍA EN SISTEMAS

TEMA:

ANALISIS Y PLANIFICACION DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NORMAS ISO 27000 DE LA COMPAÑIA DE TRANSPORTE PESADO 17 DE NOVIEMBRE

EGRESADA:

ZAIDA ANDREA CRUZ CANDELARIO

TUTOR:

ING. FREDDY MAXIMILIANO JORDAN CORDONES.

AÑO:

2022 - 2023

INTRODUCCIÓN

El propósito de la investigación es analizar y planificar la seguridad de la información en la compañía de transporte pesado 17 de noviembre S.A., basándose en las normas ISO 27000. El objetivo principal es identificar las posibles vulnerabilidades en la seguridad de la información y diseñar medidas para prevenir posibles incidentes de seguridad.

La investigación se basa en una revisión exhaustiva de las normas ISO 27000 y su aplicación en organizaciones similares. Se llevó a cabo una auditoría de seguridad de la información en la compañía 17 de noviembre S.A. para identificar las debilidades existentes en el sistema de seguridad y luego se diseñó un plan de acción basado en las mejores prácticas y recomendaciones de ISO 27000.

Se integraron los conocimientos adquiridos en la investigación para desarrollar un plan de seguridad de la información para la compañía 17 de noviembre S.A. El plan incluye la identificación y clasificación de la información crítica, el diseño de políticas y procedimientos de seguridad, la implementación de controles de acceso y la capacitación del personal en seguridad de la información.

Preguntas de reflexión: ¿Cómo podría la compañía 17 de noviembre S.A. medir el éxito de la implementación del plan de seguridad de la información? ¿Qué tan efectivas son las normas ISO 27000 en la prevención de incidentes de seguridad en organizaciones similares? ¿Cómo podría la compañía 17 de noviembre mejorar la conciencia y capacitación en seguridad de la información de sus empleados?

La investigación muestra que la implementación de un sistema de seguridad de la información basado en las normas ISO 27000 puede ayudar a las organizaciones a proteger su información y prevenir posibles incidentes de seguridad. El plan de seguridad de la información

desarrollado para la compañía 17 de noviembre S.A. proporciona una guía clara y detallada para mejorar la seguridad de la información en la organización.

En relación a la línea de investigación “Sistemas de información y comunicación, emprendimiento e innovación”, se puede destacar que la implementación de un plan de seguridad de la información basado en las normas ISO 27000 en la compañía de transporte pesado 17 de noviembre S.A. puede ser considerada una innovación, en cuanto a la adopción de “Redes y Tecnologías Inteligentes de Software y Hardware” para proteger la información de la empresa y mejorar su competitividad en el mercado.

DESARROLLO

La compañía de transporte pesado 17 de noviembre S.A. inicio sus actividades en el 2009, cuya representante legal es la Sra. Bonifas Lozano Patricia, con RUC #1291735947001, se dedica a todas las actividades de transporte y carga por carretera incluido en automóviles, camionetas de tronco, ganado, carga pesada, transporte refrigerado, carga a granel, transporte de camiones cisternas, desperdicios de desechos sin recogidas ni eliminación.

Dado que la compañía maneja información crítica relacionada con sus operaciones de transporte, es esencial que tenga un enfoque riguroso para identificar, gestionar y mitigar los riesgos de seguridad de la información. Esto podría incluir el establecimiento de políticas y procedimientos claros para la gestión de información sensible, la implementación de medidas de seguridad tecnológicas y físicas adecuadas y la formación de los empleados en prácticas de seguridad de la información. La norma ISO/IEC 27001 puede proporcionar un marco útil para que la compañía establezca y mantenga un sistema de gestión de seguridad de la información efectivo. Al aplicar estos principios, la compañía 17 de noviembre puede mejorar la seguridad de su información y garantizar la continuidad de sus operaciones críticas de transporte.

El objetivo principal de este proyecto es analizar y planificar la seguridad de la información en la compañía de transporte pesado 17 de noviembre S.A., utilizando un enfoque basado en las normas ISO 27000.

La implementación de un SGSI basado en la norma ISO 27000 es factible en la compañía de transporte pesado 17 de noviembre porque permite cumplir con los requisitos normativos, proteger los activos de la compañía, reducir riesgos y mejorar continuamente la seguridad de la información.

Es relevante destacar que el propósito de contar con un Sistema de Seguridad de la Información es asegurar que los miembros de la compañía conozcan, gestionen y minimicen

los riesgos asociados. Según ISO/IEC 2700, (2022) es esencial documentar, sistematizar y estructurar cada procedimiento con el fin de establecer políticas y procedimientos relacionados con los objetivos de la institución y obtener el máximo beneficio. Para lograr esto, se recomienda seguir los estándares internacionales que se detallan a continuación.

Para realizar el análisis y planificación del SGSI, es fundamental contar con una comprensión general de la terminología y las definiciones que se utilizarán durante todo el proceso. De esta manera, se puede evitar confusiones o malentendidos que surjan debido a interpretaciones diferentes.

