RESUMEN – TRABAJO DE GRADO

AUTORES	JOSÉ DANIEL PAREDES ARIAS LINA LUCIA GRAZZIANI CRIADO
FACULTAD	DE INGENIERIAS
PLAN DE ESTUDIOS	INGENIERIA DE SISTEMAS
DIRECTOR	ALBA CECILIA PEÑARANDA SOTO
TÍTULO DE LA TESIS	EVALUACION DE LA SEGURIDAD EN LA INFORMACIÓN PARA LA EMPRESA TRANSPORTADORES DE NORTE DE SANTANDER SAS, BASADOS EN LA NORMA ISO/IEC 27001:2013

RESUMEN

(70 PALABRAS APROXIMADAMENTE)

LA NORMA ISO 27001 DEL 2013, BUSCA ESTABLECER LA PROTECCIÓN IDÓNEA PARA EVITAR EL ACCESO O DIVULGACIÓN A PERSONAS NO AUTORIZADAS DE LA INFORMACIÓN ALMACENADA O PROCESADA A TRAVÉS DE LOS DISPOSITIVOS MÓVILES O ESTACIONES DE TRABAJO REMOTAS. EL ACCESO REMOTO POR MEDIO DE REDES PÚBLICAS A LOS SISTEMAS DE INFORMACIÓN DE LA ORGANIZACIÓN DEBE CONTAR CON MECANISMOS ADECUADOS DE CONTROL PARA DE IDENTIFICAR Y AUTENTIFICAR A CADA USUARIO.

CARACTERÍSTICAS

PÁGINAS: 88	PLANOS: 0	ILUSTRACIONES: 0	CD-ROM: 1

EVALUACION DE LA SEGURIDAD EN LA INFORMACIÓN PARA LA EMPRESA TRANSPORTADORES DE NORTE DE SANTANDER SAS, BASADOS EN LA NORMA ISO/IEC 27001:2013

AUTORES:

JOSÉ DANIEL PAREDES ARIAS

LINA LUCIA GRAZZIANI CRIADO

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

Directora:

ALBA CECILIA PEÑARANDA SOTO

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERÍAS

ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS

Ocaña, Colombia Agosto de 2018

Agradecimientos

Los autores del proyecto de grado expresan sus agradecimientos a todos y cada uno de los docentes y directivos de la Universidad Francisco de Paula Santander Ocaña, y de igual forma a la directora Esp. Alba Cecilia Peñaranda Soto, por su guía y acompañamiento en este proceso.

Índice

Lista de figuras

Lista de tablas

Lista de apéndices

Resumen

La Norma ISO 27001 del 2013, busca establecer la protección idónea para evitar el acceso o divulgación a personas no autorizadas de la información almacenada o procesada a través de los dispositivos móviles o estaciones de trabajo remotas. El acceso remoto por medio de redes públicas a los sistemas de información de la organización debe contar con mecanismos adecuados de control para de identificar y autentificar a cada usuario. Los equipos móviles se deben proteger físicamente contra el robo.

Si el equipo cuenta con información sensible o critica de la organización no se debe dejar sin prestarle atención y ser bloqueado con un medio físico. El personal que porta este equipo debe ser informado de los riesgos, controles, obligaciones y deberes que se tienen. Dicho trabajo debe ser autorizado a personas claves para la empresa y llevar las disposiciones y controles de seguridad que estén acordes con las políticas de seguridad que la entidad tenga.

Introducción

El presente trabajo es un auditoria que permitió determinar los riesgos y vulnerabilidades que posee la información en la empresa Transportadores de Norte de Santander S.A.S, estableciendo las necesidades reales de generar estrategias para preservar la información y evitar pérdidas en las mismas, se analizó la normas ISO 27001 teniendo en cuenta sus estándares y procesos asociados a la seguridad de la información como son los dominios.

Por medio de éste análisis se creó una entrevista y lista de verificación con el objetivo de hacer una recolección de la información y poder emitir un informa, de igual forma se tuvo en cuenta un marco histórico, que comprendía antecedentes a nivel internacional, nacional y local del tema, un marco conceptual, contextual, teórico y legal, que le dio bases teóricas a la investigación.

Por último se desarrollaron objetivos como son la realización de un diagnóstico a la situación actual de la empresa Transportadores de Norte de Santander SAS en cuanto a la seguridad de la información, se mencionaron los dominios de la norma ISO 27001:2013 y su importancia en la seguridad de la información, se determinó una metodología adecuada para la evaluación de la seguridad de la información existente y se elaboró un informe de recomendaciones de acuerdo a los hallazgos identificados, todo lo anterior permitió llegar a unas conclusiones y recomendaciones de la investigación.

Capítulo 1. Evaluación de la seguridad en la información para la empresa Transportadores de Norte de Santander SAS, basados en la norma ISO/IEC 27001:2013

1.1 Planteamiento del problema

El transporte en Colombia está regulado dentro de las funciones del Ministerio de Transporte, el cual lleva procesos muy de la mano con la autoridad ambiental la Unidad de Planeación Minero energética, la empresa Colombiana de Petróleos (Ecopetrol), el Ministerio de Minas y Energía y otras entidades de índole estatal. De igual forma se debe mencionar que en la región Andina, la Costa Norte y el piedemonte llanero, donde se concentra la mayor parte de la población colombiana, la carretera es el principal medio de transporte para personas y carga (Ministerio de transporte, 2005).

Actualmente existe un sistema de buses de varias empresas que operan entre las principales ciudades y pueblos ofreciendo transporte. El sistema está constituido por la Red Primaria (Grandes Troncales, A cargo de la Nación), Red Secundaria (A cargo de Departamentos y municipios) y Red Terciaria (constituida por carreteras terciarias o caminos vecinales, que son aquellos de penetración que comunican una cabecera municipal o población con una o varias veredas, o aquella que une varias veredas entre sí) (Ministerio de transporte, 2005).

De otra parte se debe decir que en la actualidad la información es un activo valioso que puede impulsar o destruir la 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 es necesario afirmar que la empresa Transportadores de Norte de Santander SAS, 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. De igual forma no se ha tomado conciencia por parte del gerente y empleados, 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 empresa.

1.2 Formulación del problema

¿Cómo se puede verificar la vulnerabilidad de la información en la empresa Transportadores de Norte de Santander SAS?

1.3 Objetivos

1.3.1 General. Evaluar la seguridad en la información para la empresa Transportadores de Norte de Santander SAS, basados en la norma ISO 27001:2013.

1.3.2 Específicos. Realizar un diagnóstico a la situación actual de la empresa Transportadores de Norte de Santander SAS en cuanto a la seguridad de la información.

Mencionar los dominios de la norma ISO 27001:2013 y su importancia en la seguridad de la información.

Determinar una metodología adecuada para la evaluación de la seguridad de la información existente, en la empresa de Transportes de Norte de Santander SAS.

Elaborar un informe de recomendaciones de acuerdo a los hallazgos identificados.

1.4 Justificación

En el mundo de la Seguridad de la Información, la solución a los problemas planteados no se puede buscar en una herramienta o tecnología a utilizar, sino en una serie de políticas,

procedimientos y buenas prácticas que, apoyándose en las distintas tecnologías, permita mejorar el nivel de protección de la información sensible, sin olvidar que toda esta gestión se apoya también en el eslabón humano. Una vez se llega a la conclusión de que la Seguridad de la Información es un proceso en el que se debe combinar distintas medidas de seguridad para conseguir el objetivo. Para ello, se deben apoyar en las normativas y buenas prácticas existentes, como las normas ISO 27001:2013 y, por supuesto, en las distintas soluciones tecnológicas que ayudan a cumplir el objetivo final, que no es otro que proteger la información sensible en cualquier formato, evitando un posible mal uso de la misma o su extravío, ya sea de una manera accidental o intencionada (Berciano, 2018).

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 empresa, 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.

Por último se debe tener un análisis de riesgos en la empresa, 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.

De igual forma se debe decir que para la empresa es muy importante el trabajo de grado, ya que el establecimiento de metodologías, prácticas y procedimientos que buscan proteger la información como activo valioso, es el objetivo del conjunto de estándares de la ISO/IEC 27000. En este sentido, se debe minimizar las amenazas y riesgos continuos a los que está expuesta cualquier organización y a efectos de asegurar la continuidad de negocio y minimizar los daños que se puedan presentar.

1.5 Delimitaciones

1.5.1 Geográfica. El desarrollo del trabajo de grado se llevó a cabo en la ciudad de Ocaña, Norte de Santander, específicamente en la empresa de Transportes de Norte de Santander SAS.

1.5.2 Temporal. El proyecto de grado se realizó en dos (2) 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 presentaron 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 de la empresa a nivel internacional.

La Seguridad Informática ha experimentado un profundo cambio en los últimos años. Inversiones aisladas llevadas a cabo con el objetivo de fortalecer la seguridad en puntos muy concretos han dado paso a inversiones para asegurar el bien más valioso de la empresa, la información, enfocando la seguridad hacia los procesos de negocio de la empresa. Durante los años 80 y principios de los 90 la Seguridad Informática se centraba en proteger los equipos de los usuarios, es decir, proporcionar seguridad a los ordenadores y su sistema operativo. Esta seguridad lógica, entendida como la seguridad de los equipos informáticos para evitar que dejasen de funcionar correctamente, se centraba en la protección contra virus informáticos (Grupo control seguridad, 2016).

Con la aparición de Internet y su uso globalizado a nivel empresarial la Seguridad Informática comenzó a enfocarse hacia la conectividad de redes o networking, protegiendo los equipos servidores de aplicaciones informáticas, y los equipos servidores accesibles públicamente a través de Internet, y controlando la seguridad a nivel periférico a través de dispositivos como Firewalls. Es decir, la posibilidad tecnológica de “estar conectados” llevaba implícita la aparición de nuevas vulnerabilidades que podían ser explotadas, la exposición de

información crucial para el negocio que podía ser accesible precisamente gracias a esa conectividad (Grupo control seguridad, 2016).

El perfil de atacante de un sistema informático ha cambiado radicalmente. Si bien antes los objetivos de un atacante o hacker podían ser más simples (acceder a un sitio donde nadie antes había conseguido llegar, o infectar un sistema mediante algún tipo de virus, pero sin ningún tipo de ánimo de lucro), en la actualidad los atacantes se han percatado de lo importante que es la información y sobre todo de lo valiosa que puede ser. Se trata de grupos organizados que aprovechan las vulnerabilidades de los sistemas informáticos y las redes de telecomunicaciones para acceder a la información crítica y sensible de la empresa, bien a través de personal especializado en este tipo de ataques, o bien comprando en el mercado negro kits de explotación de vulnerabilidades para obtener información muy específica.

Los nuevos vectores de ataque, el cambio en los perfiles de los atacantes, y sobre todo la importancia crucial de la información clave y crítica para el negocio de una empresa, hacen que el concepto de Seguridad Informática haya evolucionado hacia el concepto de Seguridad de la Información, cuyo objetivo principal consiste en alinear las inversiones en seguridad con los objetivos generales de la empresa y sus estrategias de negocio. La Seguridad de la Información se basa en el diseño de Políticas de Seguridad integrada en los planes estratégicos de la empresa. Para la definición de dichas Políticas es necesario tener en cuenta diversos factores, tales como la localización de la empresa, tamaño y número de sedes, condicionantes geográficos, cumplimientos legales y normativas vigentes, normas ISO de la empresa, etc (Grupo control seguridad, 2016).

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)

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).

En el proyecto de titulación se pretende dar una adecuada solución de seguridad a la empresa A&CGroup S.A., la cual consiste en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), tomando como base el estándar ISO 27001:2005.

El primer capítulo, el marco teórico, se refiere a revisar los conceptos básicos que van a permitir tener una visión clara del conjunto de acciones necesarias para que la entidad involucrada pueda contar con un sistema para la seguridad y gestión de riesgos de la información. Por otra parte, en el segundo capítulo se presentan los antecedentes del proyecto, en donde se describirá el problema, la solución propuesta, el objetivo general y los objetivos específicos (Tola Franco, 2015).

En el tercer capítulo, se detalla el levantamiento de información necesario para la implementación del SGSI (Sistema de Gestión de Seguridad de la Información). El cuarto capítulo trata sobre la metodología PDCA (Plan – Do – Check - Act) y los conceptos por cada una de las etapas implicadas en el modelo. Se detalla el alcance que se desea establecer, indicando los lineamientos y principios a implementar, mantener y así mejorar la gestión de la seguridad de la información dentro de la empresa; continuando con una breve descripción de las políticas generales que se deben aplicar.

