RESUMEN – TRABAJO DE GRADO

AUTORES	WILLIGTON SANJUÁN MUÑOZ
FACULTAD	DE INGENIERIAS
PLAN DE ESTUDIOS	INGENIERIA DE SISTEMAS
DIRECTOR	JESSICA LORENA GAONA CÁCERES
TÍTULO DE LA TESIS	EVALUACION DE LA SEGURIDAD EN LA INFORMACIÓN PARA LA TERMINAL DE TRANSPORTES DE LA CIUDAD DE OCAÑA NORTE DE SANTANDER, BASADOS EN LA NORMA ISO/IEC 27001

RESUMEN

(70 PALABRAS APROXIMADAMENTE)

LOS ACTIVOS DE INFORMACIÓN HAN PASADO A FORMAR PARTE DE LA ACTIVIDAD COTIDIANA DE ORGANIZACIONES E INDIVIDUOS; LOS EQUIPOS DE CÓMPUTO ALMACENAN INFORMACIÓN, LA PROCESAN Y LA TRANSMITEN A TRAVÉS DE REDES Y CANALES DE COMUNICACIÓN, ABRIENDO NUEVAS POSIBILIDADES Y FACILIDADES A LOS USUARIOS, PERO SE DEBEN CONSIDERAR NUEVOS PARADIGMAS EN ESTOS MODELOS TECNOLÓGICOS Y TENER MUY CLARO QUE NO EXISTEN SISTEMAS CIEN POR CIENTO SEGUROS, PORQUE EL COSTO DE LA SEGURIDAD TOTAL.

CARACTERÍSTICAS

PÁGINAS: 78	PLANOS: 0	ILUSTRACIONES: 0	CD-ROM: 1

EVALUACION DE LA SEGURIDAD EN LA INFORMACIÓN PARA LA TERMINAL DE TRANSPORTES DE LA CIUDAD DE OCAÑA NORTE DE SANTANDER, BASADOS EN LA NORMA ISO/IEC 27001

AUTOR:

WILLIGTON SANJUÁN MUÑOZ

Trabajo de grado para Optar el título de Especialista en Auditoria de Sistemas

Directora:

JESSICA LORENA GAONA CÁCERES

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERIAS

ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS

Ocaña, Colombia Febrero de 2017

Dedicatoria

Dedico esta tesis a DIOS, a mis padres quienes me dieron vida, educación, apoyo y consejos, a mis maestros, amigos, y a TI; quienes sin su ayuda nunca hubieran podido hacer esta tesis. A todos ellos se los agradezco desde el fondo de mi corazón. Para todos ellos hago esta dedicatoria.

Agradecimientos

El autor expresa sus más sinceros agradecimientos a la directora del trabajo de grado Esp. JESSICA LORENA GAONA CACERES, por su guía, orientación y colaboración para este objetivo, de igual forma a mi familia, amigos y personas especiales en mi vida; no son nada más y nada menos que un solo conjunto. Este nuevo logro es en gran parte gracias a ustedes, porque he logrado concluir con éxito un nuevo proyecto.

Muchas gracias a aquellos seres queridos que siempre guardo en mi corazón.

Índice

Resumen

Hoy en día los sistemas de información son el alma de las organizaciones, empresas y entidades, el grado de responsabilidad reposa en los sistemas, datos e información encaminados al logro de los objetivos internos, estos se pueden mejorar y mantener teniendo una adecuada sistematización y documentación.

Es por esto que los activos de información han pasado a formar parte de la actividad cotidiana de organizaciones e individuos; los equipos de cómputo almacenan información, la procesan y la transmiten a través de redes y canales de comunicación, abriendo nuevas posibilidades y facilidades a los usuarios, pero se deben considerar nuevos paradigmas en estos modelos tecnológicos y tener muy claro que no existen sistemas cien por ciento seguros, porque el costo de la seguridad total es muy alto (aunque en la realidad no es alcanzable idealmente), y las organizaciones no están preparadas para hacer este tipo de inversión (Perafán Ruiz, 2014).

Introducción

El tratamiento de la información abarca aspectos que van desde el manejo de documentos en medio físico como el proceso de almacenaje y recuperación conocido también como proceso de gestión documental, hasta los sistemas de información que tenga la organización o sistemas externos a los que esté obligada a reportar información, pasando por aspectos tan importantes como la forma de almacenamiento de los datos digitales, modelos de respaldo de información y planes de contingencia o de continuidad del negocio, si existen, claro está, incluyendo además los sistemas físicos de protección y accesibilidad a sitios o áreas restringidas (Perafán Ruiz, 2014).

Para lo anterior se realizó un marco referencial que está compuesto del marco histórico, conceptual, teórico, legal y contextual, al igual que el diseño metodológico, con su población, técnicas y procesamiento de información, lo que arrojo conclusiones y recomendaciones. Por último el análisis de riesgo permite realizar un diagnóstico para conocer las debilidades y fortalezas internas encaminadas en la generación de los controles adecuados y normalizados dentro de las políticas de seguridad informática que hacen parte de un Sistema de Gestión de Seguridad de la Información.

Capítulo 1. Evaluación de la seguridad en la información para la Terminal de Transportes de la Ciudad de Ocaña, Norte de Santander, basados en la norma ISO/IEC 27001

1.1 Planteamiento del problema.

La información es un activo valioso que puede impulsar o destruir su empresa. Si se gestiona de forma adecuada, le permite trabajar con confianza. La gestión de la Seguridad de la Información le ofrece la libertad para crecer, innovar y ampliar su base de clientes sabiendo que toda su información confidencial seguirá siéndolo. De igual forma los Sistemas de Gestión de Seguridad de la Información (SGSI) son el medio más eficaz de minimizar los riesgos, al asegurar que se identifican y valoran los activos y sus riesgos, considerando el impacto para la organización, y se adoptan los controles y procedimientos más eficaces y coherentes con la estrategia de negocio. (BSI, 2016)

Teniendo en cuenta lo anterior se debe decir que en la ciudad de Ocaña, desde el año 1993, se empezó a construir la terminal de transportes con el objeto de prestar servicios públicos y todas sus actividades mediante una unidad de servicio permanente y de equipo e instalaciones y organización administrativa que concentrará la oferta y la demanda del transporte automotor de pasajeros, regulándolas en beneficio de los usuarios para la seguridad y comodidad de los mismo, además contribuir a la solución del problema de la actividad transportadora para efectos

socio-urbanísticos y en el mejoramiento del servicio mediante la construcción y explotación de una terminal de transporte de pasajeros en el municipio de Ocaña y su provincia.

Esta entidad desde la fecha de su creación no ha contado con un sistema de seguridad en la información manejada al interior, que permita la gestión de vulnerabilidades, riesgos y amenazas a las que normalmente se ve expuesta la información presente en cada uno de los procesos internos, de igual forma no se tienen estandarizados controles que lleven a mitigar delitos informático o amenaza a los que están expuestos los datos comprometiendo la integridad, confidencialidad y disponibilidad de la información.

También se debe decir que en la terminal se han evidenciado inconvenientes en el manejo de la información debido a que la entidad ha ido creciendo a pasos agigantados y no se ha tomado conciencia por parte de los directivos, de la importancia de asegurar la información existente; siendo para esto indispensable realizar un análisis de riesgos de la seguridad de la información, como también hacer recomendaciones de la seguridad que se debe empezar a implementar en la entidad.

1.2 Formulación del problema.

¿Qué beneficios puede traer a la Terminal de Transportes, la identificación de riesgos y amenazas en la seguridad de la información?

1.3 Objetivos.

1.3.1 General. Evaluar la seguridad en la información para la Terminal de Transportes de la Ciudad de Ocaña, Norte de Santander, basados en la norma ISO/IEC 27001

1.3.2 Específicos. Identificar los dominios de la norma ISO 27001, más pertinentes para la Terminal de Trasportes de la ciudad de Ocaña.

Proponer una metodología de evaluación de riesgos que permita definir las vulnerabilidades y amenazas de seguridad existentes, en la Terminal de Transportes de Ocaña, Norte de Santander.

Sugerir mecanismos de control y gestión que minimicen las vulnerabilidades encontradas en el estudio del análisis de riesgos realizado.

Elaborar un informe de recomendaciones donde se muestre los hallazgos que permita definir un Sistema de seguridad de la información ajustada a la realidad de la Terminal.

1.4 Justificación.

El Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001 ofrece la protección ante cualquier amenaza que pueda poner en peligro a las organizaciones, tanto públicas como privadas, por el contrario podrían realizarse algún daño para la salud empresarial. La realidad nos ofrece que las empresas se enfrentan diariamente a un enorme número de riesgos e inseguridad que proviene de una elevada variedad de fuentes diferentes,

entra las que se pueden entrar los nuevos negocios y nuevas herramientas relacionadas con la tecnología de la información y la comunicación, que los directores generales y los directores informáticos de la organización deben aplicar. (Blog especializado en sisetma de gestion de seguridad de la información, 2015)

Todas las herramientas se tiene que aplicar según los diferentes objetivos que tengan fijados las organizaciones con la mayor seguridad, y garantizando la confidencialidad, integridad y disponibilidad. Para poder proteger la información se tiene que realizar la implementación, el mantenimiento y la mejora de las medidas de seguridad para que cualquier tipo de organización consiga sus objetivos y además garantice que cumple con la legislación, aumentando el prestigio y la imagen de la compañía. (Blog especializado en sisetma de gestion de seguridad de la información, 2015)

Teniendo en cuenta la importancia de la seguridad en la información de las empresas, se debe decir que sin importar la actividad económica a la que se dedica, debe considerar planes para el aseguramiento de la información, generando políticas y controles bien sea en busca de garantizar la continuidad del negocio o de una certificación como carta de presentación y de distinción ante la competencia. La Terminal de Transportes de Ocaña, Norte de Santander, debe tomar conciencia de la necesidad de alinear sus objetivos institucionales, asegurar el flujo de información, optimizar recursos y garantizar la confidencialidad, disponibilidad e integridad de la misma.