Normas ISO

De acuerdo con ISO/IEC 2700 (2022) Una norma ISO se define como un modelo de requisitos, directrices o especificaciones técnicas que establecen una serie de criterios que deben cumplirse para garantizar la calidad, seguridad, fiabilidad y eficiencia de los productos o servicios que se ofrecen.

Norma de seguridad informática ISO 27000

En octubre de 2005, la Organización Internacional de Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) aprobaron y publicaron el Estándar Internacional ISO/IEC 27000 para la seguridad de la información. Para Martínez (2021)

> Los objetivos de seguridad de una organización varían dependiendo del sector en el que se encuentre, pero en general están relacionados con la seguridad de los procesos organizativos y de producción, el ciclo de vida de la información y el cumplimiento de las leyes aplicables.

Protección de activos

La norma propone una estrategia completa para la seguridad de la información, la cual considera que los activos que deben ser protegidos son diversos, tales como la información digital, los documentos impresos y los activos físicos como computadoras y redes. Según Fernández, (2020) para alcanzar este objetivo, se implementan una serie de medidas que abarcan desde el desarrollo de la competencia del personal de la organización hasta la implementación de medidas técnicas para protegerse contra fraudes informáticos.

Según Contreras (2021), menciona que se pueden identificar tres principios fundamentales en la seguridad de la información:

- La disponibilidad, que asegura que los usuarios autorizados tengan acceso a la información y a los activos relacionados cuando sea necesario.
- La confidencialidad, que garantiza que solo las personas autorizadas tengan acceso a la información.
- La integridad, que protege la exactitud y la integridad de la información y los métodos de procesamiento utilizados.

Sistemas de Información y Comunicación

Una organización es un sistema compuesto por diferentes componentes, que trabajan juntos para generar beneficios para empleados y accionistas. Para Davalos, (2019) “el sistema organizacional depende de un sistema de información, que es la forma en que los datos fluyen entre los departamentos y personas”. Estos sistemas pueden incluir desde comunicaciones internas hasta sistemas de cómputo que generan informes. Los sistemas de información enlazan todos los componentes de la organización y los hacen trabajar de manera eficiente para alcanzar los mismos objetivos.

Los sistemas de información se componen de subsistemas, que engloban hardware, software y dispositivos de almacenamiento de datos. Estos subsistemas se combinan para formar lo que se conoce como una aplicación de sistemas de información, que puede ser utilizada en diversas áreas como ventas, contabilidad y compras. Los componentes están estrechamente relacionados y permiten reunir, procesar, guardar y distribuir información con el objetivo de facilitar la toma de decisiones y el control de una organización.

Tipos y funciones de los sistemas de información

Las funciones que cumplen los sistemas de información en las organizaciones son los siguientes:

- Proporcionar datos que justifiquen el procedimiento para llegar a una decisión.
- Automatización de procesos operativos.
- Crea una ventaja estratégica empleándola y utilizándola de manera efectiva.

(ISOTools, 2023)

Normas ISO 7001

La norma principal de esta serie de normas establece que la seguridad de la información se refiere a la protección de la confidencialidad, integridad y disponibilidad de los sistemas y datos que se manejan. Es decir, se trata de mantener la privacidad de la información, asegurar que no se modifica sin autorización y que está disponible cuando se necesita.

La ISO 27001 propone un modelo de gestión de seguridad de la información basado en la estructura que consta de tres fases: planificar, hacer y verificar. Para Rodríguez, (2019)

> En la fase de planificación, se establece el alcance del sistema de gestión de seguridad de la información (SGSI), se crea una política de seguridad y se identifican los riesgos de la información. Durante la fase de ejecución, se

implementan los controles necesarios para minimizar los riesgos y se documentan los procedimientos para su aplicación. En la fase de verificación, se evalúa el rendimiento del SGSI, se analizan los riesgos y la eficacia de los controles, se realiza una revisión interna y se supervisa la gestión por parte de la dirección.

ISO 27002

La Norma ISO/IEC 27002 describe prácticas recomendadas para la gestión de la seguridad de la información y ofrece consejos a aquellos responsables de establecer, implementar o mantener sistemas de seguridad de la información y gestión de la seguridad de la información. Según Terranova, (2022) menciona que la norma define la seguridad de la información como la preservación de la confidencialidad (asegurando que solo personas autorizadas puedan acceder a la información), la integridad (asegurando que la información y su justificación sean correctas y completas) y la disponibilidad (asegurando que los usuarios autorizados tengan acceso a la información y sus activos asociados cuando sea necesario).

ISO 27003

La ISO 27003, (2020) establece directrices para la implementación de un SGSI y es útil tanto para aquellos que buscan establecer uno como para consultores en su trabajo diario. La norma aborda el dimensionamiento y el diseño del SGSI, un proceso para obtener el consentimiento y un cronograma de implementación, además de proporcionar instrucciones para su implementación.

Según Vera, (2019) menciona que la información que se encuentra en el estándar es la siguiente:

- Efectividad
- Revisiones legislativas
- El acuerdo de los líderes de la compañía que permite el inicio del SGSI.
- Definiciones y explicaciones

- Estandarización parametrizada
- Evaluar los requisitos de seguridad de la información.
- Implementación de la SGSI.
- Describe la extensión, la política y las limitaciones del SGSI.