El quinto capítulo describe la metodología para la gestión del riesgo con el concepto y ventajas principales de su implementación, se detalla el inventario de activos de información dentro de la organización y se especifica el análisis de riesgo con sus apropiados criterios de valoración; de igual manera se realiza la evaluación del riesgo dentro del cual se procede a describir la metodología para calcular los valores de riesgo y la selección de las estrategias para el tratamiento de los mismos (Tola Franco, 2015).

El desarrollo del sexto capítulo se centra en la explicación de la implementación de las políticas y el plan de tratamiento a utilizar para la debida gestión de riesgos que se encontraron. Por último, en el séptimo capítulo se muestra el análisis de los resultados obtenidos y las estrategias de difusión aplicadas en la empresa. Se presentan las conclusiones y recomendaciones, así como los anexos del trabajo realizado (Tola Franco, 2015).

Por otra parte (Espinoza Aguinaga, 2013), en los últimos 20 años la información se ha convertido en un activo muy importante y crucial dentro de las organizaciones. Por esta razón la organización tiene la necesidad de protegerla si es que la información tiene relación ya sea con el negocio o con sus clientes. Para gestionar la información y su seguridad, las entidades pueden adoptar alguna de las normas y buenas prácticas existentes en el mercado. Para el caso de una empresa del rubro de producción y distribución de alimentos de consumo masivo, también aplica esta necesidad de proteger la información.

Por ejemplo, en unos de sus principales procesos que es el de producción, está implicada información de gran importancia para la empresa, como "recetas" de productos, programación de manufactura, sistemas que se usan, tipos de pruebas de calidad de producto, etc., la cual debe estar resguardada correctamente para evitar que dicha información se pierda o caiga en manos indebidas y así garantizar que se logren los objetivos del negocio. En el presente proyecto de fin de carrera se tomaran en cuenta los aspectos más importantes de la norma ISO/IEC 27001:2005, a partir de los cuales se buscará poder desarrollar cada una de las etapas del diseño de un sistema de gestión de seguridad de información para que pueda ser empleado por una empresa dedicada a la producción de alimentos de consumo masivo en el Perú, lo cual permitirá que ésta cumpla con

las normas de regulación vigentes en lo que respecta a seguridad de información (Espinoza Aguinaga, 2013).

Para efectos del análisis de riesgos para este proyecto de tesis, se decidió trabajar con el proceso de producción, ya que se consideró que era el proceso más importante dentro del funcionamiento de la empresa. Este proceso de producción a su vez se dividió en 4 subprocesos que lo conforman, los cuales fueron el proceso de planificación, manufactura, calidad y bodegas e inventarios (Espinoza Aguinaga, 2013).

2.1.2 Antecedentes de la seguridad en la información de la empresa a nivel nacional.

Colombia está bien posicionada en el mundo en manejo de ciberseguridad, de acuerdo con la clasificación global de la Unión Internacional de Telecomunicaciones (UIT). El informe ubica el país en el quinto lugar en la lista de las Américas, por encima de Chile y México, y ocupa el noveno lugar en la tabla mundial, frente a países como Francia, España, Egipto y Dinamarca.

La UIT publica el Índice Mundial de Ciberseguridad (IMC), que evalúa el grado de desarrollo de la ciberseguridad en cada país y, según la propia organización: "tiene el objetivo fundamental de fomentar la cultura mundial de la ciberseguridad y su integración en el núcleo de las tecnologías de la información y la comunicación". La empresa de seguridad informática Fortinet realizó un diagnóstico sobre los ataques que reciben los sistemas del gobierno colombiano. Según las cifras que recolectó, la Nación es víctima del 3 % de los ataques, lo que no necesariamente significa que sea víctima de los piratas cibernéticos. Pero es claro que los

delincuentes intentan robar datos del Estado mediante ataques (Seguridad en la información Colombia, 2015).

El año anterior el gobierno Santos había anunciado la creación de la 'Agencia Nacional de Seguridad Cibernética', que estaría liderada por el ministerio de Defensa con la colaboración del MinTic, pero el proyecto sigue en estructuración. Mientras tanto, las amenazas que recibe el Gobierno las enfrenta el Centro Cibernético Policial, adscrito a la Policía Nacional. De acuerdo con el Boletín 002 de la entidad, la Policía nacional evitó más de 822 sitios de pornografía infantil en el 2014 y ha realizado más de 422 capturas por delitos informáticos. En cuanto a la seguridad de sitios gubernamentales, se registraron más de 200 denuncias de ataques cibernéticos a sitios con información sensible para los colombianos (Seguridad en la información Colombia, 2015).

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." (MINTIC, 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. (MINTIC, 2012)

Según (Chacon Hurtado, 2016), en los últimos años, la computación en la nube ha tenido un incremento en su utilización. Se espera que dentro de los próximos 5 a 10 años este modelo de despliegue de servicios esté en una fase de producción, y que no sea de uso exclusivo de expertos en tecnologías de información y comunicaciones, sino también de académicos, empresarios y personas comunes que se vean atraídos por las ventajas ofrecidas por este modelo.

La seguridad de la información es uno de los aspectos que más preocupan a los directivos de TI para migrar sus aplicaciones e información a la nube, debido a que están confiando sus datos privados a un tercero. Por este motivo, las organizaciones toman medidas que garanticen el control de su información y que minimicen los riesgos que la pueden impactar, basándose en estándares de seguridad pensados para la computación tradicional. Existen iniciativas y marcos de trabajo, tales como PCI o CSA, que pueden aportar información, pero al no haber un modelo completo de seguridad para la computación en la nube, existe la posibilidad de no hacer consciencia de los diferentes riesgos, o tratarlos de forma inadecuada.

De otra parte en este documento se centra en la aplicación de la norma ISO/IEC 27001 en atención a los numerales 4.2.2 Implementación y Operación de un Sistema de Gestión de la Seguridad de la Información (por sus siglas, SGSI), identificando las acciones de: la gestión

apropiada, prioridades y responsabilidades de la gerencia en la creación de políticas que garanticen el cumplimiento de los objetivos del SGSI, además se hace referencia a la creación de planes de acción para el tratamiento, análisis y gestión de los riesgos implementando procedimientos que brindan una atención oportuna a los incidentes de seguridad de la información, acompañados de estrategias de capacitación y formación para los integrantes de la organización (Ayala Gonzalez & Gómez Izasa, 2011).

2.1.3 Antecedentes de la seguridad en la información de la empresa a nivel local.

Según la investigación realizada en el hospital de Rio de Oro, mediante un SGSI – sistema de gestión de seguridad de la información, el área de contabilidad de la E.S.E hospital local de Rio de Oro Cesar conseguirá minimizar considerablemente el riesgo de que su productividad se vea afectada debido a la ocurrencia de un evento que comprometa la confidencialidad, disponibilidad e integridad de la información o de alguno de los sistemas informáticos. Este sistema permite identificar, gestionar y minimizar los riesgos reales y potenciales de la seguridad de la información, de una forma documentada, sistemática, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. Esta investigación busca darle un tratamiento diferente a la información en la cual se basa en centralizar el diseño del SGSI, solo en los procesos contables que maneja el hospital de rio de oro, recomendando pautas para el mejoramiento de los procesos contables (Casadiego Santana, Quintero Jimenez, & Toro Ruedas, 2014).

De otra parte 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.

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 (Sanjuán Muñoz, 2017).

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 (Sanjuán Muñoz, 2017).

2.2 Marco contextual

La empresa Transportadores de Norte de Santander SAS, fue registrada bajo el número de identificación tributaria 900 719 398-8 y en la actualidad se encuentra ubicada en la calle 7A No 35 -40 APTO 201, barrio la Primavera, de otra parte se tiene como actividad principal el transporte de carga por carretera. De otra parte se debe decir que la sociedad tiene por objeto principal el desarrollo de la industria del transporte terrestre automotor público en la modalidad de carga, en el ámbito nacional e internacional a través del empleo de todos los medios y en sus variadas modalidades, además puede realizar actividades como el transporte de crudo y todos sus derivados, combustibles, carga masiva, ganado, encomiendas, giros, servicios mecánicos, reparación automotriz, compra y venta de productos, repuestos, combustibles, lubricantes, llantas, servicio de lavado y engrase, compra y venta de vehículos.

Además de lo anterior la empresa puede contratar medios de transporte, representar firmas nacionales o extranjeras, almacenas, distribuir, empacar, reempacar y manipular todo tipo de bienes, entre otras inherentes a su actividad económica. De otra parte la empresa TNS se conformó en el año 2014 en Ocaña, Norte de Santander, con el esfuerzo y unión de un grupo de

64 socios, quienes detectaron las necesidades para transportar los principales tipos de carga de la región a todo el territorio nacional, la sociedad contaba con una amplio parque automotor que les respaldaba para un crecimiento importante dentro del sector de transporte.

La empresa abrió sus puertas desde el mes de febrero de 2014 en Ocaña, Norte de Santander, radicando en la Cámara de Comercio su constitución el 8 de abril del mismo año. En el mes de agosto de 2014 se obtuvo autorización del ministerio de transportes mediante Resolución 264. Sus inicios de carga se dieron en el mes de septiembre; en la actualidad nuestra empresa cuenta con 60 vehículos cisterna y aproximadamente 130 vehículos tipo carrocería para carga seca (Páez García, 2009).

La empresa cuenta con un grupo interdisciplinario, compuesto por profesionales destacados y transportadores con amplia experiencia, con combinación correcta de conocimientos y habilidades. Para TNS el recurso humano es el activo más significativo, cada integrante del capital humano es consistente de la importancia de su trabajo dentro de la organización y está comprometido con la misión y visión de la misma. La capacidad permanente ha garantizado el mejoramiento continuo de los procesos y de esta manera superar la experiencia de nuestros clientes.

Se cuenta con la misión de ser una empresa regionalista colombiana que provee servicios de transporte terrestre de carga líquida y seca a nivel nacional de forma segura y eficaz, generando satisfacciones a nuestros clientes y garantizando el crecimiento económico social y cultural de nuestros asociados empleados y la comunidad.

La visión es que el año 2017 se consolide como una organización líder en la operación logística de carga terrestre de la región Norte de Santandereana, mejorando continuamente la calidad de sus servicios y superando las expectativas de los clientes (Acosta López, 2015).

2.3 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)

Sistema de Gestión de Seguridad de la Información (SGSI). 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) (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)

2.4 Marco teórico.

Según (Sierra Jaramillo, 2011), la posibilidad de monitorear los principales procesos asegurando su efectividad, posibilidad de llevar registros apropiados de la gestión, de los procesos y de los procedimientos, mejora la satisfacción de los usuarios o clientes, la mejora continua de los procesos, tanto en operación como en calidad, reducir las incidencias en la producción o prestación del servicio, las normas aparecieron por primera vez en 1987 teniendo como base la norma estándar británico, su gran extensión es a partir de la versión de 1994, y actualmente se encuentra en la versión 2008, publicada el 13 de noviembre de 2008.

Con la revisión del año 2000 se consiguió una norma menos burocrática para las organizaciones, pudiéndose aplicar sin ningún problema a empresas de servicios e incluso a la administración pública.

Para realizar los procesos de verificación, existen entidades de certificación que dan sus propios certificados con su sello. Estas entidades están vigiladas por organismos nacionales que dan su acreditación. Si se desea implementar la norma por primera vez es conveniente que se apoye en una empresa de consultoría, que tenga buenas referencias, y el compromiso de la dirección de la organización que quiera implementar el sistema, debido a que se requiere personal de la empresa para implementarlo (Sierra Jaramillo, 2011).

La organización que cumple con la norma ISO 9001:2008 cumple con los requisitos básicos en cuanto a la norma de calidad. Si se quiere ir más allá se debe cumplir con requisitos adicionales. La ISO 9004:2000 establece estos requisitos adicionales.

Sistema de gestión de la calidad significa disponer de una serie de elementos como manual de calidad, procedimientos de inspección, instrucciones de trabajo, plan de capacitación, registros de la calidad, todo hace parte de un equipo para producir bienes y servicios de la calidad requerida por los clientes (Sierra Jaramillo, 2011).