Este es uno de los retos que debe asumir los directivos de la entidad con la asesoría del gerente, para estar acorde a los modelos y estándares actuales; para ello es necesario empezar con la ejecución del análisis de riesgos de la seguridad de la información que en un futuro será la base para implementar el sistema de gestión de seguridad de la información (SGSI), que permitirá mantener un modelo de negocio estable logrando un valor agregado y posicionamiento a nivel local, regional, nacional e internacional.

Por último se debe tener un análisis de riesgos en la Terminal de Transportes, con el objetivo de garantizar una mayor efectividad y eficiencia dentro de cada uno de los procesos; teniendo en cuenta que al conocer las fortalezas y debilidades se mejora el control y administración de recursos tecnológicos acorde a las directrices nacionales e internacionales que buscan proporcionar mecanismos y herramientas para adoptar buenas prácticas de seguridad y que de esta forma se logren los objetivos propuestos en la entidad.

1.5 Delimitaciones.

1.5.1 Geográfica. El desarrollo del trabajo de grado se llevará a cabo en la ciudad de Ocaña, Norte de Santander, específicamente en la Terminal de Transportes, ubicado en la Circunvalar.

1.5.2 Temporal. El proyecto de grado se realizara en cuatro (4) meses, de acuerdo a las diferentes actividades a realizar durante el desarrollo del mismo.

1.5.3 Conceptual. Los conceptos pertenecientes al área de conocimiento de este proyecto se relacionan con la Seguridad de la Información, Sistema de Gestión de Seguridad de la Información (SGSI), Riesgos, transporte, información, vulnerabilidad, amenazas, entre otros.

1.5.4 Operativa. Los inconvenientes que se pueden presentar a lo largo del trabajo de grado, pueden ser la falta de tiempo, poca información acerca del tema que se trabaja, veracidad de la información, problemas climáticos (lluvia), entre otros.

Capítulo 2. Marco referencial

2.1 Marco histórico.

2.1.1 Antecedentes de la seguridad en la información en el mundo. La estandarización Internacional comenzó en el campo electrotécnico: la Comisión Electrotécnica Internacional (IEC) fue establecida en 1906. Iniciando el trabajo en otros campos fue realizado por la Federación Internacional de la Organización Estandarizadora Nacional (ISA), que fue instalada en 1926. El énfasis dentro de ISA fue puesto pesadamente en la ingeniería industrial. Las actividades de ISA acabaron en 1942. En 1946, delegados de 25 países se reunieron en Londres y decidieron crear una nueva organización internacional, de la cual el objeto sería "facilitar la coordinación y la unificación internacional de estándares industriales". La nueva organización, ISO, comenzó oficialmente operaciones el 23 de febrero de 1947. (Castro Toro, 2010)

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution, la organización británica equivalente a AENOR en España) es responsable de la publicación de importantes normas como:

1979 Publicación BS 5750 - ahora ISO 9001

1992 Publicación BS 7750 - ahora ISO 14001

1996 Publicación BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa , británica o no, un conjunto de buenas prácticas para la gestión de la seguridad de su información. (Castro Toro, 2010)

La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente. Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000. (Castro Toro, 2010)

ISO/IEC 17799 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

La versión de 2005 del estándar incluye las siguientes once secciones principales:

1. Política de Seguridad de la Información.
2. Organización de la Seguridad de la Información.
3. Gestión de Activos de Información.
4. Seguridad de los Recursos Humanos.
5. Seguridad Física y Ambiental.
6. Gestión de las Comunicaciones y Operaciones.
7. Control de Accesos.
8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
9. Gestión de Incidentes en la Seguridad de la Información.
10. Gestión de Continuidad del Negocio.
11. Cumplimiento.

En toda organización que haga uso de las tecnologías de información se recomienda implementar buenas prácticas de seguridad, pues en muchas ocasiones el no seguir un proceso de implementación adecuado como el que establece el ISO 17799 puede generar huecos por la misma complejidad de las organizaciones, en ese sentido, aumenta la posibilidad de riesgos en la información. El objetivo de la seguridad de los datos es asegurar la continuidad de las operaciones de la organización, reducir al mínimo los daños causados por una contingencia, así como optimizar la inversión en tecnologías de seguridad. (Castro Toro, 2010)

Como todo buen estándar, el ISO 17799 da la pauta en la definición sobre cuáles metodologías, normas o estándares técnicos pueden ser aplicados en el sistema de administración de la seguridad de la información, se puede entender que estos estándares son auxiliares y serán aplicados en algún momento al implementar el mismo. La aplicación de un marco de referencia de seguridad basado en el ISO 17799 proporciona beneficios a toda organización que lo implemente, al garantizar la existencia de una serie de procesos que permiten evaluar, mantener y administrar la seguridad de la información. (Castro Toro, 2010)

Las políticas, estándares locales y los procedimientos se encuentran adaptados a las necesidades de la organización debido a que el proceso mismo de su elaboración integra mecanismos de control y por último, la certificación permite a las organizaciones demostrar el estado de la seguridad de la información, situación que resulta muy importante en aquellos convenios o contratos con terceras organizaciones que establecen como requisito contractual la certificación BS7799. (Castro Toro, 2010)

Es importante entender los principios y objetivos que dan vida al ISO 17799, así como los beneficios que cualquier organización, incluyendo las instituciones públicas, privadas y ambientes educativos pueden adquirir al implementarlo en sus prácticas de seguridad de la información. Cada una de las áreas establece una serie de controles que serán seleccionados dependiendo de los resultados obtenidos en el análisis de riesgos, además, existen controles obligatorios para toda organización, como es el de las políticas de seguridad cuyo número dependerá más de la organización que del estándar, el cual no establece este nivel de detalle. ISO 27000. (Castro Toro, 2010)

Con el Modelo de Seguridad para las entidades del Estado, el Ministerio TIC entrega una guía para que puedan construir su Sistema de Gestión de Seguridad de la Información (SGSI). Se busca generar una conciencia colectiva sobre la importancia de clasificar, valorar y asegurar los activos de cada entidad. (Ministerio de las TICs, 2016)

Por eso mismo, el Ministerio TIC está profundizando en elementos que permitan entender la realidad frente al proceso de implementación de SGSI en el Estado. Se debe forjar una línea base sobre cuáles son los motivadores, inhibidores, actores, resultados, entre otros aspectos, que cada entidad afronta en el camino hacia la seguridad de la información. Para tal fin, se ha contratado un estudio para "conocer cuál es el estado actual de adopción y apropiación de los SGSI en las entidades del Estado, del orden nacional y territorial". (Ministerio de las TICs, 2016)

Entre las conclusiones de dicho estudio se encuentra que:

"El proyecto de creación de un Sistema de Gestión de Seguridad de la Información, comienza generalmente por el área de TI.

La mayoría plantea un alcance inicial que incluye mínimo el área de TI y los sistemas de información de la entidad.

Las razones para este tipo de alcance inicial son: practicidad y recursos".

Solo con la puesta en marcha del proyecto de adopción las entidades reconocen la importancia práctica del tema, la diferencia real entre SI y seguridad informática, hasta dónde pueden llegar en corto plazo y hasta dónde les gustaría llegar.

Las entidades son conscientes que el tema no sólo abarca el aseguramiento con software y hardware, si no que en gran medida el resultado exitoso se refleja en la sensibilización y compromiso del personal para cumplir cada política, conociendo el porqué de cada una. (Ministerio de las TICs, 2016)

En Colombia, por parte del Ministerio de las Tecnologías de la Información y la Comunicación, dentro de sus objetivos de desarrollo 2011- 2014 ha planteado el impulso a la masificación y uso eficiente de las TIC para el cumplimiento de los objetivos del Gobierno Nacional de: disminuir pobreza, aumentar seguridad y aumentar empleo. Bajo esa concepción se ha hecho necesario también la capacitación en temas relacionados con la seguridad de la información de acuerdo a lo planteado en el documento CONPES 3701 por parte del Departamento Nacional de Planeación: "Solicitar al Ministerio de Tecnologías de la Información y las Comunicaciones realizar las gestiones necesarias con el Ministerio de Educación Nacional y el SENA, para la generación de un plan de capacitación para el sector

privado en temas de ciberseguridad y de seguridad de la información.” (Ministerio de tecnologia de la infromación y la comunicación, 2012)

El documento CONPES tiene como objetivo central fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio. (Ministerio de tecnologia de la infromación y la comunicación, 2012)

2.2 Marco conceptual.

Seguridad de la Información. La seguridad informática, también conocida como ciberseguridad o seguridad de tecnologías de la información, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada. (Sanso, 2011)

De otra parte la seguridad en un ambiente de red es la habilidad de identificar y eliminar vulnerabilidades. Una definición general de seguridad debe también poner atención a la necesidad de salvaguardar la ventaja organizacional, incluyendo información y equipos físicos,

tales como los mismos computadores. Nadie a cargo de seguridad debe determinar quién y cuándo puede tomar acciones apropiadas sobre un ítem en específico. Cuando se trata de la seguridad de una compañía, lo que es apropiado varía de organización en organización. Independientemente, cualquier compañía con una red debe tener una política de seguridad que se dirija a la conveniencia y la coordinación. (Sanso, 2011)

Sistema de Gestión de Seguridad de la Información (SGSI). SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.
En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración. (Vargas, 2016)

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:
Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran. Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI. (Vargas, 2016)

Riesgos. El riesgo es aquello que puede acontecer en un futuro, más o menos cercano, y que preocupa por sus consecuencias porque está siempre presente en cualquier actividad que se realice. Pero no sólo tiene una vertiente negativa, relacionada con pérdidas económicas o daños físicos, o morales; también puede entenderse desde su lado positivo cuando la exposición a determinados riesgos permite obtener ganancias (por ejemplo, al arriesgar en una apuesta para ganar dinero, o al invertir en un determinado negocio para conseguir unos beneficios futuros).