ISO 27004

El estándar ISO 27004 define las mejores prácticas para medir los resultados de los Sistemas de Gestión de Seguridad de la Información (SGSI) en ISO 27001. Establece la estructura del sistema de medición, los datos a medir, cuándo y cómo medirlos. Ayuda a establecer objetivos y criterios de éxito. Los métodos a utilizar dependen de la complejidad, el tamaño de la organización y la relación costo-beneficio. Esta norma describe cómo deben integrarse y documentarse los datos obtenidos en el SGSI.

Para Contreras, (2021) los pasos recomendados por ISO27004 para evaluar o medir la eficacia de la seguridad de la información son los siguientes:

- La organización necesita medir una variedad de métodos y solo se deben considerar los procesos documentados sistemáticamente.
- Es importante definir valores clave que sirvan como puntos de referencia para cada objeto medido.
- La medición debe incluir la realización de procedimientos o controles y las acciones de los empleados.
- Se debe desarrollar un sistema de medición lógico que aplique varias propiedades del objeto seleccionado para la medición.
- Los datos utilizados para la medición deben ser precisos, oportunos y dimensionales. Se pueden utilizar técnicas de recopilación de datos programados.
- La interpretación y análisis de los valores medidos se realiza utilizando tecnología y procedimientos apropiados.

- Los indicadores se utilizan como fuente de datos para mejorar el desempeño de los programas relacionados con la seguridad de la información.
- Los datos obtenidos de la medición deben ser comunicados a los interesados mediante paneles de operación, informes, boletines o formularios gráficos.

ISO 27005

ISO 27005 es un estándar para la gestión de riesgos de seguridad de la información que se aplica a todas las organizaciones, se basa en ISO 27001 y reemplaza a normas anteriores. No recomienda una metodología específica. Se basa en los requisitos definidos en ISO 27001 y es aplicable a todas las organizaciones. Esta norma reemplaza a las normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000 sobre gestión de la información y seguridad de la tecnología de las comunicaciones. Según Santillán, (2022) esta norma utiliza el modelo PHVA:

1. Planear: se establecen objetivos y metas, se determinan los procesos necesarios para lograrlos y se definen los indicadores de desempeño.
2. Hacer: se implementan los procesos planificados y se recopilan los datos necesarios.
3. Verificar: se comparan los resultados obtenidos con los objetivos y metas establecidos, y se analizan las desviaciones.
4. Actuar: se toman medidas para corregir las desviaciones y se establecen mejoras en los procesos para la siguiente iteración del ciclo PHVA.

ISO 27006

De acuerdo con ISOTools, (2023) la norma ISO 27006 proporciona directrices a los organismos de certificación para realizar auditorías de sistemas de gestión de seguridad de la información (SGSI) de acuerdo con los requisitos formales. Esta norma garantiza la validez de los certificados emitidos basados en la norma ISO 27001.

La norma aborda los siguientes requisitos generales:

- Directrices de equidad específicas para el SGSI.
- Una lista de trabajos que podrían generar conflictos.
- Una lista de actividades al aire libre que se pueden realizar.

ISO 27007

ISO/IEC 27007 (2020) es una norma que brinda orientación a los organismos de certificación y auditores en la evaluación del cumplimiento del estándar ISO/IEC 27001 para la gestión de seguridad de la información. Esta norma se basa en los requisitos de evaluación de conformidad de la norma ISO 17021 y en la acreditación de organismos de certificación de SGSI según la norma ISO/IEC 27006. Su enfoque es proporcionar orientación específica para la auditoría de la CMSI, y se basa en la norma ISO 19011.

El estándar ISO/IEC 27007 se enfoca en la auditoría de cumplimiento del SGSI y brinda orientación sobre cómo administrar el programa de auditoría del SGSI, realizar una auditoría de SGSI efectiva y gestionar al auditor del SGSI. Esto incluye determinar qué debe ser auditado, quiénes serán los auditores, cómo se llevará a cabo la auditoría, cómo se mantendrán los registros de evaluación y cómo se mejorará continuamente el proceso. También se aborda la planificación del proceso de auditoría, la realización de actividades clave de auditoría y la gestión de las habilidades, competencias, atributos y evaluaciones del auditor del SGSI.

El estudio se llevó a cabo utilizando una metodología cualitativa, a través de entrevistas directas con los participantes. Como resultado, se realizó un análisis y se propusieron soluciones alternativas. Se llevó a cabo una investigación documental, la cual consistió en consultar diversas fuentes de información, como libros, tesis, e internet, con el fin de obtener datos relevantes para el proyecto. Esta información se utilizó como sustento científico del mismo, y permitió profundizar en problemas similares.

Se llevó a cabo una investigación exploratoria con el propósito de evaluar el estado actual de la seguridad de los sistemas de información y comunicación. La investigación se llevó a cabo con un enfoque descriptivo, con el fin de analizar detalladamente el problema en cuestión, identificar sus causas y consecuencias, así como las dificultades involucradas.