De otra parte 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)

Es necesario también decir que los objetivos del cobit es el control para la Información y la Tecnología relacionada (COBIT), brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, presentando las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de los expertos, están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones relacionadas con tecnología de la información TI, asegurarán la entrega del servicio y brindarán una medida con base en la cual comparar o medir cuando las cosas no vayan bien. Para que la TI tenga éxito en satisfacer los requerimientos del negocio, la dirección debe implantar un sistema de control interno o un marco de trabajo (Sierra Jaramillo, 2011).

El marco de trabajo de control COBIT contribuye a estas necesidades de la siguiente manera:

Estableciendo un vínculo con los requerimientos del negocio.

Organizando las actividades de TI en un modelo de procesos.

Identificando los principales recursos de TI a ser utilizados.

Definiendo los objetivos de control gerenciales a ser considerados.

La orientación al negocio que enfoca COBIT consiste en vincular las metas de negocio con las metas de TI, brindando métricas y modelos de madurez para medir sus logros, e identificando las responsabilidades asociadas de los propietarios de los procesos de negocio y de TI.

El enfoque hacia procesos de COBIT se ilustra con un modelo de procesos, el cual subdivide TI en 34 procesos de acuerdo a las áreas de responsabilidad de planear, construir, ejecutar y monitorear (Sierra Jaramillo, 2011).

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.

Dado el propósito de la presente investigación la cual es evaluar la seguridad en la información para la empresa Transportadores de Norte de Santander SAS, basados en la norma ISO/IEC 27001:2013, para lo cual se llevó a cabo una investigación cualitativa, ya que de acuerdo con una de sus definiciones, "es aquella donde se estudia la calidad de las actividades, relaciones, asuntos, medios, materiales o instrumentos en una determinada situación o problema.

La misma procura por lograr una descripción holística, esto es, que intenta analizar exhaustivamente, con sumo detalle, un asunto o actividad en particular" (Vera Velez, 2017).

Partiendo de esta definición, la investigación cualitativa, permitirá comprender y explorar los elementos que intervienen en la evaluación en mención, logrando determinar que ésta puede ser la mejor opción para optimizar los procesos de la empresa Transportadores de Norte de Santander SAS a través del uso eficiente de las tecnologías de información y comunicación (Ibáñez, 2017).

3.2 Población y muestra.

3.2.1 Población. La población estuvo conformada por 9 empleados del área administrativa de la empresa Transportadores de Norte de Santander SAS.

3.2.2 Muestra. Teniendo en cuenta que la población es muy reducida se tomó en su totalidad.

3.3 Técnicas para la recolección de la información.

Como técnica de indagación directa se utilizará 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, de igual forma se aplicó una entrevista a los nueve empleados del área administrativa, para poder determinar la seguridad real que posee y por último una lista de verificación para corroborar la información suministrada por los empleados.

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 Diagnóstico a la situación actual de la empresa Transportadores de Norte de Santander SAS en cuanto a la seguridad de la información.

La empresa Transportadora de Norte de Santander S.A.S, se conformó en el año 2014 en Ocaña, Norte de Santander, con el esfuerzo y unión de un grupo de 64 socios, quienes detectaron las necesidades para transportar los principales tipos de carga de la región a todo el territorio nacional, la sociedad contaba con un amplio parque automotor que les respaldaba para un crecimiento importante dentro del sector de transporte. La empresa abrió sus puertas desde el mes de febrero de 2014 en Ocaña Norte de Santander, radicando en Cámara de Comercio su constitución el 8 de abril del mismo año. En el mes de agosto de 2014 se obtuvo autorización del Ministerios de Transporte mediante Resolución 264. Sus inicios de carga se dieron en el mes de septiembre; en la actualidad nuestra empresa cuenta con 60 vehículos cisternas y aproximadamente 130 vehículos tipo carrocería para carga seca (Acosta Lopez, 2017).

Transportadores del Norte de Santander es una empresa regionalista Colombiana que provee servicios de transporte terrestre de carga líquida y seca a nivel nacional de forma segura y eficaz, generando satisfacción a nuestros clientes y garantizando el crecimiento económico, social y cultural de nuestros asociados, empleados y la comunidad, de igual forma pretende para el año 2022 consolidarse como una organización líder en la operación logística de carga terrestre de la región Norte Santandereana, mejorando continuamente la calidad de sus servicios y superando las expectativas de los clientes (Acosta López, 2015).

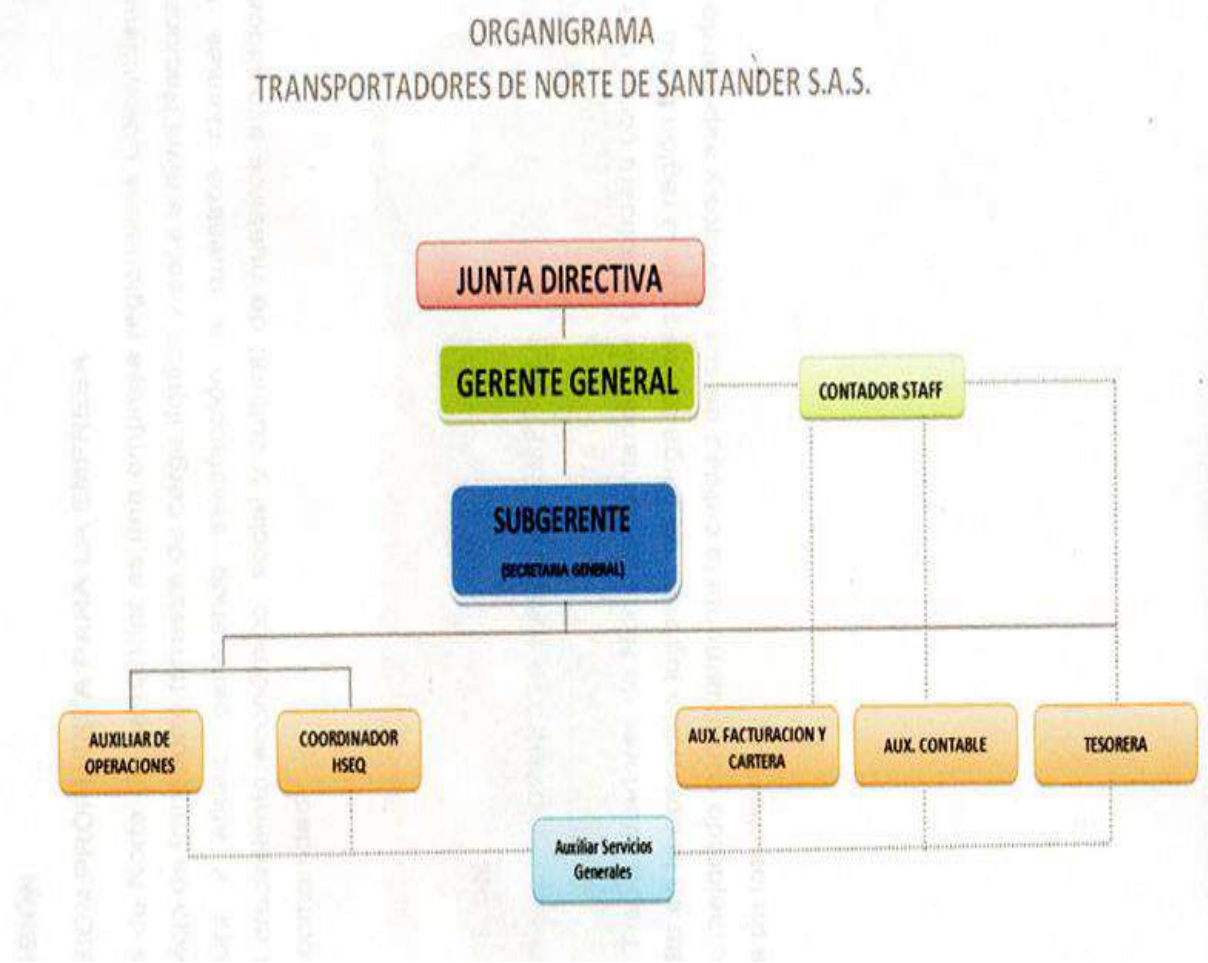


Figura 1. Organigrama

Fuente. Eddie Jesús Acosta López.

De otra parte los valores corporativos definidos para TNS son de vital importancia y hacen parte de nuestra cultura organizacional son:

Unidad Familiar. Es entender que la célula fundamental de la sociedad es la familia y que debe preservarse sana, unida y en armonía.

Lealtad. Es honrar la confianza recibida; es no defraudar a quienes han depositado su confianza en nosotros.

Autocuidado. Desarrollar en las personas la responsabilidad para consigo mismas y su integridad física.

Responsabilidad. Es cumplir todo lo que una persona libremente se comprometió a hacer con los demás y consigo mismo (autocontrol).

Consideración. Entendido como el reconocimiento y la atención que merecen las personas. Este valor contiene otros valores y actitudes como el orden, el aseo, la organización, la puntualidad y la planificación, entre otros.

Transparencia. Que no haya discrepancia entre lo que se dice y lo que se hace o practica, enfocado en actitudes de honradez y rectitud.

Conciencia ambiental. Es entender la necesidad de aprovechar los recursos naturales racionalmente, y hacerlo.

Creatividad. Capacidad de idear soluciones originales para los problemas, y en términos efectivos mejorar lo existente.

Trabajo en equipo. Es la actitud que nos lleva a comprender que nuestro trabajo es influido por los demás, sin perder de vista los objetivos estratégicos de la empresa, y la voluntad de ayudarle a los demás.

Mejoramiento continuo. Es estar convencido de que lo que se haga hoy se puede mejorar hacia el futuro y, además, tratar de obtenerlo.

Patriotismo. Procura cultivar el respeto y amor que debemos a la patria, mediante nuestro trabajo honesto y la contribución personal al bienestar común.

Comunicación. Nos ayuda a intercambiar de forma efectiva pensamientos, ideas y sentimientos con las personas que nos rodean, en un ambiente de cordialidad y buscando el enriquecimiento

personal de ambas partes. Entender y hacerse comprender es un arte que facilita la convivencia y la armonía en todo lugar (Acosta Lopez, 2017).

Teniendo como objetivo la evaluación de la seguridad en la información para la empresa Transportadores de Norte de Santander SAS, basados en la norma ISO 27001:2013, se diseñó una entrevista, elaborado con un cuestionario de preguntas abiertas, aplicada a los nueve empleados de la entidad y donde los mismos afirman que la seguridad en la información es muy baja ya que se corren riesgos como es la perdida de la información, sin tener copias de seguridad que eviten tal situación.

Además se desconoce que la información es un activo fundamental para el desarrollo, operativa, control y gestión del Modelo de Negocio / Servicio de cualquier Organización.
A través de sus Sistemas de Información se canalizan la práctica totalidad de las actividades corporativas, 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.

Hoy en día se le debe dar mucha importante a 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. En los entornos globalizados actuales, donde las transacciones de negocio (Empresas) y servicio (Administraciones Públicas) llevan en su praxis el sufijo "electrónico", esta prioridad se maximiza ante las especiales características del medio en que se desarrollan y sus riesgos asociados.

Estas cuestiones derivan en la existencia de una serie de Normas estándares, aceptadas como acreditaciones de la Seguridad de la Información universalmente, y cuya implementación aporta a la Organización no solo una certificación reconocida sino, como punto fundamental, una cultura y práctica de la Seguridad que le aporta valores al negocio / servicio en muy diferentes aspectos.

Mejora de la competitividad

Mejora de la imagen corporativa

Protección y continuidad del negocio

Cumplimiento legal y reglamentario

Optimización de recursos e inversión en tecnología

Reducción de costes

La norma ISO/IEC 27001 especifica los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información (SGSI).

Entre las actividades propias a desarrollar al abordar una implantación a ISO27001 se encuentran:

Definición del alcance del SGSI

Definición de una Política de Seguridad

Definición de una metodología y criterios para el Análisis y Gestión del Riesgo

Identificación de riesgos

Evaluación de los posibles tratamientos del riesgo

Elaboración de una Declaración de Aplicabilidad de controles y requisitos

Desarrollo de un Plan de Tratamiento de Riesgos

Definición de métricas e indicadores de la eficiencia de los controles

Desarrollo de programas de formación y concienciación en seguridad de la información

Gestión de recursos y operaciones

Gestión de incidencias

Elaboración de procedimientos y documentación asociada

La plena integración con la Capa Operativa de GesConsultor GRC ofrece una colección diferencial de automatismos que permiten conseguir niveles máximos de calidad en la implementación, mantenimiento y evolución del SGSI. Así, se minimizan las cargas internas de trabajo, sistematizando las operaciones y controles relacionados con la Seguridad TIC y enlazando directamente con los requerimientos de ISO/IEC 27001 (Monitorización, Métricas e Indicadores, Incidentes, Seguridad Gestionada, Vulnerabilidades, Formación, Gestión de Recursos, etc.).