El seguro actúa en cualquiera de estas dos perspectivas, interviniendo como una de las respuestas más efectivas frente a las consecuencias de los riesgos y como forma de garantía ante situaciones futuras previstas en la vida de las personas. (Seguros y pensiones para todos, 2016)

Transporte. El transporte es una actividad del sector terciario, entendida como el desplazamiento de objetos, animales o personas de un lugar (punto de origen) a otro (punto de destino) en un vehículo (medio o sistema de transporte) que utiliza una determinada infraestructura (red de transporte). Esta ha sido una de las actividades terciarias que mayor expansión ha experimentado a lo largo de los últimos dos siglos, debido a la industrialización; al

aumento del comercio y de los desplazamientos humanos tanto a escala nacional como internacional; y los avances técnicos que se han producido y que han repercutido en una mayor rapidez, capacidad, seguridad y menor coste de los transportes.

Vulnerabilidad. En este contexto, la vulnerabilidad puede definirse como la capacidad disminuida de una persona o un grupo de personas para anticiparse, hacer frente y resistir a los efectos de un peligro natural o causado por la actividad humana, y para recuperarse de los mismos. Es un concepto relativo y dinámico. La vulnerabilidad casi siempre se asocia con la pobreza, pero también son vulnerables las personas que viven en aislamiento, inseguridad e indefensión ante riesgos, traumas o presiones. (Federación Internacional de Sociedades de la Cruz Roja, 2010)

Amenazas. Una amenaza es un fenómeno o proceso natural o causado por el ser humano que puede poner en peligro a un grupo de personas, sus cosas y su ambiente, cuando no son precavidos. Existen diferentes tipos de amenazas. Algunas son naturales, otras son provocadas por el ser humano, como las llamadas industriales o tecnológicas (explosiones, incendios y derrames de sustancias tóxicas). Las guerras y el terrorismo también son amenazas creadas por el ser humano. (Unisdr, 2004)

2.3 Marco teórico

La norma ISO 17799 es un código de buenas prácticas para la Gestión de la Seguridad de la Información, esta norma surge como evolución histórica de la norma británica BS 7799 y actualmente existen varias adaptaciones de la misma que convergerán en un futuro próximo a las

normas de la serie ISO 27000. La ISO 17799 introduce un cambio importante en los sistemas de gestión de la seguridad de la información ya que los aborda desde un punto de vista de continuidad de negocio y de mejora continua. Esta norma hereda muchos conceptos de la serie de normas ISO 9000 y subraya la seguridad entendida como proceso. (Villalon Huertas, 2016)

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO e IEC que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña; Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044. (Villalon Huertas, 2016)

2.4 marco contextual.

En el país son dos los hechos más relevantes:

El Primero: nuestro ineficiente sistema de transporte se soporta en el medio carretero a pesar de poseer dos valles interandinos, el del río Magdalena y el del río Cauca, que ofrecen en su orden posibilidades más económicas para el transporte fluvial y ferroviario.

El flete por tonelada / km a lo largo del río Magdalena entre Honda y Barranquilla, dos lugares separados unos 900 km, en Tractomula cuesta U$0,12, mientras por FFCC cuesta entre U$0,03 y U$0,04, y por agua utilizando botes de 80 TEUS costaría menos de U$0,02.
El Segundo: el país nunca ha tenido visión marítima a pesar de poseer dos océanos y de estar ubicado en la mejor esquina de América.

A pesar de las ventajas comparativas asociadas a esa posición geoestratégica y a la riqueza marítima, perdimos a Panamá, nos mantuvimos con los mismos puertos de siempre. Por

eso sin advertir que había llegado la era de los contenedores, vimos desaparecer nuestra Flota Mercante Gran colombiana creada en 1946, que sin los efectos de la competencia mantuvo en su medio siglo de existencia su política de utilidades basada en altos precios y bajos niveles de calidad.

Transporte carretero colombiano. Los vehículos para el parque automotor de carga, son el 56% privados y el 44% públicos. Los camiones rígidos de 2 ejes (C2) y las tractomulas (C3S), configuran el 90% de la capacidad ofrecida, con similar participación. El servicio particular ofrece el 25% de la capacidad instalada, y el público el 75% restante. En cuanto a la demanda, el sector manufacturero ocupa un 51%, el agropecuario un 31% y el minero un 18% restante. Las exportaciones son el 10% de esta demanda. Por generación de carga, el occidente colombiano con el Valle al frente genera el 31%, el eje Santander Cundinamarca Tolima, el 30% con Bogotá a la cabeza, y la Costa Atlántica el 17% con Barranquilla en primer lugar. (Bosca & M.J, 2004)

De otra parte se puede decir que la ciudad de Ocaña cuenta con el Aeropuerto Aguas Claras y la Terminal de Transportes; ambos de servicio nacional. El aeropuerto está ubicado a 9 kilómetros al noroeste de la ciudad. Actualmente cubren rutas aéreas con vuelos charter de empresas privadas con destino a las ciudades de Cúcuta, Bogotá y Bucaramanga. (Paez Garcia, 2009)

2.5 Marco legal.

Ley 1266 del 31 de diciembre de 2008. El Congreso de Colombia decretó: "Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones." (Congreso de Colombia, 2015)

Artículo 71 de la Constitución Política de Colombia. Este artículo otorga al Estado la responsabilidad de promover el desarrollo tecnológico e incentivar a quienes se dediquen a trabajar en este ámbito "… El Estado creará incentivos para personas e instituciones que desarrollen y fomenten la ciencia y la tecnología y las demás manifestaciones culturales y ofrecerá estímulos especiales a personas e instituciones que ejerzan estas actividades." (República de Colombia, 2012)

Es de gran importancia lo que se acaba de mencionar puesto que es precisamente la Constitución Política que estando por encima de todas las leyes, ampara la actividad de desarrollo tecnológico.

Ley 1273 del 5 de enero de 2009. El Congreso de Colombia decretó: "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones."

(Congreso de Colombia, http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf, 2015)

Ley 1581 del 17 de octubre de 2012. El Congreso de Colombia decretó que esta ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política de Colombia; así como el derecho a la información consagrado en el artículo 20 de la misma. (República de Colombia, Ley 1581 de 2012, 2012)

Capítulo 3. Diseño metodológico

3.1 Tipo de investigación.

La investigación cualitativa o metodología cualitativa es un método de investigación usado principalmente en las ciencias sociales que se basa en cortes metodológicos basados en principios teóricos tales como la fenomenología, hernenéutica, la interacción social empleando métodos de recolección de datos que son no cuantitativos, con el propósito de explorar las relaciones sociales y describir la realidad tal como la experimentan los correspondientes.

La investigación cualitativa requiere un profundo entendimiento del comportamiento humano y las razones que lo gobiernan. A diferencia de la investigación cuantitativa, la investigación cualitativa busca explicar las razones de los diferentes aspectos de tal comportamiento. En otras palabras, investiga el por qué y el cómo se tomó una decisión, en contraste con la investigación cuantitativa la cual busca responder preguntas tales como cuál, dónde, cuándo. La investigación cualitativa se basa en la toma de muestras pequeñas, esto es la observación de grupos de población reducidos, como salas de clase, etc.

3.2 Población y muestra.

En cuanto a la población objeto de estudio se tuvo como población cinco funcionarios, los cuales tienen una directa relación con la información manejada al interior de la Terminal de Transportes, de igual forma por ser tan reducida la población se tomó en su totalidad y estos aportaron los datos necesarios para realizar el proyecto.

3.3 Técnicas para la recolección de la información.

Como técnica de indagación directa se utilizó la observación documental siendo el más viable para el desarrollo de los objetivos y el instrumento de recolección de información más importante que consiste en el registro sistemático, válido y confiable de comportamientos o conducta manifiesta.

3.4 Procesamiento de la información recolectada.

Teniendo en cuenta la información recolectada esta fue presentada de forma cualitativa describiendo cada uno de los aspectos relevantes para la investigación y desarrollo de los objetivos.

Capítulo 4. Presentación de resultados

4.1 Dominios de la norma ISO 27001, más pertinentes para la Terminal de Trasportes de la ciudad de Ocaña.

En la Terminal de Transporte de Ocaña, los dominios no están centrados en los aspectos tecnológicos y organizativos de la gestión de la seguridad, la actividad de la empresa solo ha estado centrada en el transporte y se ha olvidado la importancia de proteger la información, y de la Norma ISO 27001, al igual que sus objetivos, los cuales son:

La definición clara y transmitida a toda la organización de los objetivos y directrices de seguridad.

La sistematización, objetividad y consistencia a lo largo del tiempo en las actuaciones de seguridad.

El análisis y prevención de los riesgos en los Sistemas de Información.

La mejora de los procesos y procedimientos de gestión de la información.

La motivación del personal en cuanto a valoración de la información.

El cumplimiento con la legislación vigente.

Una imagen de calidad frente a clientes y proveedores.

De otra parte estos dominios traen beneficios como son demostrar la garantía independiente de los controles internos y cumplir los requisitos de gestión corporativa y de continuidad de la actividad comercial, demostrar independencia frente a las leyes y normativas que sean de aplicación, proporcionar una ventaja competitiva al cumplir los requisitos

contractuales y demostrar a los clientes que la seguridad de su información es primordial, verificar independientemente que los riesgos de la organización estén correctamente identificados, evaluados y gestionados al tiempo que formaliza unos procesos, procedimientos y documentación de protección de la información, demuestra el compromiso de la cúpula directiva de su organización con la seguridad de la información, el proceso de evaluaciones periódicas ayuda a supervisar continuamente el rendimiento y la mejora.

Para que la Terminal de Transportes de la ciudad de Ocaña, Norte de Santander, logre el pleno dominio de la información tiene que llevar a cabo la implentación de un Sistema de Gestión para la Seguridad de la Información de la mano de ISO 27001.

La norma ISO 27001 ofrece a las organizaciones una guía para su implementación, ayudándolas a controlar y evaluar su exposición ante los posibles riesgos de la información a través del empleo de controles para paliarlos, y así, conseguir un sistema de información integrado, confidencial y disponible de los activos de la información.