El proyecto está dirigido a un grupo específico de individuos compuesto por cinco empleados del departamento de sistemas de la compañía de transporte pesado 17 de noviembre S.A.

Con ayuda de la entrevista realiza se pueden sacar los siguientes interpretaciones:

Tabla 1. Aplican políticas

RESPUESTA	CANTIDAD	PORCENTAJE
Políticas para los sistemas de comunicación	0	0%
No	0	0%
Políticas para los sistemas de información	1	20%
Políticas para los usuarios	4	80%
Total	5	100%

Elaborado por la autora.

Gráfico 1. Aplican políticas

Interpretación

Según la respuesta del 80% de los empleados, se han establecido políticas exclusivas para los usuarios, lo que significa que cada individuo tiene su propia contraseña para acceder a la computadora y a las aplicaciones correspondientes. Por otro lado, el 20% de los encuestados indicaron que existen políticas que se aplican a los sistemas de información, como la realización de respaldos, copias de seguridad y la instalación de antivirus.

Análisis

Las políticas de seguridad existentes están dirigidas únicamente a los usuarios, lo que deja desprotegidos los sistemas de información y comunicación.

Tabla 2. Control interno

RESPUESTA	CANTIDAD	PORCENTAJE
Buena	1	20%
Envió de respaldos	1	20%
Asignación de contraseñas	3	60%
Total	5	100%

Elaborado por la autora.

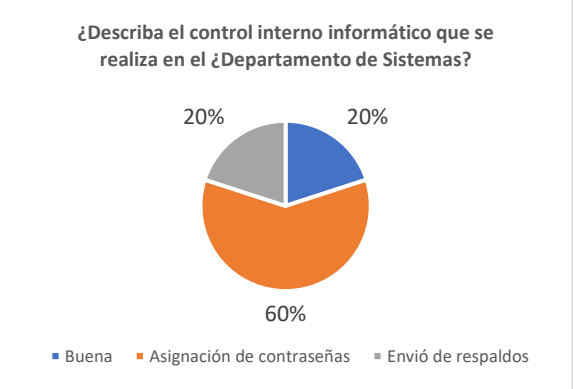


Gráfico 2. Control interno

Interpretación

De acuerdo a la encuesta, el 60% de los entrevistados afirmaron que se mantiene un control interno informático a través de la asignación de contraseñas a los usuarios de las aplicaciones. El 20% consideró que el control informático es bueno, ya que el departamento de sistemas es tratado como una pequeña o mediana empresa. El 20% restante dijo que el control se realiza mediante el envío de copias de seguridad a una custodia externa de los archivos de registro.

Análisis

No se realiza un análisis minucioso de todas las actividades relacionadas con los sistemas de información y comunicación.

Tabla 3. Control de la seguridad

RESPUESTA	CANTIDAD	PORCENTAJE
Bitácoras de cambios	1	20%
Mediante uso de aplicaciones	1	20%
Auditoría externa	1	20%
Módulos de administración	2	40%
Total	5	100%

Elaborado por la autora.

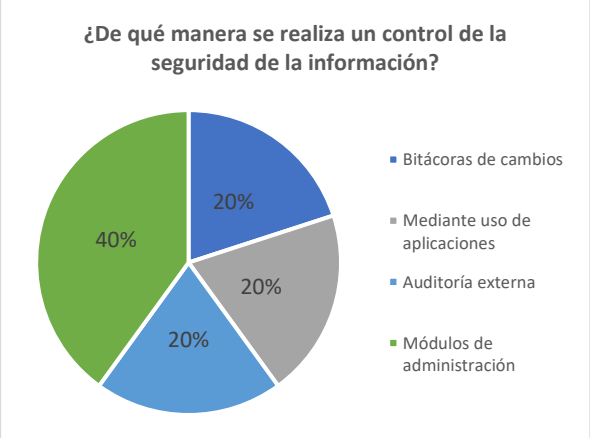


Gráfico 3. Control de la seguridad.

Interpretación

El 40% del personal encuestado utiliza módulos de administración basados en perfiles de usuario para controlar la seguridad de la información, mientras que el 20% utiliza auditorías externas y otro 20% mantiene una bitácora de cambios en las funciones y desempeño de los empleados. El restante 20% utiliza aplicaciones de seguridad como Check Point y Firewall.

Análisis

No hay un control de revisión que verifique la información que se ha establecido con el propósito de llevar a cabo esta tarea.

Tabla 4. Conoce los SGSI.

RESPUESTA	CANTIDAD	PORCENTAJE
Si	1	20%
No	4	80%
Total	5	100%

Elaborado por la autora.

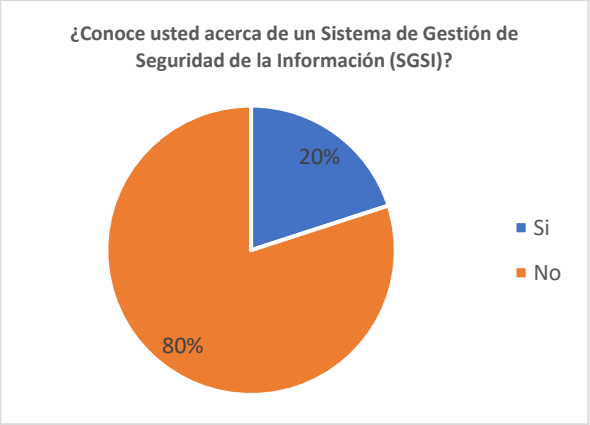


Gráfico 4. Conoce los SGSI.