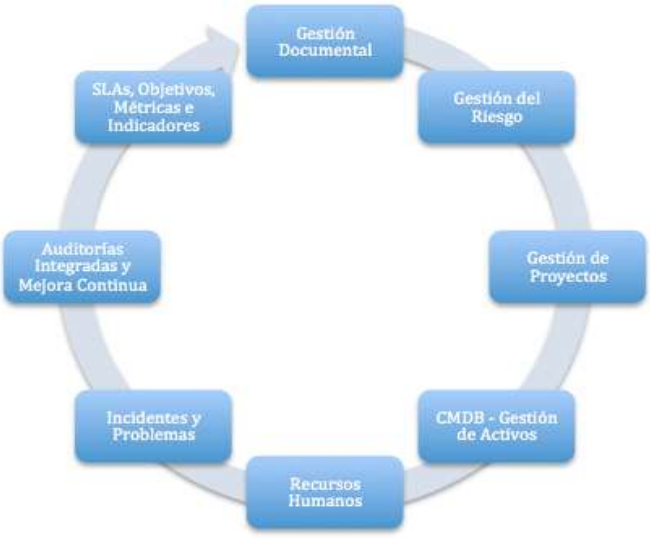


Figura 2. Sistema de Gestión de la Seguridad de la Información

Fuente. ISO 270001 del 2013

Teniendo en cuenta la entrevista realizada a los empleados de la empresa Transportes de Norte de Santander SAS, afirman que el computador asignado para cumplir con las actividades asignadas no recibe mantenimiento periódico, esto porque en la empresa no existe el sistema de gestión de seguridad de la información, por lo que la información de la empresa corre mucho peligro, por otra parte la empresa realiza pocas capacitaciones en cuanto a la forma como los empleados deben proteger la información y a esto se suma que no se tiene una política clara para la protección de la información contraseñas en los equipos.

De otra parte todos los empleados afirman que al ingresar a la empresa no se les entrega el manual de los equipos, por lo que desconocen cuál es su funcionamiento y el cuidado que deben tener con ellos, por lo que cuando ocurre un evento relacionado con la seguridad de la información se desconoce a quien se deben dirigir, de igual forma no se realizan copias de seguridad, por lo que se evidencia la necesidad que la empresa invierta en la implementación de un sistema de seguridad de la información basado en la ISO 27001 y así asegurar un activo muy importante de la empresa como es la información.

La mayoría de empleados afirman que en muchas ocasiones han recibido equipos sin antivirus siendo esto lo más mínimo que deben tener, en cuanto al software legal se dice que desconocen si cuentan con la legalidad o no, de otra parte las equipos que manejan información importante para la empresa no están en una zona restringida, lo que hace que con mayor razón la información esté en riesgo.

Por otra parte manifiestan que en el mantenimiento no se tiene en cuenta la prevención de los daños y riesgos, de igual forma como no hay zonas restringidas, pues lógicamente no existe seguridad a dichas zonas, otro aspecto muy importante son las alarmas en caso de incendio, humo y demás que pueden llegar a afectar los equipos, estas son nulas en la entidad, de igual forma los equipos están ubicados en las oficinas y por lo tanto no se cuenta con aire acondicionado, ya que se afirma que el clima de Ocaña no lo requiere, por otra parte según las preguntas realizadas los equipos no estas asegurados con pólizas y demás, constituyendo otra debilidad para la información de la empresa y por último no se tienen controles en la navegación a internet y uso de correo electrónico, por lo que se puede decir que la seguridad en la empresa es bastante baja. Por último y teniendo en cuenta los riesgos de la información evidenciados a lo largo de la investigación en la empresa se elaboró una matriz de riesgos, donde el color verde es bajo, amarillo medio y rojo alto.

Tabla 1.

Hallazgos encontrados de acuerdo a la entrevista aplica.

Hallazgos	**CUMPLE**	
	SI	**NO**
No existe mantenimiento de los equipos		X
Inexistencia de manual de equipos		X
Equipos sin antivirus		X
Falta de prevención de daños y riesgos		X
No hay zonas restringidas		X
Acceso a todos los equipos		X
No existe el departamento de sistemas		X
Falta control de la información		X

Nota. Fuente. Autores del proyecto

En la actualidad los sistemas de información han tomado valor en las diferentes organizaciones que manejan recursos de posición y ubicación. La gestión de estos sistemas requiere como todo sistema de información una definición de normas de uso y administración adecuadas.

Por lo tanto la investigación estuvo orientada a realizar un análisis de riesgos de un sistema de información, en el que se tratan las técnicas de seguridad de la norma ISO/IEC 27001, se pretende identificar los riesgos con mayor probabilidad de suceso ante un análisis de impacto/probabilidad, y así mismo establecer los controles o medidas de protección correspondientes al riesgo para proteger los activos de la empresa que es la información, es por esto que de acuerdo a la entrevista se determinaron los riesgos a los que se les dio una valoración de alto, medio y bajo, de igual forma dependiendo del riesgo se le dio un color de rojo-alto, amarillo-medio y verde-bajo.

Tabla 2.

Riesgos a los que esta sometida la información en la empresa.

Riesgos	Evaluación
Físicos	
Incendios, sobre carga eléctrica	Medio
Polvos, falta de ventilación	Medio
Falta de inducción, capacitación y sensibilización sobre riesgos	Alto
Perdida de datos por error de los empleados	Alto
Infección de sistemas a través de unidades portables sin escaneo	Alto
Perdida de datos por error hardware	Bajo
Falta de mantenimiento físico (proceso, repuestos e insumos)	Alto
Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Alto
Red cableada expuesta para el acceso no autorizado	Alto
Ausencia de documentación	Alto
Acceso electrónico no autorizado a sistemas internos	Alto
Manejo inadecuado de contraseñas.	Alto

Nota. Fuente. Autores del proyecto

4.2 Dominios de la norma ISO 27001:2013 y su importancia en la seguridad de la información.

Dominio del aspecto administrativo. 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.

Dominio de gestión de activos. Este dominio tiene el objetivo de llevar a cabo una protección adecuada en cuanto a los activos de la empresa.

En todo momento los activos se encuentran inventariados y controlados por un responsable que también se encarga de manipularlos de forma correcta.

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.

Dominio sobre la 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 enfocado 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.

Dominio de seguridad de los recursos humanos. Su objetivo es fijar las medidas necesarias para controlar la seguridad de la información, que ha sido manejada por los recursos humanos de la empresa.

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.

Dominio en cuanto la seguridad física y del medio ambiente. Con este dominio se consigue proteger todas las instalaciones de la empresa y toda la información que maneja. Por esto, se establecen diferentes barreras de seguridad y controles de acceso**.**
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.

Dominio gestión de las comunicaciones y operaciones. El objetivo se encuentra en determinar los procesos y responsabilidades de las operaciones que lleva a cabo la organización. Se debe asegurar que todos los procesos se encuentren relacionados con la información ejecutada de forma adecuada**.** Este es el dominio más amplio, en él 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.

Dominio control de acceso. Se asegura el acceso autorizado a todos los sistemas de información de la empresa**.** Es necesario realizar diversas acciones como controles para evitar el acceso de usuarios no autorizados, controles de entrada, etc.

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.

Dominio de adquisición, desarrollo y mantenimiento de los sistemas de información. Este dominio se encuentra dirigido a aquellas empresas que desarrollen software internamente o que tenga un contrato con otra empresa que se encarga de desarrollarlo. Se tiene que establecer los requisitos en la etapa de implantación y desarrollo de software para que sea seguro.

Dominio de gestión de incidentes en la seguridad de la información. Con este dominio se aplica un proceso de mejora continua en la gestión de percances de seguridad de la información.

Dominio de gestión de continuidad de negocio. El objetivo es asegurar la continuidad operativa de la empresa**.** Se requiere aplicar controles que eviten o reduzcan todos los incidentes de las actividades desarrolladas por la empresa que puedan generar un impacto.

Dominio de cumplimiento. Su finalidad es asegurar que los requisitos legales de seguridad que han sido referidos al diseño y gestión de los sistemas de información de este hace parte los siguientes aspectos.

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**.**

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.

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 empresa 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.

De igual forma se debe tener en cuenta que la gestión de los incidentes de seguridad es un aspecto muy importante para lograr el mejoramiento continuo en la empresa, siendo el principal inconveniente que muchas organizaciones no lo utilizan adecuadamente. A pesar que la norma ISO 27001, hace mención de este tema como uno de los dominios fundamentales, la gestión de los incidentes de seguridad es un aspecto muy importante para lograr el mejoramiento continuo de la seguridad de la información de cualquier ente económico, el principal inconveniente es que muchas organizaciones no lo utilizan adecuadamente.

El objetivo que se persigue los dominios es garantizar que las causas, los tratamientos y la solución de los eventos que puedan ocurrir se prevengan y corrijan adecuadamente y para lograrlo se deben implementar los canales apropiados que garanticen la agilidad en la comunicación de los eventos de seguridad que pudieran presentarse y permitir que los usuarios reporten las debilidades encontradas o que crean que pueden utilizarse para poner en riesgo la seguridad de la información. Estos sistemas pueden apoyarse en los desarrollo de los dominios.

4.3 Metodología adecuada para la evaluación de la seguridad de la información existente, en la empresa de Transportes de Norte de Santander SAS.

El tema de la seguridad de la información en las empresas, no es solamente un tema ético, sino que también involucra procesos administrativos asegurando una continua gestión de los riesgos y los niveles de seguridad requeridos por la organización. La norma ISO/IEC 27001, especifica el sistema de controles aplicables a la seguridad de la información alineados en cada uno de los dominios y procesos.

De otra parte para realizar la auditoría a la seguridad de la información, el proceso se dividió en etapas sucesivas y sistemáticas; en cada una de ellas se trata de establecer objetivos y metas claras con productos entregables, donde los productos resultado de la primera etapa servirán para adelantar la segunda y los de las segunda servirán para proseguir con la tercera etapa y así sucesivamente, ya que se plantea que la auditoría debe ser periódica o permanente dependiendo de la organización y los cambios en la tecnología de información usada en el tratamiento y procesamiento de la información.

Fase I. Determinación de vulnerabilidades, amenazas y riesgos: En esta fase se hace el estudio de las vulnerabilidades, amenazas y riesgos para los procesos y sistemas implementados actualmente en las organizaciones, que fueron objeto de la investigación. Para recolectar la información se aplicaron las técnicas de la observación directa, entrevista a los empleados de la empresa y una lista de verificación para corroborar la información dada por los entrevistados.

La entrevista diseñada y aplicada a los empleados de la empresa contiene un cuestionario de preguntas abiertas, las cuales son de fácil respuesta y la lista de verificación contiene una serie de pregunta las cuales el observados puede contestar si o no a la afirmación (Ver apéndice 3 y 4)

De otra parte se debe decir que según (Bernal, 2014), afirma que el ciclo PDCA, Es el sistema más usado para implantar un sistema de Gestión de la Seguridad de la Información. El nombre del Ciclo PDCA (o 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.

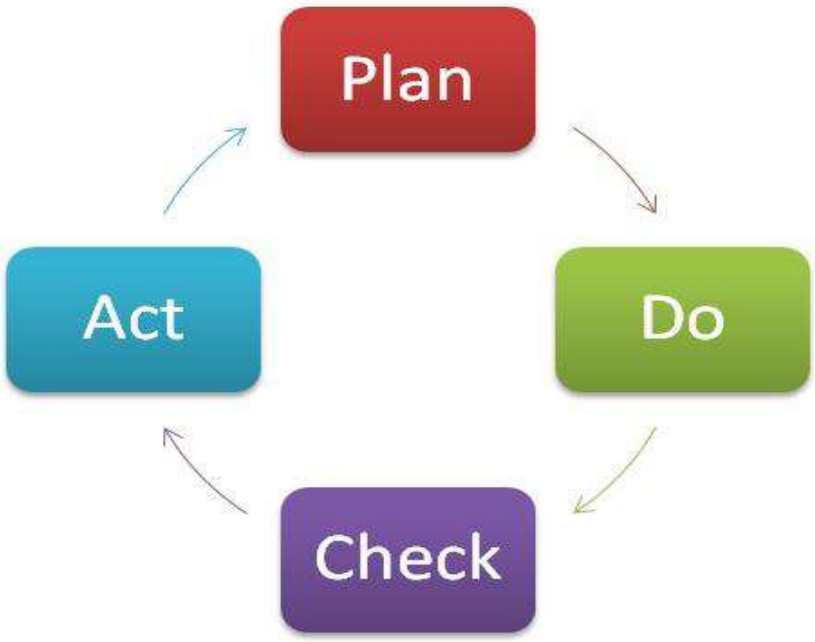


Figura 3. Ciclo PDCA.