Dicha norma tiene como objetivo la salvaguardia de la información de una organización impidiendo que ésta se pierda, proporcionando la certeza a las mismas de la continuidad de los servicios prestados en situaciones de riesgo. Los objetivos contemplados en la norma ISO27001 de los dominios de la información a valuar se muestran de forma resumida a continuación:

La norma desarrolla 11 áreas o dominios que recogen los 133 controles, siendo estos los siguientes:

4.1.1 Política de seguridad. La norma ISO 27001 requiere que la Política de gestión de la seguridad de la información (SGSI), al ser el documento más importante, contenga lo siguiente: el marco para establecer objetivos, tomando en cuenta los diferentes requisitos y obligaciones, la alineación con la realidad de la organización respecto de la gestión estratégica del riesgo y el establecimiento de criterios de evaluación. Una política de estas características, en realidad, debería ser muy corta (tal vez una o dos páginas) porque tiene como objetivo principal que la alta gerencia puede controlar su SGSI.

Por otro lado, las políticas detalladas deben estar orientadas al uso operativo y enfocadas en un campo más acotado de actividades de seguridad. Algunos ejemplos de este tipo de políticas son: Política de clasificación, Política sobre el uso aceptado de los activos de información, Política de creación de copias de seguridad, Política de control de acceso, Política de contraseñas, Política de escritorio y pantalla despejados, Política de uso de redes, Política sobre equipos móviles, Política sobre el uso de controles criptográficos, etc. Nota: la norma ISO 27001 no requiere la implementación ni la documentación de todas estas políticas porque la decisión de si corresponden dichos controles, y con qué alcance, depende de los resultados de la evaluación de riesgos.

4.1.2 Aspectos administrativos. Este dominio se refiere a la asignación de responsabilidades relativas a la seguridad de la información, donde se encuentra el proceso de autorización de recursos

para el tratamiento de la información, los acuerdos de confidencialidad, el manejo de los grupos de interés y la revisión independiente de la seguridad de la información. Además los aspectos que se tienen que tener en cuenta con el manejo de terceros como la identificación de los riesgos derivados del acceso de terceros y la seguridad en contratos con terceros.

4.1.3 Gestión de activos. Este segundo dominio contempla los lineamientos para la gestión de activos que incluye el inventario y las declaraciones de uso de los mismos. Como parte de esta gestión de activos se detallan las directrices para la clasificación de la información.

4.1.4 Los recursos humanos y la seguridad de la información. El recurso humano es una de las principales fuentes de riesgo para la seguridad de la información por lo tanto en este dominio se tratan los aspectos que se deben tener en cuenta antes, durante y después de la relación laboral. Se incluyen en este apartado los términos y condiciones de contratación, los programas de concienciación, formación y capacitación, los procesos disciplinarios y los puntos a tener en cuenta en caso de cese de la relación laboral o cambio de puesto de trabajo como pueden ser la devolución de activos y la suspensión de las credenciales de acceso.

4.1.5 Seguridad física. Este dominio trata dos aspectos: las áreas seguras, donde se incluyen la definición de perímetros de seguridad física y los controles físicos de entrada entre otros aspectos, y la seguridad de los equipos donde se relaciona, entre otras, la seguridad del cableado, el mantenimiento y la seguridad de los equipos fuera de la compañía.

4.1.6 Gestión de comunicaciones. Este es el dominio más amplio, en el se tratan las responsabilidades y procedimientos de operación, la gestión de los servicios con terceros, la protección contra código malicioso, las copias de seguridad, la seguridad de redes, el intercambio de información, entre otros aspectos.

4.1.7 Control de acceso. Como parte de este dominio se desarrollan los lineamientos para la política de control de acceso, la gestión de accesos de usuarios, los controles de acceso a la red, al sistema operativo, a las aplicaciones y a la información. Además incluye las consideraciones para el manejo de ordenadores portátiles y teletrabajo.

4.1.8 Gestión de sistemas de información. Se desarrollan los requisitos de seguridad de los sistemas de información, el tratamiento correcto de las aplicaciones, los controles criptográficos, la seguridad en los procesos de desarrollo y soporte y la gestión de las vulnerabilidades.

4.1.9 Gestión de incidentes. Se tratan recomendaciones alrededor de la notificación de eventos y puntos débiles de seguridad de la información y los procedimientos y responsabilidades que se deberían asignar para la gestión de incidentes y mejoras de seguridad de la información**.**

4.1.10 Continuidad del negocio. Se mencionan los aspectos de seguridad que se deberían tener en cuenta en la gestión de la continuidad del negocio;

ya que al ser una etapa donde la información puede estar altamente expuesta se debe desarrollar e implantar de planes de continuidad que incluyan la seguridad de la información.

4.1.11 Requisitos legales. En este apartado se incluyen los aspectos que se deben observar para el cumplimiento de los requisitos legales y las políticas y normas de seguridad y cumplimiento técnico.

Teniendo en cuenta que la información es un activo fundamental para el desarrollo, operativa, control y gestión del Modelo de Negocio y que a través de estas se canaliza las prácticas, desde sus aspectos operativos hasta las decisiones gerenciales, siendo estos sistemas elementos clave en el gobierno corporativo de dichas Organizaciones, sea cual sea su tamaño y sector de igual forma la Seguridad de la Información, extendida a todas las infraestructuras físicas, lógicas y organizativas donde se gestiona, se ha convertido en una prioridad al máximo nivel, es necesario afirmar que en la Terminal de Transportes de Ocaña se evidencia la necesidad de implementar los once dominios con el objetivo de proteger la información y así evitar daños en el futuro que puedan llegar a perjudicar la empresa.

Por último el cumplimiento e implantación de los dominios puede contribuir a mejorar de la competitividad, mejorar de la imagen corporativa, protección y continuidad del negocio, cumplimiento legal y reglamentario, optimización de recursos e inversión en tecnología y reducción de costos.

Con el objetivo de analizar la situación actual de la información en la Terminal de Transportes de Ocaña, se llevó a cabo una observación directa que permitió analizar el cumplimiento bajo el estándar ISO 27001, incluyendo sus catorce (14) dominios, e involucrando los siguientes procesos:

Sistema de Información. Telecomunicaciones y Tecnología, Gestión Humana, Gestión Administrativa y Financiera y Control Interno.

El informe de la auditoría realizada se presenta a continuación:

La Terminal de Transportes de Ocaña, tiene por objeto social la prestación de servicios públicos con todas sus actividades mediante una unidad de servicio permanente y de equipo e instalaciones y organización administrativa que concentre la oferta y la demanda del transporte automotor de pasajeros, regulándolas en beneficio de los usuarios para la seguridad y comodidad de los mismo, además contribuir a la solución del problema de la actividad transportadora para efectos socio-urbanísticos y en el mejoramiento del servicio mediante la construcción y explotación de una terminal de transporte de pasajeros en el municipio de Ocaña y su provincia ; además que por medio de la organización del servicio de turismo, correos y telégrafo, restaurantes y cafeterías, expendio de tiquetes, parqueaderos y demás servicios que guarden relación de medio a fin con su objeto social fundamental en desarrollo de este, la sociedad podrá ejecutar todos los actos y contratos que fueren necesarios y convenientes para el cabal cumplimiento de su objeto social y que tengan relación directa con el fin mencionado, incluyendo formar parte de otras sociedades adquiriendo acciones o parte de ellas de interés social o haciendo aportes de cualquier especie, adquirirlas o incorporarlas o fusionarse con ellas siempre que el objeto de aquellas sociedades sea similar al de esta o complementario del mismo,

para lo cual la sociedad deberá obtener permiso previo de que trata el artículo cuarto del decreto ley 3130 de 1968 adquirir o enajenar bienes muebles e inmuebles que posean, girar, protestar y aceptar toda clase de operaciones con entidades nacionales o extranjeras mediante cumplimiento de los requisitos de mutuo, con o sin interés, constituir o aceptar gravamentos reales o personales en garantía de las operacionales que se contraigan y en general, disponer, desarrollar y llevar a término todos aquellos actos relacionados directamente con los que constituyen su objeto social.

Dentro de su estructura se encuentran las siguientes funciones:

Analizar las necesidades relacionas con las tecnologías de la información en las áreas de la entidad.

Asignar objetivos a la Terminal, siguiendo el desarrollo de proyecto y actividades, controlar los resultados en materia informática y de telecomunicaciones.

Llevar a cabo la función gerencial para el desarrollo de los sistemas de información y telecomunicaciones en la Terminal.

Adecuar los procedimientos en el uso de los sistemas informáticos y las normas de seguridad vigentes e implantar los medios y las medidas necesarias para ello.

Responder consultas técnicas, de seguridad y documentar la configuración del sistema.

Ofrecer soporte a la institución en la adquisición y uso de tecnologías de informática y de telecomunicaciones.

Asesorar en la utilización de sistemas de información a los diferentes procesos de la empresa.

Efectuar ajustes sobre los sistemas que están operando de acuerdo a las nuevas necesidades.

Responder por el inventario de todos los equipos existentes en la terminal.

La Terminal de Transportes de Ocaña, cuenta con:

Proveer la infraestructura tecnológica para el funcionamiento de Internet, redes alámbricas e inalámbricas.

Administración de servidores.

Administración de la infraestructura de red.

Backup’s, protección y recuperación de la información.

Administración de salas de cómputo.

Administración de la base de datos.

Administración de cámaras de vigilancia y monitoreo.

ASPECTOS DE LA AUDITORIA. Objetivo General. Realizar una auditoría de cumplimiento bajo el estándar ISO 27001.

Objetivos Específicos. Evaluar el cumplimiento de las actividades relacionadas con la seguridad de la información.

Verificar la eficiencia de los controles implementados para preservar la seguridad de la información.

ALCANCES. Teniendo en cuenta la importancia de la seguridad de la información, se hizo necesario evaluar la existencia y eficiencia de los controles implementados para gestionar adecuadamente la seguridad de la información. La observación incluyó la evaluación de dichos controles, involucrando los siguientes procesos: Sistema de Información, Telecomunicaciones y Tecnología, Gestión Humana, Gestión Administrativa y Financiera y Control Interno.

RECURSOS NECESARIOS. Para la ejecución de la auditoría realizada, se hizo necesaria la utilización de los siguientes recursos:

Recursos de Hardware. Se utilizaron elementos como: equipo de cómputo, impresora, medios de almacenamiento.

Recursos de Software. Se hizo necesario un editor de texto como Microsoft Word 2010.