Interpretación

De todas las respuestas recopiladas, solo el 20% estaba familiarizado con las funciones de un sistema de gestión de seguridad de la información. Este grupo pudo citar ejemplos como los sistemas de cifrado de disco PGP y Active Directory. La gran mayoría, que comprende el 80% restante, tenía poco o ningún conocimiento del tema.

Análisis

Prácticamente en su totalidad, el personal del departamento de sistemas carece de conocimientos acerca de lo que implica un sistema de gestión de seguridad de la información, lo que a su vez les impide conocer las ventajas y beneficios que puede ofrecer contar con un sistema de este tipo.

Para asegurar la confiabilidad, integridad y disponibilidad de la información que es procesada en los sistemas de información y comunicación, es posible utilizar sistemas de hardware y software robustos, así como aplicaciones como Firewall y antivirus. También se

pueden hacer respaldos de la base de datos y definir niveles de acceso a través de perfiles de usuarios con contraseñas.

Se están utilizando varios mecanismos de seguridad como la encriptación de contraseñas y enlaces de comunicación, así como herramientas como Check Point y Antivirus. Sin embargo, el control y administración de riesgos no se lleva a cabo de forma óptima, ya que se realiza externamente. Además, el monitoreo de los sistemas de comunicación y de información no se realiza de manera planificada, lo que aumenta la vulnerabilidad a ataques. Se han realizado algunos simulacros de caída de los sistemas, pero se basan en planes de contingencia previamente escritos.

CONCLUSION

Después de completar la investigación y analizar la información recopilada, llegamos a la conclusión de que:

- La mayoría de las políticas de seguridad se centran en los usuarios individuales, dejando desprotegidos los sistemas de información y comunicación.
- El conocimiento sobre los sistemas de gestión de seguridad de la información es limitado, lo que limita la capacidad del personal para aprovechar al máximo estas herramientas.
- Aunque se utilizan varios mecanismos de seguridad, como la encriptación de contraseñas y herramientas antivirus, el control y la administración de riesgos no se llevan a cabo de manera óptima.
- El monitoreo de los sistemas de comunicación y de información no se realiza de manera planificada, lo que aumenta la vulnerabilidad a ataques. Se han realizado algunos simulacros de caída de los sistemas, pero se basan en planes de contingencia previamente escritos.

RECOMENDACIONES

- Implementar políticas de seguridad integrales: es importante establecer políticas que no solo se enfoquen en los usuarios, sino también en los sistemas de información y comunicación. Esto incluye la realización de respaldos, copias de seguridad, la instalación de antivirus, entre otras medidas.
- Fortalecer el control interno informático: es necesario realizar un análisis minucioso de todas las actividades relacionadas con los sistemas de información y comunicación. Para ello, se puede asignar contraseñas a los usuarios de las aplicaciones, llevar una bitácora de cambios en las funciones y desempeño de los empleados, utilizar módulos de administración basados en perfiles de usuario, entre otros mecanismos.
- Capacitar al personal en seguridad de la información: es importante que todo el personal del departamento de sistemas tenga conocimientos sobre lo que implica un sistema de gestión de seguridad de la información. De esta manera, podrán conocer las ventajas y beneficios que puede ofrecer contar con un sistema de este tipo.
- Fortalecer la seguridad de los sistemas de hardware y software: se deben utilizar sistemas de hardware y software robustos, como Firewall y antivirus, para asegurar la confiabilidad, integridad y disponibilidad de la información que es procesada en los sistemas de información y comunicación. Además, se deben definir niveles de acceso a través de perfiles de usuarios con contraseñas.
- Realizar monitoreo y administración de riesgos de forma óptima: es necesario llevar a cabo un monitoreo de los sistemas de comunicación y de información de manera planificada para aumentar la seguridad y reducir la vulnerabilidad a ataques. También es importante realizar simulacros de caída de los sistemas y actualizar los planes de contingencia de manera regular.

BIBLIOGRAFÍA

Calder A. (2019). IT Governance: An International Guide to Data Security and ISO27001/ISO27002. Kogan Page.

Contreras B. (2021). Guía para la implementación de un Sistema de Gestión de Seguridad de la. BOOKET. https://www.pmgssi.com/2014/01/isoiec-27003-guia-para-la-implementacion-de-un-sistema-de-gestionde-seguridad-de-la-informacion/

Contreras R. (2021). Guía para la implementación de un Sistema de Gestión de Seguridad de la Información. PARA DUMMIES.

Davalos F. (2019). ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION. CROSSBOOKS. https://normaiso27001.es/a6-organizacion-de-la-seguridad-de-lainformacion/

Fernández K. (2020). Estrategia para la seguridad de la información. AUSTRAL.