Fuente. Bernal, 2014

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. (Bernal, 2013)

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. (Bernal, 2013)

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. (Bernal, 2013).

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. (Bernal, 2013).

Teniendo en cuenta que la auditoria es una revisión de los procesos donde se da a conocer un informe de lo encontrado y sus recomendaciones, se debe mencionar que para este trabajo de

investigación se tuvo en cuenta como objetivo la evaluación de la seguridad en la información para la empresa Transportadores de Norte de Santander SAS, basados en la norma ISO 27001:2013.

De igual forma como objetivo específico verificar la existencia y 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 de los cual no se tiene ninguno en el momento.

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:

Auditores

Criterios de auditoría. La auditoría realizada se llevó a cabo bajo el estándar ISO/IEC 27001.

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.

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.

Actividades.

Definición del objeto y los alcances de la auditoría.

Reunión del equipo de trabajo para definir responsabilidades y tareas

Diseño de instrumentos de recolección de información

Aplicación de instrumentos para la realización de la auditoría de cumplimiento bajo el estándar ISO 27001

Realización de entrevistas adicionales

Análisis de la información recolectada

Reunión Pre - Informe

Elaboración Informe de

Hallazgos de la auditoría**.** Para presentar los hallazgos, se tuvo en cuenta la entrevista y la lista de verificación (Ver apéndices 3 y 4)

4.4 Informe de recomendaciones de acuerdo a los hallazgos identificados.

El informe de auditoría es el resultado de la información, estudios, investigación y análisis efectuados por los auditores durante la realización de una auditoría, que de forma normalizada expresa por escrito su opinión sobre el área o actividad auditada en relación con los objetivos fijados, señalan las debilidades en cuanto a la seguridad en la información y formula recomendaciones pertinentes para eliminar las causas de tales deficiencias y establecer las medidas correctoras adecuadas.

En cuanto a la lista de verificación se debe decir que según la observación y preguntas realizadas se afirma que en muchos casos se ha perdido información, que no se ha podido recuperar y que es muy importante para el buen funcionamiento de la entidad, afortunadamente hasta el momento no se ha conocido que se halla divulgado información privada, se ha evidenciado que se insertan memorias y se para información de un equipo al otro lo que puede ser contraproducente ya que dicha información puede quedar en equipos menos protegidos.

En muchas ocasiones por olvidos personales, el equipo ha quedado funcionando o alguien lo ha prendido ya que en la empresa no se tiene control al respecto, por lo que ha pasado que archivos importantes han desaparecido sin saber quién es el culpable, en cuanto a la instalación de nuevos programas el vendedor del mismo hace una pequeña inducción del programa, orientando a los empleados en lo básico.

Se debe afirmar que cuando ha ocurrido daños en el sistema no se ha podido informa porque no hay una persona como tal encargada del sistema y de igual forma no hay un

departamento de sistemas y cuando hay ocurrido daños, los mismo empleados ha tratado de arreglar dichas averías pero como ya se dijo en muchas ocasiones la información se ha perdido lo que es un detrimento para la empresa y riesgo muy grande que asume la misma por lo valioso de la información, lo mismo ocurre cuando hay cortes de energía como no se tiene una copia de seguridad la información que se está elaborando o manejando en el momento se pierde lo que hace que los procesos se ven retrasados.

Teniendo en cuenta lo anterior se recomienda a la empresa trazar un perímetro seguro donde se recibe la información con el objetivo de evitar pérdidas y daños de la misma y así generar un ambiente seguro para la empresa y sus activos, de igual forma se debe ubicar un equipo estratégico donde se guarde toda la información con copias de seguridad y a donde no pueda acceder todo el personal.

Se debe tener una cuenta electrónica institucional con el fin de restringir el acceso a correos personales y así lograr la mayor protección de la información, la empresa debe contar con un personal autorizado y avadado por ellos para manejar la información confidencial.

De otra parte debe tener claro la empresa que la información manejada por ellos es un recurso que, como el resto de los activos, tiene valor para la organización y por consiguiente debe ser debidamente protegida. Es conveniente que se implemente medidas de seguridad comprendidas y aceptadas por la empresa, a efectos de asegurar su vigencia y nivel de eficacia, por lo que se debe establecer directrices, procedimientos y los requisitos para asegurar la protección oportuna y correcta de los equipos de comunicación en la empresa.

De igual forma para lograr una adecuada protección de la información se debe realizar actividades de protección a la información restringiendo el acceso a terceros a la información, 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.

Se debe buscar la seguridad física con el fin de minimizar los riesgos los riesgos de daños e interferencias a la información y a las operaciones de la empresa, de igual formar el control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio, como es la humedad.

Se debe adquirir sistemas de control que revisen constantemente 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 y por último se deben tomar un plan de riesgos con el objetivo de tomar acciones más apropiada de tratamiento para cada uno de las vulnerabilidades identificadas, con base a las secciones. Identificación de amenazas y identificación de vulnerabilidades.

Capítulo 5. Conclusiones

Teniendo en cuenta la entrevista y la lista de chequeo realizada en la empresa Transportadores de Norte de Santander SAS se pudo determinar, que la seguridad de la información en la empresa es muy baja y no se poseen controles necesarios para asegurarla.

Teniendo en cuenta la Norma ISO 27001:2013, se identificaron los dominios que posee la norma se mencionaron y se expuso su importancia para la seguridad de la información en la empresa.

De igual forma se tuvo en cuenta la metodología de planificar, hacer, verificar y actuar, como también se planifico la auditoria a realizar en el trabajo de grado.

Por último se elaboró el informe el cual estuvo basado en los hallazgos identificados en la elaboración de la auditoria.

Capítulo 6. Recomendaciones

Se recomienda continuar realizando diagnósticos de la situación actual en la empresa Transportadores de Norte de Santander SAS en cuanto a la seguridad de la información y así solucionar las debilidades encontradas.

Es conveniente que la empresa tenga en cuenta la importancia de la Norma para la seguridad de la información, al igual que los dominios y tenerlos como base para las próximas investigaciones.

Se debe tener en cuenta la metodología escogida para evaluar los riesgos y de igual forma se le recomienda a la empresa Transportes de Norte de Santander SAS, tener en cuenta aspectos de la Norma para la seguridad de la información en la empresa.

Por último es necesario 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

Acosta Lopez, E. J. (2017). *Informacion de la empresa.* Ocaña.

Aguilar. (2002). *Globalización y Capitalismo.* Mexico: Plaza & Janés.

Álvarez. (2009). *Manual de la Micro, Pequeña y Mediana Empresa. Una contribución a la mejora de los sistemas de información y el desarrollo de las políticas públicas.* San Salvador.

Alvarez, & Duran. (2009). *Manual de la Micro, Pequeña y Mediana Empresa. Una contribución a la mejora de los sistemas de información y el desarrollo de las políticas públicas.* San salvador.

Asociación de jovenes empresarios. (5 de Febrero de 2016). *http://www.ajeimpulsa.es/documentos/banco_recursos/recurso_13.pdf*. Obtenido de Analisis de los factores que contribuyen al éxito de proyectos empresariales: http://www.ajeimpulsa.es/documentos/banco_recursos/recurso_13.pdf

Ayala Gonzalez, G., & Gómez Izasa, J. A. (2011). *Guía de buenas practicas de seguridad de la información en contextos de micro, pequeñas y medianas empresas de la región.* Pereira: Universidad Tecnologica de Pereira.

Barnes, H. E. (2000). *Historia de la econimia del mundo occidental.* Mexico.

Barrera, M. (2001). *Mecanismos de promoción de exportaciones para las pequeñas y medianas empresas en los países de la ALADI.* Montevideo.

Berciano, J. (2018). *La importancia y la necesidad de proteger la información sensible.*

Bernal, J. (21 de Octubre de 2014). *http://www.pdcahome.com/5202/ciclo-pdca/*. Obtenido de Metodologia.

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.

Casadiego Santana, A. L., Quintero Jimenez, m., & Toro Ruedas, M. (2014). *Sistema de seguridad de la información para el áre de contabilidad de la ESE Hospital de Rio de Oro Cesar.* Rio de Oro: Universidad Francisco de Paula Santander Ocaña.

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

Chacartegui. (4 de Octubre de 2010). *http://comunicandova.com/que-es-la-diferenciacion-y-por-que-la-necesitas/*. Obtenido de Estrategias de posicionamiento: http://marketingyconsumo.com/estrategias-de-posicionamiento.html

Chacon Hurtado, A. F. (26 de Marzo de 2016). *http://www.estadistica.mat.uson.mx/Material/queesunaencuesta.pdf*. Obtenido de Información para computación en nubes privadas y comunitarias.

Colombia, R. (2016). *Decreto 410 de 1971.* Bogotá: Littio.

Colombia, R. d. (2012). *Constitución Politica de Colombia.* Bogotá: Editorial Cupido.

Congreso de Colombia. (2010). *Ley 590 de 2000.* Bogotá: Littio.

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.

Dávila, A. F. (2005). *La micro y pequeña empresa mexicana, Observatorio de la Economía Latinoamericana.* Mexico.

Díaz, C. (2003). *La Creación de Empresas en Extremadura. Un Análisis Institucional.*

Dubois, A. (2002). *Un concepto de desarrollo para el siglo XXI.* España: Editorial Vasco.

Duran, O. M. (2010). *Una mirada al sector tercierio como dinamizador del desarrollo regional.* Ocaña: Ingenio.

Espinosa. (2011). *Teoría de la oferta.* Editorial Mac Graw Hill.

Espinoza Aguinaga, H. R. (2013). *Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo* . Lima: Pontificia Universidad Catolica de Perú.

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

Garay, L. J. (2016). *Colombia: estructura industrial e internacionalización 1967-1996.* Bogotá.

Gerencie.com. (4 de 10 de 2012). *http://www.gerencie.com/estrategias-para-no-pasar-el-regimen-comun.html*. Obtenido de Estrategias para no pasar el régimen común: http://www.gerencie.com/estrategias-para-no-pasar-el-regimen-comun.html

Grupo control seguridad. (2016). *https://www.grupocontrol.com/evolucion-de-la-seguridad-informatica*. Obtenido de Evolución de la seguridad informática.

Hurtado. (2011). *PYMES y corporaciones en contextos de globalización.* Palmira: UNAD.

Ibáñez, J. (2017). *La guerra incruenta entre cuantitativistas y cualitativistas».* Revista de Investigación científica. ISSN: 2017-5057.

Jürgen. (2007). *Innovacion en los negocios.* Auflage. Vahlen, München.

Lagos, Galeas, Barrios, & Ruiz. (2014). *Asociatividad de las MIPYMES en Honduras.* Honduras.

Marquina, S. M. (2013). *Gobernanza Global del Comercio en Internet.* Mexico: Ed INAP, 1.ª Edición.

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.

Ministerio de transporte. (2005). *Caracterización del Transporte en Colombia Diagnostico y Proyectos de Transporte e Infraestructura* . Bogotá.

MINTIC. (12 de Julio de 2012). *http://www.mintic.gov.co/portal/604/articles-5259_doc_pdf.pdf*. Obtenido de Infrome de gestion.