Recurso Humano. El equipo auditor estuvo conformado de la siguiente manera:

WILLIGTON SANJUÁN MUÑOZ, auditor

CRITERIOS DE AUDITORÍA. La auditoría realizada se llevó a cabo bajo el estándar ISO/IEC 27001, teniendo en cuenta sus 14 dominios, 35 objetivos de control y 114 controles.

METODOLOGÍA. Para llevar a cabo la auditoría de cumplimiento bajo el estándar ISO/IEC 27001 a las áreas que tienen que ver con los procesos de gestión de seguridad de la información en la empresa, se organizaron las siguientes actividades:

PLAN DE AUDITORÍA. Contiene el conjunto de actividades que como equipo auditor, se establecieron para llevar a cabo los acuerdos para la organización del trabajo, así como el lugar y fecha de encuentro con los auditados.

Empresa: **Terminal de Transportes Ocaña** Fecha Inicio: 10/11/2016

Fecha Final: 10/12/2016

Objetivo General

Realizar una auditoría de cumplimiento bajo el estándar ISO 27001.

No.	ACTIVIDAD	FECHA	LUGAR	RESPONSABLE
1	Definición del objeto y los alcances de la auditoría.	11/11/2016	Terminal de Transportes	AUDITOR
2	Reunión del equipo de trabajo para definir responsabilidades y tareas	15/11/2016		AUDITOR
3	Solicitud de documentación de	20/11/2016		AUDITOR

	los procesos relacionados con la gestión de la seguridad de la información		
4	Reunión del equipo de trabajo para el análisis de la documentación	22/11/2016	AUDITOR
5	Diseño de instrumentos de recolección de información	25/11/2016	AUDITOR
6	Aplicación de instrumentos para la realización de la auditoría de cumplimiento bajo el estándar ISO 27001	2711/2016	AUDITOR
7	Realización de entrevistas adicionales	30/11/2016	AUDITOR

8	Análisis de la información recolectada	05/12/2016	AUDITOR
9	Recolección de información adicional	05/12/20156	AUDITOR
11	Reunión Pre - Informe	06/12/2016	AUDITOR
12	Elaboración Informe de Auditoría	10/12/2016	AUDITOR

PROGRAMA DE AUDITORÍA. Comprende las actividades propias de la auditoría para evaluar el grado de cumplimiento de los controles del estándar ISO/IEC 27001, relacionados con la gestión de la seguridad de la información en la Terminal. En la presente tabla se relaciona el objetivo general y dos objetivos específicos que van a permitir su cumplimiento. Asociada a cada objetivo, se establece una actividad con sus correspondientes instrumentos de recolección de información que van a permitir materializar su realización.

Empresa: Terminal de Transportes	Fecha Inicio: 10/11/2016
Proceso**: Gestión de la Seguridad de los Sistemas de Información**	Fecha Final: 10/12/2016

Auditora Líder**: WILLIGTON SANJUÁN MUÑOZ**

Objetivo General. Realizar una auditoría de cumplimiento bajo el estándar ISO 27001

Objetivos Específicos. Evaluar el cumplimiento de las actividades relacionadas con la seguridad de la información.

Verificar la eficiencia de los controles implementados para preservar la seguridad de la información.

Alcances. La auditoría se llevará a cabo a la Seguridad Física y Ambiental en la Terminal de Transportes Ocaña.

ÍTEM	**ACTIVIDAD**	**RPT**	**AUDITADO**
1.1	Medir el grado de cumplimiento de los controles presentes en el estándar ISO/IEC 27001, dentro del Sistema de Gestión de la Seguridad de la Información, mediante la		

	realización de entrevistas.
2.2	Verificar la eficiencia en la implementación de los controles de la norma antes citada, mediante pruebas de cumplimiento.

HALLAZGOS DE LA AUDITORÍA**.** Para presentar los hallazgos, se tuvo en cuenta los 14 dominios del estándar ISO/IEC 27001

Los dominios que se evaluaron se relacionan a continuación:

Políticas de Seguridad

Aspectos organizativos de la seguridad de la información

Seguridad ligada a los recursos humanos

Gestión de activos

Control de accesos

Cifrado

Seguridad física y ambiental

Seguridad en la operativa

Seguridad en las telecomunicaciones

Adquisición, desarrollo y mantenimiento de los sistemas de información

Relaciones con suministradores

Gestión de incidentes en la seguridad de la información

Aspectos de seguridad de la información en la gestión de la continuidad del negocio

Cumplimiento

A continuación se presentan los hallazgos y las recomendaciones respectivas por cada dominio:

Políticas de seguridad de la información

Hallazgos. No existe un documento de Políticas de Seguridad de la Información, que contenga los lineamientos para la protección y uso correcto de los activos de información.

Recomendaciones. La revisión de las políticas de seguridad de la información debería tener en cuenta los resultados de las revisiones por parte de la gerencia. Así mismo, establecer criterios y procedimientos formales para la revisión que pudieran sugerir modificaciones al documento, como cambios en el entorno institucional, nuevas tendencias tecnológicas, reportes de amenazas y/o vulnerabilidades, recomendaciones de autoridades relevantes, entre otros.

De igual forma, se sugiere socializar y/o comunicar a los diferentes áreas de la terminal, los lineamientos contemplados en el documento de Políticas de Seguridad de la Información, para que se adopte una cultura de la protección de la información y de los demás activos de información de la institución.

Aspectos organizativos de la seguridad de la información. Actualmente la Terminal de Transportes de Ocaña, no cuenta con un marco regulatorio para iniciar y controlar los procesos de implementación de la seguridad de la información. De igual forma no existen

responsabilidades claramente definidas para la protección de los activos individuales, ni se conocen procesos de seguridad específicos para cada uno de ellos.

De la misma manera, Terminal de Transportes de Ocaña, no cuenta con procedimientos formales para establecer contacto con autoridades relevantes para los casos en los que se presente un incidente de seguridad que pueda poner en riesgo la continuidad de las operaciones.

Recomendaciones. Definir un marco regulatorio que garantice el cumplimiento de los controles de seguridad contemplados en la política de seguridad de la información. Igualmente, se deben definir claramente las responsabilidades para la protección de los activos individuales y llevar a cabo los procesos de seguridad específicos, definiendo y documentando claramente los niveles de autorización.

Seguridad ligada a los recursos humanos. En la etapa de reclutamiento de personal, una vez se hace todo el proceso de convocar a nuevos empleos, se hace la recepción de las hojas de vida de los aspirantes y se realiza el estudio y revisión de los perfiles y competencias laborales solicitadas, así como el estudio de antecedentes.

Con respecto a la etapa de contratación del personal, se realizan los diligenciamientos de ley y el empleado firma el contrato. Cabe destacar que aunque el contrato no estipula una cláusula de confidencialidad específica, existe un ítem que se refiere a la reserva total de la información a la cual tendrá acceso.

Por su parte, los empleados no reciben capacitación específica en cuanto a procedimientos de seguridad de la información que tienen bajo su responsabilidad. Solo reciben a su correo institucional, tips de seguridad enviados por el Administrador Web.

El contrato de trabajo tampoco contempla reglas claras para el uso aceptable de algunos activos como correo electrónico, dispositivos, datos, equipos, entre otros.

En el momento de terminación del contrato, no existe un formato denominado FORMATO ENTREGA DEL PUESTO DE TRABAJO, que contiene las actividades necesarias para hacer entrega oficial de su puesto de trabajo y la conformidad de las distintas dependencias de la Terminal de Transportes de Ocaña con las cuales se establece relación directa.

Recomendaciones**.** Establecer un acuerdo de confidencialidad para cada uno de los empleados de la Terminal de Transportes de Ocaña en el momento de su contratación o cuando haya algún cambio de puesto de trabajo, que contemple los requerimientos para proteger la información, utilizando términos legalmente ejecutables y especificando entre otros aspectos, el tipo de información que debe protegerse, la duración esperada del acuerdo, las responsabilidades para usar información confidencial, así como para evitar su divulgación, condiciones específicas de terminación del contrato laboral y las sanciones impuestas para los casos de incumplimiento de dicho acuerdo.

Gestión de activos. La Terminal de Transportes de Ocaña no cuenta con un inventario de todos sus activos, debidamente clasificados y mantenidos. Todos los activos no se encuentran etiquetados de tal manera que son de fácil acceso. Cabe resaltar que aunque estas funciones son delegadas, no existen documentos formales que establezcan dicha responsabilidad.

No existen formatos para entrega de activos, así como reportes de baja de elementos. En relación con las licencias de software como activo de información, están bajo la responsabilidad y custodia.

Recomendaciones**.** Acordar y documentar la propiedad para cada uno de los activos de información. De igual manera, establecer una clasificación específica para la Terminal de Transportes de Ocaña, que indique los niveles de protección de acuerdo con la importancia de los mismos y el valor comercial que representan para la empresa.
Documentar e implementar reglas para el uso aceptable y seguro de los activos de información.

Control de accesos. El documento de Políticas de Seguridad de la Información, no contempla las reglas de control de acceso y los derechos para cada usuario o grupos de usuarios de los sistemas de información. Así mismo, establece la responsabilidad de los usuarios en el tratamiento de la información, actualización de hardware y software, uso del correo electrónico, almacenamiento y respaldo de los datos, uso adecuado de la red interna, entre otros.

Recomendaciones**.** Establecer un procedimiento formal para la gestión de los derechos de acceso de los usuarios de los sistemas de información, donde se entregue un documento a cada usuario indicando la información relacionada con el acceso y los requerimientos de protección de la información que tendrá bajo su responsabilidad.

Cifrado. No existe un control para la asignación de privilegios de acceso a los sistemas de información, los mismos no se revisan periódicamente, ni existe procedimiento formal para

realizarlo. El sistema automáticamente solicita cambio de contraseña de usuario cada seis (6) meses.

Recomendaciones. Establecer protocolos y documentar los procedimientos para la gestión de los derechos y niveles de acceso a los sistemas de información.

Seguridad física y ambiental. En el ítem de Áreas Seguras, se pudo determinar que no existen medidas efectivas para controlar el acceso a las áreas críticas en la Terminal de Transportes de Ocaña. Esta situación pone en riesgo la seguridad de los activos que se encuentran en el área y la integridad, confidencialidad y disponibilidad de la información que allí se maneja.