ISO 27003. (2020). Tecnología de la Información. Técnicas de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información. EDICIONES PAIDÓS. http://www.iso27000.es.

ISO 27007. (2020). ISO/IEC 27001. ZENITH. http://es.wikipedia.org/wiki/ISO/IEC_27007

ISO/IEC 27001. (7 de 8 de 2022). *Sistema de Seguridad de la Información* .

ISOTools, E. (12 de 3 de 2023). *Dominios de Seguridad de la ISO-27001*. https://www.isotools.pe/ntp-iso-27001-dominios/#:~:text=Estos%20son%20los%20dominios%20incluidos,provisi%C3%B3n%20de%20bienes%20y%20servicios.

Martinez P. (2021). Norma de seguridad informática ISO 27001. Scielo. http://www.iso27000.es/download/Evaluacion_Riesgo_iso27001.pdf

Monserrate J. (2020). Buenas prácticas de seguridad informática aplicado al comercio electrónico para las Pymes colombianas asociada a la norma ISO 27001. UNAD.

Rodríguez B. (2019). Análisis y evaluación del riesgo de información: aplicación de la ISO 27001 . DEUSTO.

Santillán D. (2022). Consejos de implantación y métricas de ISO/IEC 27001 Y 27002 . ZAFIRO EBOOKS.

Terranova M. (2022). Esquema Nacional de Seguridad. Corrección de erratas. EDICIONES DESTINO. http://boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2010-4054.

Vera J. (2019). Information Systems Audit and Control Association (ISACA). MAXITUSQUETS. https://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Pages/default.aspx

Villegas M. (2021). Análisis de seguridad de la información basado en la norma ISO 27001 en el Área Técnica de Reparación e Instalación de la Corporación Nacional de Telecomunicaciones. Csielo.

Tabla 5. Información obtenida de la entrevistas

Entrevistado	**Jefe de sistemas**	**Desarrollador 1**	**Desarrollador 2**	**Administrador de Sistemas**	**Asistente de mantenimiento**
Pregunta **¿Se aplican políticas de seguridad para la información?** **Si…** **Enúncielas;** **No….¿Porqué?**	Existen políticas definidas así: • Como usuarios con sus respectivas contraseñas para poder acceder a la computadora y a los sistemas de información • Perfil de acceso de uso para los usuarios • Política para el uso de internet y de correo electrónico.	Si, como, por ejemplo: • Autorizaciones de Gerencia y de Administración • Autorización de recursos humanos (encargado de crear los roles y usuarios dependiendo de las funciones que desempeña) • Identificación del personal	Si: • Roles y acceso de usuarios. • Prioridad de usuarios. • Horarios de acceso.	Pues tenemos: • Creación de usuarios y roles dependiendo de las funciones. • El acceso a los servidores es restringido. • Restricciones del uso de flash memory	Contamos con: • Respaldos • Antivirus • Copias de Seguridad
¿De qué manera se realiza un control de la seguridad de la información?	Se realiza con: • Auditorías externas mediante un auditor informático que realiza estas tareas. Se cuenta con manualesde monitoreo para los jefes departamentales.	Se controla: Mediante módulos: Módulos de administración/seguridad/ usuarios/páginas/roles. Las páginas se relacionan con roles y los roles con los usuarios.	• Se asigna roles y controles de acuerdo a funciones de cada empleado Se cuenta con una bitácora de cambios de las funciones y desempeño de los empleados que registra el departamento de Recursos Humanos.	Mediante el uso de roles de cada usuario.	Mediante el uso de Check point, Firewall, IPTable de LINUX.

Entrevistado Pregunta	Jefe de sistemas	Desarrollador 1	Desarrollador 2	Administrador de Sistemas	Asistente de mantenimiento
¿Describa el control interno informático que se realiza en el Departamento de Sistemas?	El control se realiza: • Por el envió de respaldos de custodia externa (archivos logs) • Bitácora de visitas a sitios de internet • Control Biométrico • Custodio de claves para los sistemas.	En cuanto a Redes se hace mediante una red local y red inalámbrica, la red inalámbrica se gestiona con un AccesPoint y Chek Point. El acceso a la información es mediante contraseñas	Es –buena‖ ya que se maneja por contraseñasde acceso, subredes, la seguridad se define como una pequeña o mediana empresa.	Se basa en usuarios con sus respectivo roles y de igual forma el acceso a los sistemas de información es a base de contraseñas.	Controlando permanente con reglas de seguridad, actualizando a diario los servidores de antivirus.
¿Conoce usted acerca de un Sistema de Gestión de seguridad de la información (SGSI)?	Si, tales como: • Sistemas de encriptación de discos PGP • Active Directory • Sistemas de Password de una sola vez	No, la verdad solo de active directory nada mas	No, Pero conozco: • LDAP Microsoft (Active Directory) • OPENLDAP • Es un Control más granulad para acceder a la información • Tiene un nivel de seguridad elevado	No, tal vez conozca con otro nombre, pero no escuchado de un sistemas de gestión de seguridad de la información	Como el Check Point ya que por medio de este no se puede ingresar a páginas inseguras, ni los usuarios externos pueden ingresar a páginas institucionales. También es por el uso de IP TABLES