Mora. (2006). *Las Teorías del Desarrollo economicos, algunos postulados de enseñanza.*

Mosquera, Perez, Sanchez, & Ibañez. (2 de Junio de 2016). *https://pymesycorporaciones2013.wordpress.com/2013/02/01/caracterizacion-empresarial-de-las-pequenas-y-medianas-empresas-dedicadas-a-la-comercializacion-de-articulos-para-la-canasta-familiar-en-la-ciudadela-norte-de-la-ciudad-de-ocana-norte-de-santander-2*. Obtenido de Caracterización empresarial de las pequeñas y medianas empresas dedicadas a la comercialización de artículos para la canasta familiar en la ciudadela norte de la ciudad de Ocaña, Norte de Santander, 2012.: https://pymesycorporaciones2013.wordpress.com/2013/02/01/caracterizacion-empresarial-de-las-pequenas-y-medianas-empresas-dedicadas-a-la-comercializacion-de-articulos-para-la-canasta-familiar-en-la-ciudadela-norte-de-la-ciudad-de-ocana-norte-de-santander-2

Navarro Dino, P. (2015). *http://www.gestiopolis.com/.* Obtenido de Teoria de la factibilidad: http://www.gestiopolis.com/.

Odonell, K. Y. (2002). *Administración.* Mexico: Trillas.

Páez García, L. E. (2009). *Historia de la region de Ocaña.* Bogotá: Jaguar Group Producciones.

Perafán Ruiz, J. J. (2014). *Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca.* Popayán: Universidad Nacional Abierta y a Distancia.

Plana, C., & Cerpa, N. (2006). *Bases para la creación de una metodologia de adopción de comercio electronico para las mypimes chilenas.* Talca: P Rev. Fac. Ing. - Univ. Tarapacá, vol. 14 Nº 1.

Porter, M. (2007). *Estrategias competitivas.* Copyright Online Executive Education. .

Revista Dinero. (14 de Abril de 2016). *http://www.dinero.com/edicion-impresa/pymes/articulo/evolucion-y-situacion-actual-de-las-mipymes-en-colombia/222395*. Obtenido de Mipymes generan alrededor del 67% del empleo en Colombia: http://www.dinero.com/edicion-impresa/pymes/articulo/evolucion-y-situacion-actual-de-las-mipymes-en-colombia/222395

Rovira, S. (2016). *Innovación y desarrollo en America Latina.* Mexico.

Samuelson, P. A., & Nordhaus, W. D. (2004). *Factores de producción.* Bogotá.

Sanjuán Muñoz, W. (2017). *Evaluación de la seguridad en la información para la Terminal de Transporte de la ciudad de Ocaña.* Ocaña: Universidad Francsico de Paula Santander Ocaña.

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

Seguridad en la información Colombia. (17 de Junio de 2015). *http://seguridadinformacioncolombia.blogspot.com.co*. Obtenido de ¿Qué tan preparado está el Gobierno Colombiano contra ataques cibernéticos?

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/.

Sierra Jaramillo, O. A. (2011). *Estudio de los procesos de la seguridad en la información.* Pereira: Universidad Tecnologica de Pereira.

Smith. (1994). *Investigación sobre la naturaleza y causa de la riqueza de las naciones;.* Mexico: versión en español del Fondo de Cultura Económica.

Spiegel. (1987). *El desarrollo del pensamiento económico.* Barcelona: Ediciones Omega, S.A.

Tola Franco, D. E. (2015). *Implementacion de un sistema de gestión de seguridad de la información para una empresa de consultoria y auditoria.* Guayaquil: Escuela superior politecnica del litoral.

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.

Velez. (24 de Octubre de 2015). *http://www.camaramedellin.com.co/site/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=64&PortalId=0&TabId=515*. Obtenido de Tecnologia e innivación, impacto en la competitividad:

http://www.camaramedellin.com.co/site/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=64&PortalId=0&TabId=515

Vera Velez, L. (2017). *http://www.ponce.inter.edu/cai/Comite-investigacion/investigacion-cualitativa.html*. Obtenido de La investigación cualitativa.

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

Apéndices

Apéndice 1. Certificado de Cámara de Comercio

Cámara de Comercio de Ocaña

CAMARA DE COMERCIO DE OCANA

CERTIFICADO EXPEDIDO A TRAVES DEL PORTAL DE SERVICIOS VIRTUALES (SII)

CERTIFICADO DE EXISTENCIA Y REPRESENTACION LEGAL

TRANSPORTADORES DE NORTE DE SANTANDER SAS

Fecha expedición: 2015/08/03 - 14:10:07, Recibo No. R000275007, Operación No. 01E010803039

CODIGO DE VERIFICACIÓN: d0kReEC6qE

CERTIFICADO DE EXISTENCIA Y REPRESENTACION LEGAL O INSCRIPCION DE DOCUMENTOS.
LA CAMARA DE COMERCIO DE OCAÑA , CON FUNDAMENTO EN LAS MATRICULAS E INSCRIPCIONES DEL REGISTRO MERCANTIL,

CERTIFICA:

NOMBRE : TRANSPORTADORES DE NORTE DE SANTANDER SAS
N.I.T.:900719398-8
DIRECCION COMERCIAL:CALLE 7A 35-40 APTO 201
BARRIO COMERCIAL: LA PRIMAVERA
DOMICILIO : OCAÑA
TELEFONO COMERCIAL 1: 5612854
TELEFONO COMERCIAL 2: 3164480497
DIRECCION DE NOTIFICACION JUDICIAL :CALLE 7A 35-40 APTO 201
BARRIO NOTIFICACION: LA PRIMAVERA
MUNICIPIO JUDICIAL: OCAÑA
E-MAIL COMERCIAL:transportesdelnorte1@gmail.com

E-MAIL NOT. JUDICIAL:transportesdelnorte1@gmail.com

TELEFONO NOTIFICACION JUDICIAL 1: 5612854
TELEFONO NOTIFICACION JUDICIAL 2: 3164480497
FAX NOTIFICACION JUDICIAL:

CERTIFICA:

QUE EL MATRICULADO TIENE LA CONDICION DE PEQUEÑA EMPRESA DE ACUERDO CON LO ESTABLECIDO EN EL NUMERAL 1 DEL ARTÍCULO 2 DE LA LEY 1429 DE 2010.

CERTIFICA:

ACTIVIDAD PRINCIPAL:
4923 TRANSPORTE DE CARGA POR CARRETERA

CERTIFICA:

MATRICULA NO. 00026827

********** CONTINUA **********

Fecha de Certificación: Mon Aug 03 14:10:09 COT 2015

CODIGO DE VERIFICACIÓN: d0kReEC6qE

FECHA DE MATRICULA EN ESTA CAMARA: 28 DE OCTUBRE DE 2014
RENOVO EL AÑO 2015 , EL 6 DE MARZO DE 2015

CERTIFICA:

CONSTITUCION : QUE POR DOCUMENTO PRIVADO DE ASAMBLEA CONSTITUTIVA DE OCAÑA DEL 14 DE MARZO DE 2014 , INSCRITA EL 28 DE OCTUBRE DE 2014 BAJO EL NUMERO 00003229 DEL LIBRO IX,
SE CONSTITUYO LA PERSONA JURIDICA: TRANSPORTADORES DE NORTE DE SANTANDER SAS

CERTIFICA:

QUE POR ACTA NO. 0000004 DE ASAMBLEA EXTRAORDINARIA DE OCAÑA DEL 10 DE SEPTIEMBRE DE 2014 , INSCRITA EL 28 DE OCTUBRE DE 2014 BAJO EL NUMERO 00003228 DEL LIBRO IX,
CAMBIO SU DOMICILIO DE CONSTITUCION POR CAMBIO DOMICILIO DE LA CIUDAD DE BOGOTA, D.C. A LA CIUDAD DE OCAÑA, NORTE DE SANTANDER.
LA PERSONA JURIDICA:
TRANSPORTADORES DE NORTE DE SANTANDER SAS

CERTIFICA:

REFORMAS:

DOCUMENTO	FECHA	ORIGEN	CIUDAD	INSCRIPCION	FECHA
0000008	2015/05/10	ASAMBLEA EXTRAORDINA	OCA	00003356	2015/05/20

CERTIFICA:

VIGENCIA: QUE EL TERMINO DE DURACION DE LA PERSONA JURIDICA ES INDEFINIDO

CERTIFICA:

OBJETO SOCIAL: LA SOCIEDAD TENDRÁ COMO OBJETO PRINCIPAL EL DESARROLLO DE LA INDUSTRIA DEL TRANSPORTE TERRESTRE AUTOMOTOR PÚBLICO EN LA MODALIDAD DE CARGA, EN EL ÁMBITO NACIONAL E INTERNACIONAL A TRAVÉS DEL EMPLEO DE TODOS LOS MEDIOS Y EN SUS VARIADAS MODALIDADES. ADEMÁS PODRÁ REALIZAR LAS SIGUIENTES

********** CONTINUA **********

CODIGO DE VERIFICACIÓN: d0kReEC6qE

ACTIVIDADES: - EL TRANSPORTE EN GENERAL, ESPECIALMENTE EN ESTAS ÁREAS; TRANSPORTE DE CRUDO Y TODOS SUS DERIVADOS, TRANSPORTE DE COMBUSTIBLES, TRANSPORTE DE CARGA MASIVA, TRANSPORTE DE GANADO, SERVICIOS DE ENCOMIENDAS NACIONAL, SERVICIOS DE GIROS NACIONALES E INTERNACIONALES, PRESTACIÓN DE SERVICIOS MECÁNICOS Y DE REPARACIÓN AUTOMOTRIZ PARA LOS VEHÍCULOS AFILIADOS A LA EMPRESA, COMPRA Y VENTA DE PRODUCTOS, REPUESTOS, COMBUSTIBLES, LUBRICANTES, LLANTAS, PRESTACIÓN DE SERVICIO DE LAVADO Y ENGRASE PARA TODO TIPO DE VEHÍCULOS, COMPRA Y VENTA DE VEHÍCULOS; - ADEMÁS DE LO ANTERIORMENTE MENCIONADO PODRÁ LA SOCIEDAD EJECUTAR ACTIVIDADES COMO: CONTRATAR MEDIOS DE TRANSPORTE ESPECIALIZADOS EN TODAS SUS MODALIDADES, COMBINADO Y MULTIMODAL, INCLUYENDO LA CONSIGNACIÓN DE MERCANCÍA U OTROS EFECTOS POR CUENTA PROPIA O DE TERCEROS, DIRECTAMENTE O POR MEDIO DE INTERMEDIARIOS; - REPRESENTAR FIRMAS NACIONALES O EXTRANJERAS QUE SE OCUPEN DE LOS MISMOS NEGOCIOS O ACTIVIDADES; - ALMACENAR, DISTRIBUIR, EMPACAR, RE EMPACAR Y MANIPULAR TODO TIPO DE BIENES; - EMITIR, RECIBIR, DISTRIBUIR, REGISTRAR LOS DOCUMENTOS PROPIOS DE LA ACTIVIDAD; - COORDINAR Y ORGANIZAR EMBARQUES, CONSOLIDAR Y DESCONSOLIDAR LA CARGA; - PRESTAR LOS SERVICIOS DE ASESORÍA, CONSULTORÍA, DESARROLLO Y GESTIÓN EN TODOS LOS CAMPOS QUE ESTÉN RELACIONADOS CON EL OBJETO SOCIAL DE LA SOCIEDAD A LAS ENTIDADES DE DERECHO PÚBLICO Y PRIVADO, NACIONALES Y EXTRANJERAS; - ADQUIRIR BIENES DE CUALQUIER NATURALEZA, MUEBLES O INMUEBLES CORPORALES O INCORPORALES, ASÍ COMO HACER CONSTRUCCIONES SOBRE SUS BIENES INMUEBLES Y ENAJENAR Y GRAVAR A CUALQUIER TÍTULO LOS BIENES DE QUE SEA TITULAR DEL DERECHO DE DOMINIO O CUALQUIER OTRO DERECHO REAL; - INTERVENIR ANTE TERCEROS Y ANTE LOS MISMOS SOCIOS, COMO ACREEDORA O COMO DEUDORA EN TODA CLASE DE OPERACIONES DE CRÉDITO, DANDO O RECIBIENDO LAS GARANTÍAS DEL CASO, CUANDO HAYA LUGAR A ESTAS; - DAR Y RECIBIR EN GARANTÍA DE OBLIGACIONES BIENES MUEBLES E INMUEBLES Y TOMARLOS EN ARRENDAMIENTO U OPCIÓN DE CUALQUIER NATURALEZA; - SUSCRIBIR ACCIONES O DERECHOS EN EMPRESAS QUE FACILITEN O CONTRIBUYAN AL DESARROLLO DE SUS OPERACIONES; - CELEBRAR EL CONTRATO COMERCIAL DE CAMBIO EN TODAS SUS MANIFESTACIONES COMO GIRAR, ENDOSAR, PROTESTAR, CANCELAR, AVALAR, DAR Y RECIBIR LETRAS DE CAMBIO, PAGARÉS O CUALQUIER OTROS EFECTOS DE COMERCIO O TÍTULOS VALORES EN GENERAL Y CELEBRAR TODA CLASE DE OPERACIONES CON ENTIDADES BANCARIAS Y EN