Así mismo, se encontró que las copias de respaldo que se hacen diariamente por una parte, quedan almacenadas en el mismo servidor y una copia se guarda en el servidor de backup interno.

Por otra parte, los equipos que manejan información sensible como los servidores y equipos principales de procesamiento, cuentan con un sistema de refrigeración adecuada (18^0C). Sin embargo, los niveles de humedad y la impermeabilidad en el cuarto de servidores no se controla a través de ningún mecanismo; situación que puede poner en riesgo la integridad de las copias de respaldo que se almacenan en este lugar.

Recomendaciones. Terminal de Transportes de Ocaña, debe implementar las acciones contempladas en el Plan de Contingencias y en las Políticas de Seguridad, en cuanto a riesgos de seguridad física se refiere. Para esto, se sugiere:

Implantar sistemas biométricos que permitan controlar de forma más eficiente el acceso a las áreas críticas de la Terminal de Transportes de Ocaña

Instalar alarmas contra incendios, detectores de humo y salidas de emergencia, para minimizar el impacto que puede provocar la presencia de una catástrofe ambiental.

Construir o adecuar un espacio fuera de las instalaciones de la Terminal de Transportes de Ocaña, con las medidas de seguridad física necesarias para almacenar las copias de respaldo que se realizan diariamente.

Realizar campañas de sensibilización sobre la protección tanto de los equipos como de la información que cada funcionario, específicamente los que manejan sistemas de información, tiene bajo su responsabilidad.

Adquisición, desarrollo y mantenimiento de sistemas de información. En el entorno de desarrollo aplicaciones, actualmente no existen tareas por cada etapa del proceso (análisis, diseño, implementación, instalación, entre otras) que se encuentren segregadas ni asignadas a diferentes usuarios. Quien diseña, codifica, implementa, instala, capacita, configura, etc.

A pesar que existe un procedimiento de gestión de los sistemas de información, cuyo fin es el de "solucionar las necesidades a nivel de desarrollo y actualización de software para cumplir con los requerimientos y dar soporte funcional para el mejoramiento continuo de los procesos", las actividades de cada etapa del proceso de desarrollo de aplicaciones, no se documenta.

Recomendaciones. Segregar las tareas propias en cada una de las fases del proceso de desarrollo de software. Así mismo, documentar las actividades en cada fase y definir los

controles necesarios para especificar los requerimientos de seguridad antes y después del desarrollo de aplicaciones.

Aspectos de seguridad de la información en la gestión de la continuidad del negocio. En la actualidad, Terminal de Transportes de Ocaña, no cuenta con un Plan de Continuidad del Negocio (PCN), que contemple las actividades necesarias para minimizar el impacto sobre la Institución y recuperarse de la pérdida de activos de información hasta un nivel aceptable.

Recomendaciones**.** Implementar un proceso de gestión de la continuidad del negocio, en adelante PCN, bajo estándares internacionales reconocidos y probados, para minimizar el impacto sobre Terminal de Transportes de Ocaña en caso de pérdida parcial o total de sus funciones de operación, provocada por eventos no intencionados como desastres naturales, accidentes, fallas en los equipos o cualquier otro incidente cometido de forma deliberada.

Cumplimiento. La Política de Seguridad de la Información, contempla las sanciones pertinentes y necesarias de aplicar en los casos en los que se incurra en algún delito informático de los que trata la Ley 1273 de 2009. Sin embargo, existen procedimientos que aunque se realizan, no se encuentran documentados, lo que evidencia una falta de organización y de estandarización en las actividades propias de la administración de la información y de los demás recursos informáticos.

Recomendaciones. Definir, documentar y actualizar todos los requerimientos legales, reguladores y contractuales y el enfoque de Terminal de Transportes de Ocaña, para satisfacer

esos requerimientos, para cada sistema de información. De igual forma se recomienda, que para efecto de revisión y publicación de procedimientos relacionados con sistemas de información, arquitecturas de hardware y software, telecomunicaciones, entre otros, en el equipo de Calidad, se cite a un experto en el tema, para que el resultado de dicha evaluación pueda ser lo más objetivo posible.

4.2 Metodología de evaluación de riesgos que permita definir las vulnerabilidades y amenazas de seguridad existentes, en la Terminal de Transportes de Ocaña, Norte de Santander.

La metodología hace referencia al conjunto de procedimientos racionales utilizados para alcanzar el objetivo o la gama de objetivos que rige una investigación científica, una exposición doctrinal o tareas que requieran habilidades, conocimientos o cuidados específicos. Con frecuencia puede definirse la metodología como el estudio o elección de un método pertinente o adecuadamente aplicable a determinado objeto.

No debe llamarse metodología a cualquier procedimiento, pues se trata de un concepto que en la gran mayoría de los casos resulta demasiado amplio, siendo preferible usar el vocablo método. También es de saber que existe una posición ametódica e incluso una tendencia de matizado anarquismo epistemológico.

Para el caso de la Terminal de Transportes de Ocaña, la metodología más apropiada es el ciclo PDCA. El nombre del Ciclo PDCA (o Ciclo PHVA) viene de las siglas Planificar, Hacer,

Verificar y Actuar, en inglés “Plan, Do, Check, Act”. También es conocido como Ciclo de mejora continua o Círculo de Deming, por ser Edwards Deming su autor. Esta metodología describe los cuatro pasos esenciales que se deben llevar a cabo de forma sistemática para lograr la mejora continua, entendiendo como tal al mejoramiento continuado de la calidad (disminución de fallos, aumento de la eficacia y eficiencia, solución de problemas, previsión y eliminación de riesgos potenciales…). El círculo de Deming lo componen 4 etapas cíclicas, de forma que una vez acabada la etapa final se debe volver a la primera y repetir el ciclo de nuevo, de forma que las actividades son reevaluadas periódicamente para incorporar nuevas mejoras. La aplicación de esta metodología está enfocada principalmente para para ser usada en empresas y organizaciones.

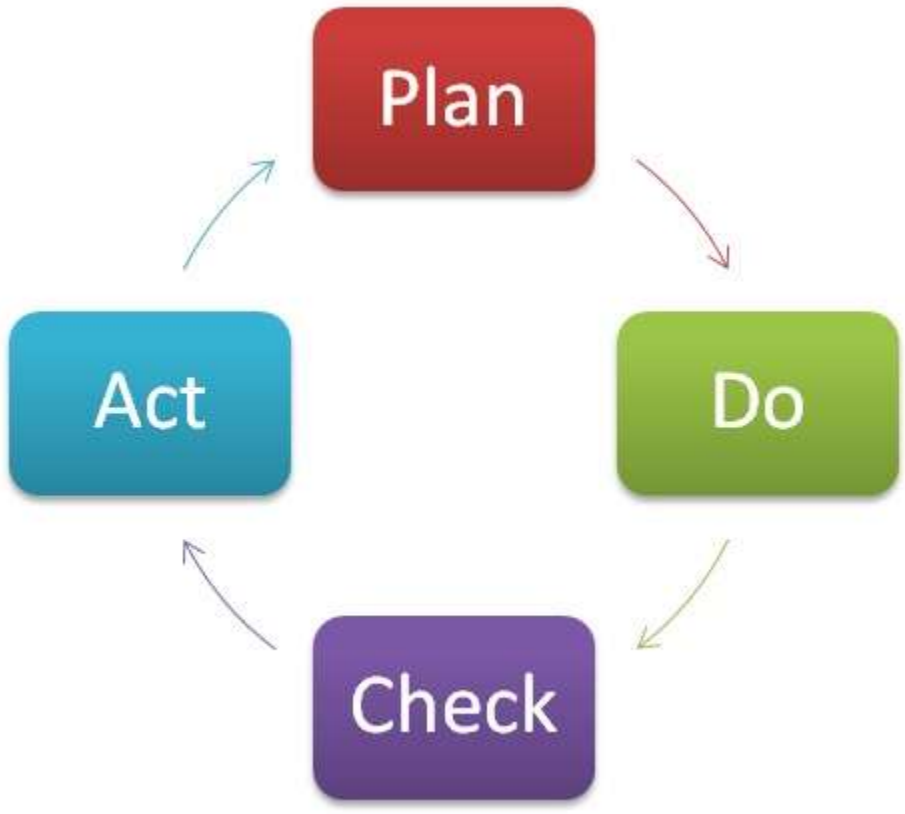

Figura 1. Ciclo PHVA: Planificar, Hacer, Verificar, Actuar.

Las cuatro etapas que componen el ciclo son las siguientes:

Planificar (Plan). Se buscan las actividades susceptibles de mejora y se establecen los objetivos a alcanzar. Para buscar posibles mejoras se pueden realizar grupos de trabajo, escuchar las opiniones de los trabajadores, buscar nuevas tecnologías mejores a las que se están usando ahora, etc.

Hacer (Do). Se realizan los cambios para implantar la mejora propuesta. Generalmente conviene hacer una prueba piloto para probar el funcionamiento antes de realizar los cambios a gran escala.

Controlar o Verificar (Check). Una vez implantada la mejora, se deja un periodo de prueba para verificar su correcto funcionamiento. Si la mejora no cumple las expectativas iniciales habrá que modificarla para ajustarla a los objetivos esperados. (ver Herramientas de Control).

Actuar (Act). Por último, una vez finalizado el periodo de prueba se deben estudiar los resultados y compararlos con el funcionamiento de las actividades antes de haber sido implantada la mejora. Si los resultados son satisfactorios se implantará la mejora de forma definitiva, y si no lo son habrá que decidir si realizar cambios para ajustar los resultados o si desecharla. Una vez terminado el paso 4, se debe volver al primer paso periódicamente para estudiar nuevas mejoras a implantar.

4.2.1 Ejemplo de implantación del ciclo PDCA. Se analizan posibles mejoras, ya sea porque se han detectado problemas,

porque los trabajadores han propuesto formas distintas de realizar alguna tarea, porque en el mercado se han implementado nuevas formas de servicio más eficientes que permiten ahorrar costes, etc.