Entrevistado Pregunta	Jefe de sistemas	Desarrollador 1	Desarrollador 2	Administrador de Sistemas	Asistente de mantenimiento
¿Qué mecanismo, técnicas y/o herramientas de seguridad se aplican en los sistemas de información y de comunicación?	• Encriptación de claves de acceso. • Enlaces de comunicación encriptados • Políticas de acceso restringido al uso de flash memory • Asignación de permisos por usuarios y perfiles • Gestión de claves custodiadas por alto nivel.	Se usa un servidorfirewall con políticas establecidas por elmismo.	• Firewall de Check Point • Antivirus Anti Spam, Mallware anti hackers • Kaspersky Internet Security	• Check Point para seguridades • Software de Antivirus • Equipo de Linux enel que se realizafiltrado de URL	Roles y usuarios dependiendo de las funciones de cada usuario.
¿Se realiza control y administración de riesgos en cuanto a la seguridad de la información?	Si: • Mediante una unidad interna que se basa en la norma de BASILEA que asigna quienes van a ser designados para esta tarea. • Se realiza tareas de riesgos a base de eventos y de mejoras continuas	Si: Mediante la replicaciónde Base de Datos con tecnología RAID5	Si: Mediante un departamento de riesgos externo a este.	Si: Mediante un registro de los eventos sucedidos que informan los usuarios al departamento.	Dentro del sistema existe una página administración de riesgos puesto en vigilo por el administrador.

Entrevistado Pregunta	Jefe de sistemas	Desarrollador 1	Desarrollador 2	Administrador de Sistemas	Asistente de mantenimiento
¿Se realizan tareas de monitoreo a los sistemas de información y de comunicación?	Si: • En los enlaces de comunicación • Trafico de red • Desempeño de servidores.	Si se lo realiza mediante la aplicación MRTG	Se lo realiza mediante sistemas que notifican cuando hay ataques	Básicamente se realiza por la revisión de logs. Los sistemas de comunicación cuentancon una aplicación web que informa los enlaces principales, además la aplicación MRTG.	Si: Se realiza todos los días para tener la conectividad con todas las oficinas y para reducir un margen de error de la conectividad.
¿Han realizado simulacros frente a la caída de los sistemas de información y de comunicación? Si…. De qué manera se lo ha realizado; No…. ¿Por qué?	Si: • Mediante un plan de contingencia • Simulacro de pérdida de enlace de datos • Pruebas de pérdidade energía eléctrica • Daños en los servidores de Base de Datos y de Aplicativos.	Se lo realiza mediante la utilización de un servidores de respaldos de Base de Datos	Si ha hecho uno cortando los sistemas de red esto se ha realizado junto con el auditor informático y el departamento de riesgos	Si se lo realiza ya que se dispone de un plan de contingencia del área.	Si he escuchado de eso, que lo han realizado, pero no he participado en ese simulacro

Elaborado por la autora.

Anexo 2: Ruc de la empresa

Consulta de RUC

RUC
1291735947001

Razón social
COMPAÑIA DE TRANSPORTE PESADO 17 DE NOVIEMBRE S.A.