********** CONTINUA **********

CODIGO DE VERIFICACIÓN: d0kReEC6qE

GENERAL DE CARÁCTER CREDITICIA; - COMPRAR O CONSTRUIR SOCIEDADES DE CUALQUIER GÉNERO, INCORPORARSE EN COMPAÑÍAS O FUSIONARSE CON ELLAS; - PARTICIPAR EN LICITACIONES PÚBLICAS O PRIVADAS DE ACUERDO CON LAS ACTIVIDADES A DESARROLLAR POR LA SOCIEDAD Y SER MIEMBRO DE UN CONSORCIO, UNIÓN TEMPORAL O SOCIEDAD CON OBJETO ÚNICO PARA CELEBRAR UN CONTRATO CON DETERMINADA ENTIDAD ESTATAL O SUSCRIBIR UNA PROMESA DE CONSTITUCIÓN DE SOCIEDAD UNA VEZ SE HAYA ADJUDICADO EL CONTRATO CON LA FINALIDAD DE PODER PARTICIPAR EN PROCESOS DE CONTRATACIÓN CON EL ESTADO COLOMBIANO, O PERSONA JURÍDICA PRIVADA; - HACER EN SU PROPIO NOMBRE, POR CUENTA DE TERCEROS O EN PARTICIPACIÓN CON ELLOS TODA CLASE DE OPERACIONES QUE SEAN NECESARIAS O CONVENIENTES PARA EL DESARROLLO DEL OBJETO SOCIAL, O QUE PUEDAN DESARROLLAR O FAVORECER SUS ACTIVIDADES O EN LAS EMPRESAS EN QUE TENGAN INTERESES Y SE RELACIONEN CON EL OBJETO SOCIAL; - LA SOCIEDAD PODRÁ LLEVAR A CABO, EN GENERAL, TODAS LAS OPERACIONES, DE CUALQUIER NATURALEZA QUE ELLAS FUEREN, RELACIONADAS CON EL OBJETO MENCIONADO, ASÍ COMO CUALESQUIERA ACTIVIDADES SIMILARES, CONEXAS O COMPLEMENTARIAS O QUE PERMITAN FACILITAR O DESARROLLAR EL COMERCIO O LA INDUSTRIA DE LA SOCIEDAD.

CERTIFICA:

CAPITAL:

** CAPITAL AUTORIZADO **
VALOR :$640,000,000.00
NO. DE ACCIONES:640.00
VALOR NOMINAL :$1,000,000.00

** CAPITAL SUSCRITO **
VALOR :$640,000,000.00
NO. DE ACCIONES:640.00
VALOR NOMINAL :$1,000,000.00

** CAPITAL PAGADO **
VALOR :$640,000,000.00
NO. DE ACCIONES:640.00
VALOR NOMINAL :$1,000,000.00

CERTIFICA:

********** CONTINUA **********

CODIGO DE VERIFICACIÓN: d0kReEC6qE

MEDIANTE INSCRIPCION NRO. 00003230 DEL 28 DE OCTUBRE DE 2014 , SE REGISTRO EL ACTO ADMINISTRATIVO NUMERO 0000264 DE FECHA 27 DE AGOSTO DE 2014 EXPEDIDO POR MINISTERIO DE TRANSPORTE :
QUE LO HABILITA PARA PRESTAR EL SERVICIO PUBLICO DE TRANSPORTE AUTOMOTOR EN LA MODALIDAD DE CARGA.

CERTIFICA:

** JUNTA DIRECTIVA: PRINCIPAL(ES) **

QUE POR ACTA NO. 0000007 DE ASAMBLEA GENERAL DEL 29 DE MARZO DE 2015 , INSCRITA EL 17 DE ABRIL DE 2015 BAJO EL NUMERO 00003337 DEL LIBRO IX , FUE(RON) NOMBRADO(S):

NOMBRE	IDENTIFICACION
MIEMBRO PRINCIPAL JUNTA DIRECTIVA	
TRILLOS VERJEL LUIS FELIPE	C.C.00013361138
MIEMBRO PRINCIPAL JUNTA DIRECTIVA	
ACOSTA LOPEZ EDDIE JESUS	C.C.00013364288
MIEMBRO PRINCIPAL JUNTA DIRECTIVA	
QUINTANA ORTEGA JENNY	C.C.00060444359
MIEMBRO PRINCIPAL JUNTA DIRECTIVA	
PACHECO PEÑARANDA HENRY ALONSO	C.C.00013507600
MIEMBRO PRINCIPAL JUNTA DIRECTIVA	
FUENTES MARTINEZ GUSTAVO	C.C.00088140415
MIEMBRO PRINCIPAL JUNTA DIRECTIVA	
CHINCHILLA RANGEL CARLOS ALONSO	C.C.00013196092

** JUNTA DIRECTIVA: SUPLENTE(S) **

QUE POR ACTA NO. 0000007 DE ASAMBLEA GENERAL DEL 29 DE MARZO DE 2015 , INSCRITA EL 17 DE ABRIL DE 2015 BAJO EL NUMERO 00003337 DEL LIBRO IX , FUE(RON) NOMBRADO(S):

NOMBRE	IDENTIFICACION
MIEMBRO SUPLENTE JUNTA DIRECTIVA	
QUINTANA QUINTANA ASTOLFO	C.C.00019129224

********** CONTINUA **********

CODIGO DE VERIFICACIÓN: d0kReEC6qE

MIEMBRO SUPLENTE JUNTA DIRECTIVA
BLANCO AREVALO ALFONSO C.C.00013460104
MIEMBRO SUPLENTE JUNTA DIRECTIVA
TRILLOS GOMEZ MELITSA MARIA C.C.01091658630
MIEMBRO SUPLENTE JUNTA DIRECTIVA
ROJAS OJEDA KEVIN ALEXANDER C.C.01098658248

CERTIFICA:

** NOMBRAMIENTOS : **

QUE POR ACTA NO. 0000009 DE JUNTA DIRECTIVA DEL 13 DE MAYO DE 2015 , INSCRITA EL 21 DE MAYO DE 2015 BAJO EL NUMERO 00003357 DEL LIBRO IX , FUE(RON) NOMBRADO(S):

NOMBRE IDENTIFICACION

REPRESENTANTE LEGAL
ACOSTA LOPEZ EDDIE JESUS C.C.00013364288

CERTIFICA:

REPRESENTACIÓN LEGAL: LA REPRESENTACIÓN LEGAL DE LA SOCIEDAD POR ACCIONES SIMPLIFICADA ESTARÁ A CARGO DE UNA PERSONA NATURAL O JURÍDICA, ACCIONISTA O NO, MIEMBRO DE LA JUNTA DIRECTIVA O NO, QUIEN TENDRÁ SUPLENTE; EN AQUELLOS CASOS EN QUE EL REPRESENTANTE LEGAL SEA UNA PERSONA JURÍDICA, LAS FUNCIONES QUEDARÁN A CARGO DEL REPRESENTANTE LEGAL DE ÉSTA; FACULTADES DEL REPRESENTANTE LEGAL: LA SOCIEDAD SERÁ GERENCIADA, ADMINISTRADA Y REPRESENTADA LEGALMENTE ANTE TERCEROS POR EL REPRESENTANTE LEGAL O SU SUPLENTE, QUIEN NO TENDRÁ RESTRICCIONES DE CONTRATACIÓN POR RAZÓN DE LA NATURALEZA NI DE LA CUANTÍA DE LOS ACTOS QUE CELEBREN. POR LO TANTO, SE ENTENDERÁ QUE EL REPRESENTANTE LEGAL O EL SUPLENTE PODRÁN CELEBRAR O EJECUTAR TODOS LOS ACTOS Y CONTRATOS COMPRENDIDOS EN EL OBJETO SOCIAL O QUE SE RELACIONEN DIRECTAMENTE CON LA EXISTENCIA Y EL FUNCIONAMIENTO DE LA SOCIEDAD SIEMPRE Y CUANDO LA ASAMBLEA GENERAL O LA JUNTA DIRECTIVA LO AUTORICEN; EL REPRESENTANTE LEGAL O EL SUPLENTE DE ESTE SE ENTENDERÁ ENVESTIDO DE LOS MÁS AMPLIOS PODERES PARA

********** CONTINUA **********

ACTUAR EN TODAS LAS CIRCUNSTANCIAS EN NOMBRE DE LA SOCIEDAD, CON EXCEPCIÓN DE AQUELLAS FACULTADES QUE, DE ACUERDO CON LOS ESTATUTOS, SE HUBIEREN RESERVADO LOS ACCIONISTAS. EN LAS RELACIONES FRENTE A TERCEROS, LA SOCIEDAD QUEDARÁ OBLIGADA POR LOS ACTOS Y CONTRATOS CELEBRADOS POR EL REPRESENTANTE LEGAL O SU SUPLENTE SIEMPRE Y CUANDO LA ASAMBLEA GENERAL O LA JUNTA LOS HAYA AUTORIZADO; LE ESTÁ PROHIBIDO AL REPRESENTANTE LEGAL O AL SUPLENTE Y A LOS DEMÁS ADMINISTRADORES DE LA SOCIEDAD, POR SÍ O POR INTERPUESTA PERSONA, OBTENER BAJO CUALQUIER FORMA O MODALIDAD JURÍDICA PRÉSTAMOS POR PARTE DE LA SOCIEDAD U OBTENER DE PARTE DE LA SOCIEDAD AVAL, FIANZA O CUALQUIER OTRO TIPO DE GARANTÍA DE SUS OBLIGACIONES PERSONALES. FUNCIONES DEL REPRESENTANTE LEGAL Y EL SUPLENTE: EL REPRESENTANTE LEGAL O SU SUPLENTE EJERCERÁ TODAS LAS FUNCIONES PROPIAS DE LA NATURALEZA DE SU CARGO, Y EN ESPECIAL, LAS SIGUIENTES: - REPRESENTA LA SOCIEDAD ANTE LOS ACCIONISTAS, ANTE TERCEROS Y ANTE TODA CLASE DE AUTORIDADES DE ORDEN ADMINISTRATIVO Y JURISDICCIONAL; - EJECUTAR TODOS LOS ACTOS U OPERACIONES CORRESPONDIENTES AL OBJETO SOCIAL, DE CONFORMIDAD CON LO PREVISTO EN LAS LEYES Y EN LOS ESTATUTOS; AUTORIZAR CON SU FIRMA TODOS LOS DOCUMENTOS PÚBLICOS O PRIVADOS QUE DEBAN OTORGARSE EN DESARROLLO DE LAS ACTIVIDADES SOCIALES O INTERÉS DE LA SOCIEDAD; - PRESENTAR A LA ASAMBLEA GENERAL EN SUS REUNIONES ORDINARIAS, UN INVENTARIO Y UN BALANCE DE FIN DE EJERCICIO, JUNTO CON UN INFORME ESCRITO SOBRE LA SITUACIÓN DE LA SOCIEDAD, UN DETALLE COMPLETO DE LA CUENTA DE PÉRDIDAS Y GANANCIAS, ASÍ COMO UN PROYECTO DE DISTRIBUCIÓN DE UTILIDADES OBTENIDAS; - NOMBRAR Y REMOVER LOS EMPLEADOS DE LA SOCIEDAD CUYO NOMBRAMIENTO Y REMOCIÓN LE DELEGUE LA JUNTA DIRECTIVA; - TOMAR TODAS LAS MEDIDAS QUE RECLAMEN LA CONSERVACIÓN DE LOS BIENES SOCIALES, VIGILAR LA ACTIVIDAD DE LOS EMPLEADOS DE LA ADMINISTRACIÓN DE LA SOCIEDAD E IMPARTIRLES LAS ÓRDENES E INSTRUCCIONES QUE EXIJAN LA BUENA MARCHA DE LA COMPAÑÍA; - CONVOCAR A LA ASAMBLEA A REUNIONES ORDINARIAS U EXTRAORDINARIAS CUANDO LO CREA CONVENIENTE O NECESARIO Y HACER LAS CONVOCATORIAS DEL CASO CUANDO LO ORDENEN LOS ESTATUTOS, LA JUNTA DIRECTIVA O EL REVISOR FISCAL DE LA SOCIEDAD; - CONVOCAR LA JUNTA DIRECTIVA CUANDO LO CONSIDERE CONVENIENTE O NECESARIO Y MANTENERLA INFORMADA DEL CURSO DE LOS NEGOCIOS DE LA SOCIEDAD; - CUMPLIR LAS ÓRDENES E INSTRUCCIONES QUE LE IMPARTAN LA ASAMBLEA

********** CONTINUA **********

CODIGO DE VERIFICACIÓN: d0kReEC6qE

GENERAL Y LA JUNTA DIRECTIVA Y EN PARTICULAR SOLICITAR AUTORIZACIONES PARA LOS NEGOCIOS QUE DEBEN APROBAR PREVIAMENTE LA ASAMBLEA O JUNTA DIRECTIVA; - CUMPLIR Y HACER CUMPLIR TODOS LOS REQUISITOS O EXIGENCIAS LEGALES QUE SE RELACIONEN CON EL FUNCIONAMIENTO Y ACTIVIDADES DE LA SOCIEDAD.