Se estudian las posibles mejoras y su impacto. Se eligen las que mejor van a funcionar y se decide implantarlas en una prueba piloto a pequeña escala.

Una realizada la prueba piloto, se verifica que los cambios funcionan correctamente y dan el resultado deseado. Si los cambios realizados no satisfacen las expectativas se modifican para que funcionen conforme a lo esperado.

Por último, si los resultados son satisfactorios se implantan a gran escala en la línea del servicio ofrecido por la empresa. Una vez finalizadas e implantadas las mejoras, las actividades de la empresa deben funcionar más eficientemente. No obstante, periódicamente habrá que volver a buscar posibles nuevas mejoras y volver a aplicar el círculo de Demming de nuevo.

4.3 Mecanismos de control y gestión que minimicen las vulnerabilidades encontradas en el estudio del análisis de riesgos realizado.

El concepto de “control” dentro de la norma agrupa todo el conjunto de acciones, documentos, procedimientos y medidas técnicas adoptadas para garantizar que cada amenaza, identificada y valorada con un cierto riesgo, sea minimizada.

De otra parte los controles se presentan para reducir el riesgo se necesita la mejora de Salvaguardas existentes o la incorporación de otras nuevas. Se define la función o servicio de salvaguarda como la acción que reduce el riesgo; el mecanismo de salvaguarda como dispositivo, físico o lógico, capaz de reducir el riesgo y opera bien de forma preventiva sobre la vulnerabilidad, "neutralizando" la materialización de la amenaza, antes de que actúe ésta, o bien de forma curativa sobre el impacto, modificando el estado de seguridad del Activo agredido y reduciendo el resultado de la agresión, o sea después de ésta.

Teniendo en cuenta lo anterior en la Terminal de Transportes de Ocaña, se realizó la evaluación de las salvaguardas en la documentación y se describieron cuáles aplican para el sistema de información de la entidad. Para este análisis se presenta los resultados teniendo en cuenta varias categorías como son:

G: Gestión.

T: Técnico.

P: Personal.

F: Seguridad física.

De igual forma las normas ISO/IEC 27001, ISO/IEC 27002 están enfocadas a todo tipo de organizaciones (por ej. empresas comerciales, agencias, gubernamentales, organizaciones sin ánimo de lucro), tamaños (pequeña, mediana o gran empresa), tipo o naturaleza. Por lo que los controles pueden ser:

4.3.1 Políticas. Un documento denominado "política" es aquel que expresa una intención e instrucción global en la manera que formalmente ha sido expresada por la Dirección de la organización.

El contenido de las políticas se basa en el contexto en el que opera una organización y suelen ser considerados en su redacción los fines y objetivos de la organización, las estrategias adoptadas para alcanzar sus objetivos, la estructura y los procesos adoptados por la organización, los objetivos generales y específicos relacionados con el tema de la política y requisitos de las políticas procedentes de niveles más superiores (legales de obligado cumplimiento, del sector al que pertenece la organización, de la propia organización de niveles superiores o más ámplios, ...) relacionadas.

Una estructura típica de los documentos de políticas podría ser:

Resumen: Política Resumen - Visión general de una extensión breve; una o dos frases y que pueden aparecer fusionadas con la introducción.

Introducción: Breve explicación del asunto principal de la política.

Ámbito de aplicación: Descripción de los departamentos, áreas o actividades de una organización a las que afecta/aplica la política. Cuando es relevante en este apartado se mencionan otras políticas relevantes a las que se pretende dar cobertura desde ésta.

Objetivos: Descripción de la intención de la política.

Principios: Descripción de las reglas que conciernen a acciones o decisiones para alcanzar los objetivos. En algunos casos puede ser de utilidad identificar previamente los procesos clave asociados con el asunto principal de la política para pasar posteriormente a identificar las reglas de operación de los procesos.

Responsabilidades: Descripción de quién es responsable de qué acciones para cumplie con los requisitos de la política. En algunos casos, esto puede incluir una descripción de los mecanismos organizativos, así como las responsabilidades de las personas con roles designados.
Resultados clave: Descripción de los resultados relevantes para las actividades de la organización que se obtienen cuando se cumplen los objetivos.
Políticas relacionadas: Descripción de otras políticas relevantes para el cumplimiento de los objetivos, usualmente se indican detalles adicionales en relación a temas específicos.

La política de alto nivel (más genérica) habitualmente relacionada con el sistema de gestión para la seguridad de la información (SGSI) suele estar apoyada por políticas de bajo nivel, específicas a aspectos concretos en temáticas como el control de accesos, la clasificación de la información, la seguridad física y ambiental, uso aceptable de activos, escritorio y pantallas libres de información sensible, dispositivos móviles y teletrabajo, backups, protección contra el malware,

4.3.2 Organización. El objetivo del presente dominio es establecer la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la organización.
Para ello se debería definir formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de las políticas de seguridad, la coordinación de la implementación de la seguridad y la asignación de funciones y responsabilidades.

Para una actualización adecuada en materia de seguridad se debería contemplar la necesidad de disponer de fuentes con conocimiento y experimentadas para el asesoramiento, cooperación y colaboración en materia de seguridad de la información.

Las protecciones físicas de las organizaciones son cada vez más reducidas por las actividades de la organización requiere por parte del personal interno/externo que acceden a información desde el exterior en situación de mobilidad temporal o permanente. En estos casos se considera que la información puede ponerse en riesgo si el acceso se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

4.3.3 Recursos humanos. El objetivo del presente dominio es la necesidad de educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de actividad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad.

Es necesario reducir los riesgos de error humano, comisión de actos ilícitos, uso inadecuado de instalaciones y recursos y manejo no autorizado de la información, junto a la definición de posibles sanciones que se aplicarán en caso de incumplimiento.

Se requiere explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado, así como, garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se

encuentren capacitados para respaldar la Política de Seguridad de la organización en el transcurso de sus tareas normales.

Suele ser responsabilidad del Área de Recursos Humanos incluir las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionar los Compromisos de Confidencialidad con el personal y coordinar las tareas de capacitación de usuarios respecto a las necesidades actuales en seguridad.

Activos. El objetivo del presente dominio es que la organización tenga conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos.

Algunos ejemplos de activos son:

Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad y contingencia, información archivada, etc.

Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo y publicación de contenidos, utilitarios, etc.

Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PABXs, máquinas de fax, contestadores automáticos, switches de datos, etc.), medios magnéticos (cintas, discos, dispositivos móviles de almacenamiento de datos – pen drives, discos externos, etc.-), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado, controles automatizados de acceso, etc.), mobiliario, lugares de emplazamiento, etc.

Servicios: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Accesos. El objetivo del presente dominio es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deberían implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso. La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

Cifrado. El objetivo del presente dominio es el uso de sistemas y técnicas criptográficas para la protección de la información en base al análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad. La aplicación de medidas de cifrado se debería desarrollar en base a una política sobre el uso de controles criptográficos y al establecimiento de una gestión de las claves que sustenta la aplicación de las técnicas criptográficas.

Física y ambiental. El objetivo es minimizar los riesgos de daños e interferencias a la información y a las operaciones de la organización. El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles de protección de las instalaciones de procesamiento de información crítica o sensible de la organización, contra accesos físicos no autorizados. El control de los factores ambientales de origen interno y/o externo permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas mientras no están siendo utilizados. Es por ello que el transporte y la disposición final presentan riesgos que deben ser evaluados, especialmente en casos en los que el equipamiento perteneciente a la organización estén físicamente fuera del mismo (housing) o en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información (hosting/cloud).

Operativas. El objetivo es controlar la existencia de los procedimientos de operaciones y el desarrollo y mantenimiento de documentación actualizada relacionada. Adicionalmente, se debería evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando las responsabilidades correspondientes y administrando los medios técnicos necesarios para permitir la segregación de los ambientes y responsabilidades en el procesamiento.

Con el fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario, sería necesario monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad. El control de la realización de las copias de resguardo de información, así como la prueba periódica de su restauración permiten garantizar la restauración de las operaciones en los tiempos de recuperación establecidos y acotar el periodo máximo de pérdida de información asumible para cada organización.

Se deberían definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados a las redes de la organización. Finalmente, se deberían verificar el cumplimiento de las normas, procedimientos y controles establecidos mediante auditorías técnicas y registros de actividad de los sistemas (logs) como base para la monitorización del estado del riesgo en los sistemas y descubrimiento de nuevos riesgos.

Telecomunicaciones. El objetivo es asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte. La gestión segura

de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicaciones legales, monitoreo y protección. La información confidencial que pasa a través de redes públicas suele requerir de controles adicionales de protección. Los intercambios de información por parte de las organizaciones se deberían basar en una política formal de intercambio y en línea con los acuerdos de intercambio, y debiera cumplir con cualquier legislación relevante.

Adq., des. y mantto. El objetivo es asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información. Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan. Definir los métodos de protección de la información crítica o sensible.

Aplica a todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software que integren cualquiera de los ambientes administrados por la organización en donde residan los desarrollos mencionados.

Suministradores. El objetivo es implementar y mantener el nivel apropiado de seguridad de la información y la entrega de los servicios contratados en línea con los acuerdos de entrega de servicios de terceros. La organización debe chequear la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados con terceras personas.

Incidentes. El objetivo es garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno. Las organizaciones cuentan con innumerables activos de información, cada uno expuesto a sufrir incidentes de seguridad. Resulta necesario contar con una capacidad de gestión de dichos incidentes que permita comenzar por su detección, llevar a cabo su tratamiento y colaborar en la prevención de futuros incidentes similares.

Continuidad negocio. El objetivo es preservar la seguridad de la información durante las fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad. Se debería integrar dentro de los procesos críticos de negocio, aquellos requisitos de gestión de la seguridad de la información con atención especial a la legislación, las operaciones, el personal, los materiales, el transporte, los servicios y las instalaciones adicionales, alternativos y/o que estén dispuestos de un modo distinto a la operativa habitual.

Se deberían analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio y desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales, manteniendo las consideraciones en seguridad de la información utilizada en los planes de continuidad y función de los resultados del análisis de riesgos.