Estado contribuyente en el RUC
ACTIVO

Representante legal

Nombre/Razón Social:	BONIFAS LOZANO PATRICIA
Identificación:	0601516834

Contribuyente fantasma	NO	**Contribuyente con transacciones inexistentes**	NO

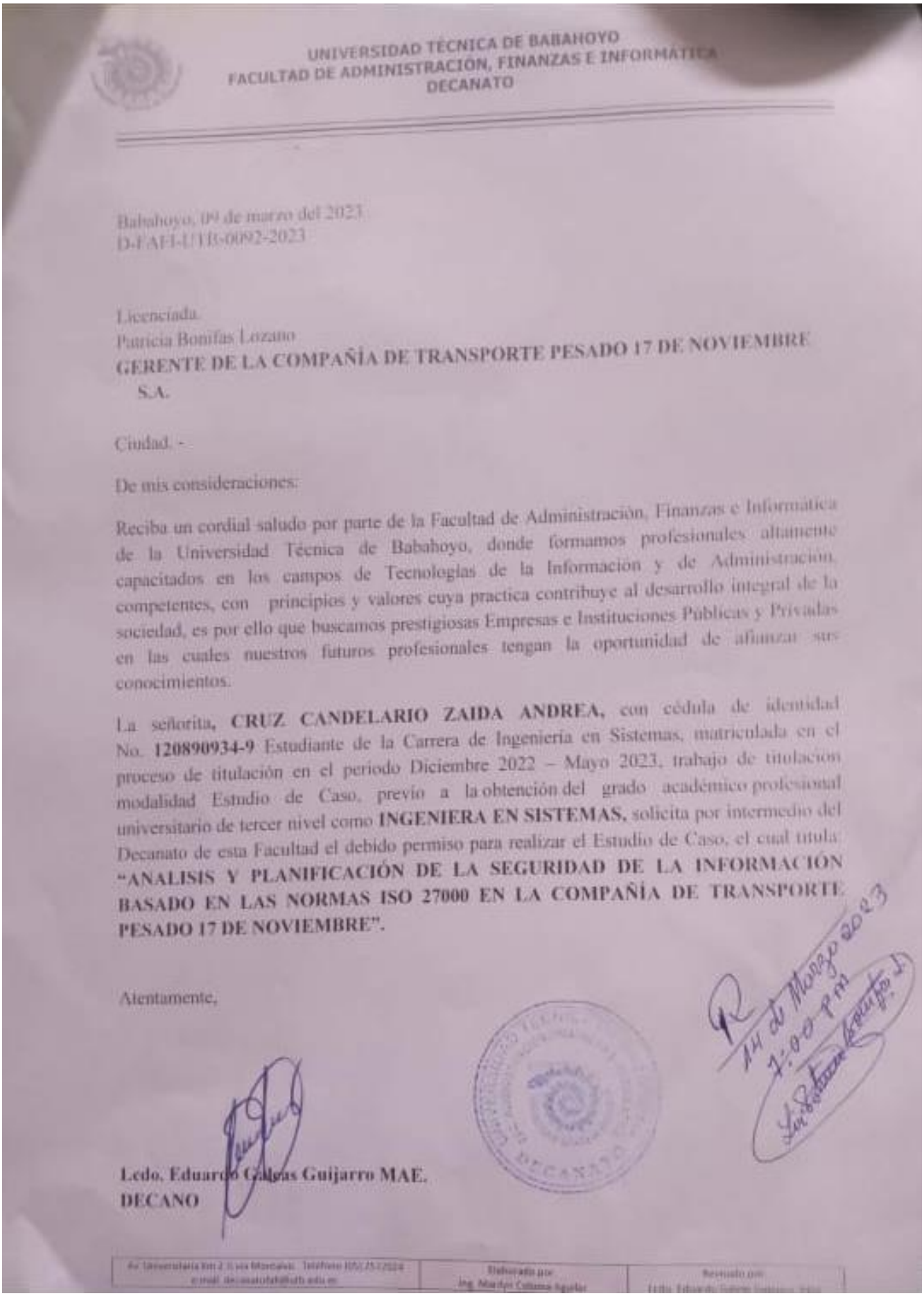
Actividad económica principal	TODAS LAS ACTIVIDADES DE TRANSPORTE DE CARGA POR CARRETERA, INCLUIDO EN CAMIONETAS DE: TRONCOS, GANADO, TRANSPORTE REFRIGERADO, CARGA PESADA, CARGA A GRANEL, INCLUIDO EL TRANSPORTE EN CAMIONES CISTERNA, AUTOMÓVILES, DESPERDICIOS Y MATERIALES DE DESECHO, SIN RECOGIDA NI ELIMINACIÓN.

Tipo contribuyente	Régimen	Categoría
SOCIEDAD	GENERAL	

Obligado a llevar contabilidad	Agente de retención	Contribuyente especial
SI	NO	NO

Fecha inicio actividades	Fecha actualización	Fecha cese actividades	Fecha reinicio actividades
2009-07-28	2021-07-19		

Anexo 3: Carta de autorización



UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
DECANATO

Babahoyo, 09 de marzo del 2023
D-FAFI-UTB-0092-2023

Licenciada.
Patricia Bonifas Lozano
GERENTE DE LA COMPAÑÍA DE TRANSPORTE PESADO 17 DE NOVIEMBRE S.A.

Ciudad. -

De mis consideraciones:

Reciba un cordial saludo por parte de la Facultad de Administración, Finanzas e Informática de la Universidad Técnica de Babahoyo, donde formamos profesionales altamente capacitados en los campos de Tecnologías de la Información y de Administración, competentes, con principios y valores cuya practica contribuye al desarrollo integral de la sociedad, es por ello que buscamos prestigiosas Empresas e Instituciones Públicas y Privadas en las cuales nuestros futuros profesionales tengan la oportunidad de afianzar sus conocimientos.

La señorita, **CRUZ CANDELARIO ZAIDA ANDREA,** con cédula de identidad No. **120890934-9** Estudiante de la Carrera de Ingeniería en Sistemas, matriculada en el proceso de titulación en el periodo Diciembre 2022 – Mayo 2023, trabajo de titulación modalidad Estudio de Caso, previo a la obtención del grado académico profesional universitario de tercer nivel como **INGENIERA EN SISTEMAS,** solicita por intermedio del Decanato de esta Facultad el debido permiso para realizar el Estudio de Caso, el cual titula: **"ANALISIS Y PLANIFICACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NORMAS ISO 27000 EN LA COMPAÑÍA DE TRANSPORTE PESADO 17 DE NOVIEMBRE".**

Atentamente,

14 de Marzo 2023
1:00 pm

Lcdo. Eduardo Galeas Guijarro MAE.
DECANO

Av. Universitaria Km 2 ½ vía Montalvo. Teléfono 052-372024
e-mail: decanatofafi@utb.edu.ec

Elaborado por:
Ing. Marlon Cabrera Aguilar

Revisado por:
Lcdo. Eduardo Galeas Guijarro, MAE