Deberían llevarse a cabo las pruebas pertinentes (tales como pruebas sobre el papel, simulacros, pruebas de failover, etc.) para (a) mantener los planes actualizados, (b) aumentar la confianza de la dirección en los planes y (c) familiarizar a los empleados relevantes con sus funciones y responsabilidades bajo condiciones de desastre.

Minimizar los efectos de las posibles interrupciones de las actividades normales de la organización asociadas a desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos, protegiendo los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación. Instruir al personal involucrado en los procedimientos de reanudación y recuperación en relación a los objetivos del plan, los mecanismos de coordinación y comunicación entre equipos (personal involucrado), los procedimientos de divulgación en uso, los requisitos de la seguridad, los procesos específicos para el personal involucrado y responsabilidades individuales.

Cumplimiento. El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales. Los requisitos normativos y contractuales pertinentes a cada sistema de información deberían estar debidamente definidos y documentados. El objetivo es cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la organización y/o a los empleados que incurran en responsabilidad civil o penal como resultado de incumplimientos. Se debe revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

Teniendo en cuenta lo anterior se debe mencionar que en la Terminal de Transportes de Ocaña, se debe implementar la ISO 27001 y posteriormente aplicar los controles, para la protección de la información ya que contiene datos confidenciales, Protección de las comunicaciones para garantizar conectividad y también evitar la captura de datos a través de las redes de comunicaciones. La gestión de claves criptográficas para dar mayor seguridad al acceso a los recursos de información ya que se debe tener un mayor control de los funcionarios o personas que ingresan a las aplicaciones o equipos que guardan la información.

4.4 Informe de recomendaciones donde se muestre los hallazgos que permita definir un Sistema de seguridad de la información ajustada a la realidad de la Terminal.

La información es un recurso que, como el resto de los activos, tiene valor para el Organismo y por consiguiente debe ser debidamente protegida. Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del Organismo. Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional. Para esto, se debe asegurar un compromiso manifiesto de las máximas Autoridades de la institución, tanto de la Terminal, como de las TIC`S en la entidad, consolidación y cumplimiento de la Política diseñada, con el objetivo de proteger los recursos de información de la institución y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las medidas de seguridad comprendidas en esta Política. Mantener la Política de Seguridad del Organismo actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

Establecer las directrices, los procedimientos y los requisitos para asegurar la protección oportuna y correcta de los equipos de comunicación en la Terminal de Transportes.

Alcance Esta Política se aplica en todo el ámbito de la empresa, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Organización de la Seguridad de la Información.

Es necesario tener bien definido un marco de gestión para efectuar diferentes tareas tales como la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades, para tener una eficiente administración de la seguridad de información. Se debe tener en cuenta que ciertas actividades de la Terminal pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información. En estos casos se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.

Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.

Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.

Garantizar que la seguridad sea parte del proceso de planificación de la información.

Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.

Promover la difusión y apoyo a la seguridad de la información dentro de la Terminal de Transportes de Ocaña.

Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información de la Institución frente a interrupciones imprevistas. Una vez integrado el Comité, es necesario se definan las funciones de los miembros del mismo para poder que este pueda desempeñar sus actividades y mejorar la seguridad en la institución.

En la implementación del sistema de seguridad, se deben especificar los miembros del Comité y proponerlos a la Junta Directiva.

Es necesario definir el proceso para la autorización de nuevos recursos para el procesamiento de información así como los requerimientos de Seguridad en contratos con Terceros, los principales puntos que se deben considerar lo siguiente:

a) Cumplimiento de la Política de seguridad de la información de la institución.

b) Protección de los activos de la institución, incluyendo:

Procedimientos para proteger los bienes de la institución, abarcando los activos físicos, la información y el software.

Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.

Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.

Restricciones a la copia y divulgación de información.

c) Descripción de los servicios disponibles.

d) Nivel de servicio esperado y niveles de servicio aceptables.

e) Permiso para la transferencia de personal cuando sea necesario.

f) Obligaciones de las partes del acuerdo y responsabilidades legales.

g) Definiciones relacionadas con la protección de datos.

h) Acuerdos de control de accesos que contemplen:

Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.

Proceso de autorización de accesos y privilegios de usuarios.

Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.

i) Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.

j) Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.

k) Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.

l) Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.

m) Proceso claro y detallado de administración de cambios.

n) Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.

o) Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.

p) Controles que garanticen la protección contra software malicioso.

q) Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.

Seguridad Física y del Entorno. La seguridad física y ambiental minimiza los riesgos de daños e interferencias a la información y a las operaciones de la Terminal. Además, trata de evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad. El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. Gran cantidad de información manejada en las oficinas se encuentra almacenada en papel, por lo que es necesario establecer pautas de seguridad para la conservación de dicha documentación. Objetivo Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información del Organismo. Proteger el equipamiento de procesamiento de

información crítica del Organismo ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados.

Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información. Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización. Controlar de mejor forma la seguridad en conexiones entre la División de TIC y los proveedores externos. Mantener un registro de eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

Adquisición, desarrollo y mantenimiento de sistemas de Información. En este control se deben revisar las aplicaciones como puntos críticos de vulnerabilidades, es necesaria una adecuada administración de la infraestructura de base, Sistemas Operativos y Software de Base, en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

Gestión de Incidentes de Seguridad de la Información. Divulgación de eventos y de debilidades de la seguridad de la información. Es importante que la División de TIC tenga un procedimiento a seguir cuando se presente un incidente de seguridad en la red, pues es necesario que pueda aprender de los errores y evitar que un ataque ocurra.

Implementación del Plan de Tratamiento de Riesgos. El objetivo de esta etapa es tomar la acción más apropiada de tratamiento para cada uno de los riesgos identificados, en base a las secciones. Identificación de amenazas y identificación de vulnerabilidades.

Conclusiones

Teniendo en cuenta los dominios de la norma ISO 27001, se debe decir que es muy importante el uso de base de datos y de la seguridad de la información para el fortalecimiento de las TIC y para el ejercicio eficiente del control, en la Terminal de Transporte de Ocaña.

Para lograr la adecuada evaluación de los riesgos se debe emplear la metodología e incluir a los clientes internos y externos, logrando de esta forma prevenir la vulnerabilidad que hasta el momento se ha visto en la entidad.

Los controles son necesarios en toda entidad por lo que se deben tener en cuenta, para lograr la vulnerabilidad y riesgos, al igual que implementar mecanismos que ayuden a mejorar los procesos en la misma.

De acuerdo al informe son muchas las falencias que se deben controlar en la Terminal de Transportes, por lo que es necesario implementar la Norma ISO 27001 y así mejorar los procesos y lograr que la empresa avance y permanezca en el mercado del transporte.

Recomendaciones

Se recomienda la implementación de la norma como tal, empezando por los dominios, ya que en la Terminal de Transportes no existe seguridad en la información manejada a diario.

Es necesario utilizar la metodología de evaluación de riesgos propuesta, siendo está la más adecuada para la implementación de la normar en la entidad.

De igual forma es necesario utilizar los mecanismos de control y gestión propuestos con el objetivo de minimizar las vulnerabilidades encontradas en el estudio del análisis de riesgos realizado en la Terminal de Transportes de Ocaña.

Se recomienda tener en cuenta las sugerencias realizadas en el informe con el objetivo de minimizar los riesgos de la información y así asegurar la misma en la entidad.

Referencias

Blog especializado en sisetma de gestion de seguridad de la información. (23 de Abril de 2015). http://www.pmg-ssi.com/2015/04/la-importancia-de-la-norma-iso-27001/. Obtenido de La importancia de la norma ISO 27001.

Bosca, J. E., & M.J, M. (2004). Efectos Macroeconómicos de las Inversiones en Infraestructuras Públicas. Valencia.

BSI. (10 de Septiembre de 2016). http://www.bsigroup.com/es-ES/Seguridad-de-la-Informacion-ISOIEC-27001/. Obtenido de Norma ISO/IEC 27001 - Gestión de la Seguridad de la Información.

Castro Toro, J. P. (2010). Compilacion bibliografica. Manizales: Universidad de Caldas.

Congreso de Colombia. (1 de Agosto de 2015). http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf. Obtenido de Ley 1273 del 5 de enero de 2009.

Congreso de Colombia. (1 de Agosto de 2015). Ley estatutaria No. 1266 del 31 de diciembre de 2008. Obtenido de http://www.sic.gov.co/drupal/sites/default/files/files/ley1266_31_12_2008(1).pdf.

Federación Internacional de Sociedades de la Cruz Roja. (2010). Que es la vulnerabilidad.

Ministerio de las TICs. (28 de Octubre de 2016). http://www.mintic.gov.co/gestionti/615/w3-article-5482.html. Obtenido de Sistemas de Gestión de la Seguridad de la Información (SGSI).

Ministerio de tecnologia de la infromación y la comunicación. (12 de Julio de 2012). http://www.mintic.gov.co/portal/604/articles-5259_doc_pdf.pdf. Obtenido de Infrome de gestion.

Paez Garcia, L. E. (2009). Historia de la Región de Ocaña. . Bogotá: Jaguar Group Producciones.

República de Colombia. (2012). Constitucion Política de Colombia. Bogotá: Cupido.

República de Colombia. (2012). Ley 1581 de 2012. Bogotá.

Sanso, R. (2011). Psicología aplicada a la seguridad informática.

Seguros y pensiones para todos. (1 de Septiembre de 2016). Riesgos. Obtenido de https://segurosypensionesparatodos.fundacionmapfre.org/syp/es/seguros/definicion-seguro-asegurar/el-riesgo-asegurar/que-es-el-riesgo-asegurar/.

Unisdr. (2004). https://www.unisdr.org/2004/campaign/booklet-spa/page4-spa.pdf. Obtenido de Amenazas.

Vargas, A. C. (Agosto de 2016). http://archivo.ucr.ac.cr/docum/ISOEIC27000.pdf. Obtenido de Que es el sistema de gestión de seguridad de la información.

Villalon Huertas, A. (29 de Octubre de 2016). http://www.shutdown.es/ISO17799.pdf. Obtenido de Sistema de gestion de seguridad de la información.