CERTIFICA:

QUE LOS DOCUMENTOS CON OCASIÓN DEL CAMBIO DE DOMICILIO FUERON PREVIAMENTE INSCRITOS Y REVISADOS JURIDICAMENTE EN LA CAMARA DE COMERCIO DE BOGOTA.

CERTIFICA:

QUE NO FIGURAN INSCRIPCIONES ANTERIORES A LA FECHA DEL PRESENTE CERTIFICADO, QUE MODIFIQUEN TOTAL O PARCIALMENTE SU CONTENIDO.

DE CONFORMIDAD CON LO ESTABLECIDO EN EL CODIGO DE PROCEDIMIENTO ADMINISTRATIVO Y DE LO CONTENCIOSO Y DE LA LEY 962 DE 2005, LOS ACTOS ADMINISTRATIVOS DE REGISTRO AQUI CERTIFICADOS QUEDAN EN FIRME DIEZ (10) DIAS HABILES DESPUES DE LA FECHA DE INSCRIPCION, SIEMPRE QUE NO SEAN OBJETO DE RECURSOS.

VALOR DEL CERTIFICADO: $4,500

IMPORTANTE: La firma digital del secretario de la CAMARA DE COMERCIO DE OCANA contenida en este certificado electrónico se encuentra emitida por una entidad de certificación abierta autorizada y vigilada por la Superintendencia de Industria y Comercio, de conformidad con las exigencias establecidas en la Ley 527 de 1999 para validez jurídica y probatoria de los documentos electrónicos.

La firma digital no es una firma digitalizada o escaneada, por lo tanto, la firma digital que acompaña este documento la podrá verificar a través de su aplicativo visor de documentos pdf.

No obstante, si usted va a imprimir este certificado, lo puede hacer desde su computador, con la certeza de que el mismo fue expedido a través del canal virtual de la cámara de comercio y que la persona o entidad a la que usted le va a entregar el certificado impreso, puede verificar por una sola vez el contenido del mismo, ingresando al enlace http://sii.confecamaras.org/cv.php seleccionando allí la cámara de comercio e indicando el código de verificación d0kReEC6qE.

Al realizar la verificación podrá visualizar (y descargar) una imagen exacta del certificado que fue entregado al usuario en el momento que se realizó la transacción.

La firma mecánica que se muestra a continuación es la representación gráfica de la firma del secretario jurídico (o que haga sus veces) de la cámara de comercio quien avala este certificado. La firma mecánica no reemplaza la firma digital en los documentos electrónicos.

********** CONTINUA **********

CAMARA DE COMERCIO DE OCANA

CERTIFICADO EXPEDIDO A TRAVES DEL PORTAL DE SERVICIOS VIRTUALES (SII)

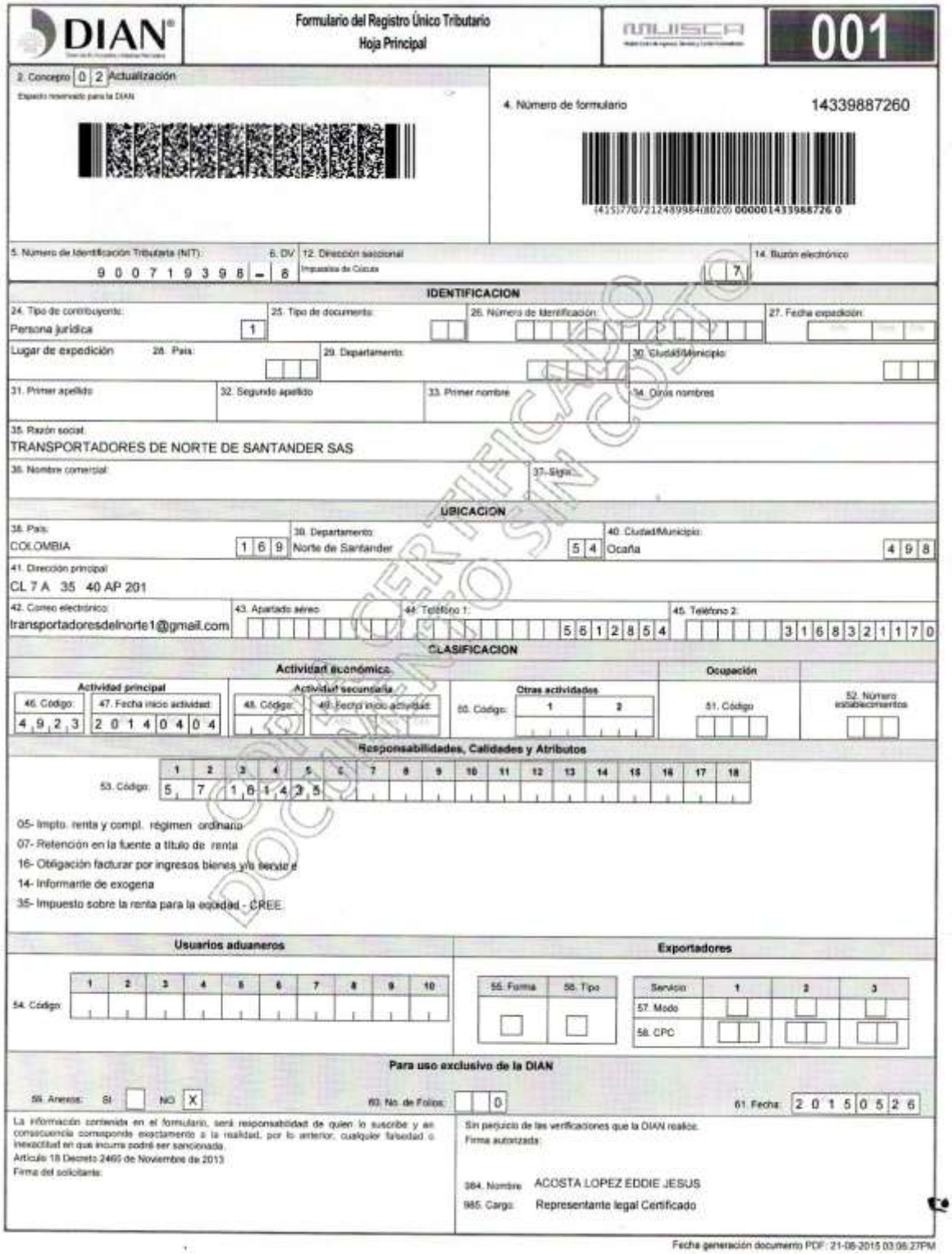
CERTIFICADO DE EXISTENCIA Y REPRESENTACION LEGAL

TRANSPORTADORES DE NORTE DE SANTANDER SAS

Fecha expedición: 2015/08/03 - 14:10:07, Recibo No. R000275007, Operación No. 01E010803039

CODIGO DE VERIFICACIÓN: d0kReEC6qE

Apéndice 2. Registro Único Tributario



DIAN

Formulario del Registro Único Tributario
Hoja Principal

MUISCA

001

2. Concepto: 0 2 Actualización

Espacio reservado para la DIAN

4. Número de formulario: 14339887260

(415)7707212489984(8020) 000001433988726 0

5. Número de Identificación Tributaria (NT): 9 0 0 7 1 9 3 9 8 - 8

6. DV

12. Dirección seccional: Impuestos de Cúcuta

13. 7

14. Buzón electrónico

IDENTIFICACION

24. Tipo de contribuyente: Persona jurídica 1

25. Tipo de documento:

26. Número de identificación:

27. Fecha expedición:

Lugar de expedición

28. País:

29. Departamento:

30. Ciudad/Municipio:

31. Primer apellido:

32. Segundo apellido:

33. Primer nombre:

34. Otros nombres:

35. Razón social: TRANSPORTADORES DE NORTE DE SANTANDER SAS

36. Nombre comercial:

37. Sigla:

UBICACION

38. País: COLOMBIA 1 6 9

39. Departamento: Norte de Santander 5 4

40. Ciudad/Municipio: Ocaña 4 9 8

41. Dirección principal: CL 7 A 35 40 AP 201

42. Correo electrónico: transportadoresdelnorte1@gmail.com

43. Apartado aéreo:

44. Teléfono 1: 5 6 1 2 8 5 4

45. Teléfono 2: 3 1 6 8 3 2 1 1 7 0

CLASIFICACION

Actividad económica

Actividad principal		Actividad secundaria		Otras actividades			Ocupación	
46. Código:	47. Fecha inicio actividad:	48. Código:	49. Fecha inicio actividad:	50. Código:	1	2	51. Código	52. Número establecimientos
4 9 2 3	2 0 1 4 0 4 0 4							

Responsabilidades, Calidades y Atributos

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
53. Código:	5	7	1	6	1	4	3	5										

05- Impto. renta y compl. régimen ordinario
07- Retención en la fuente a título de renta
16- Obligación facturar por ingresos bienes y/o servicios
14- Informante de exogena
35- Impuesto sobre la renta para la equidad - CREE

Usuarios aduaneros

	1	2	3	4	5	6	7	8	9	10
54. Código:										

Exportadores

55. Forma	56. Tipo

Servicio	1	2	3
57. Modo			
58. CPC			

Para uso exclusivo de la DIAN

59. Anexos: SI [ ] NO [X]

60. No. de Folios: 0

61. Fecha: 2 0 1 5 0 5 2 6

La información contenida en el formulario, será responsabilidad de quien lo suscribe y en consecuencia corresponde exactamente a la realidad, por lo anterior, cualquier falsedad o inexactitud en que incurra podrá ser sancionada.
Artículo 18 Decreto 2460 de Noviembre de 2013
Firma del solicitante:

Sin perjuicio de las verificaciones que la DIAN realice.
Firma autorizada:

984. Nombre: ACOSTA LOPEZ EDDIE JESUS
985. Cargo: Representante legal Certificado

Fecha generación documento PDF: 21-05-2015 03:06:27PM

Apéndice 3. Entrevista aplicada a los empleados de la empresa Transportadores de Norte de Santander SAS.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS

Objetivo. Evaluar la seguridad en la información para la empresa Transportadores de Norte de Santander SAS, basados en la norma ISO 27001:2013.

1. ¿El computador asignado para el desarrollo de sus funciones recibe mantenimiento periódicamente?_____
_____
_____

2. ¿Existe un Sistema de Gestión de Seguridad Informática en la Empresa?_____
_____
_____

3. ¿La compañía capacita al personal en temas de seguridad informática?_____
_____
_____

4. ¿Existe alguna política para el cambio regular de las contraseñas?_____
_____
_____

5. ¿Antes y después de la contratación del personal se hace entrega de un manual de funciones y responsabilidades de seguridad de la información?_____
_____
_____

6. ¿Cuándo ocurre un evento relacionado con seguridad de la información sabe a quién reportarlo?_____
_____
_____

7. ¿Realiza copias de los datos?_____
_____
_____

8. ¿Considera necesario que la compañía invierta en la implementación de un Sistema de Gestión de Seguridad de la Información?_____

_____
_____

9. ¿Posee antivirus el computador asignado?_____
_____
_____

10. ¿La compañía posee software legal en su totalidad?_____
_____
_____

11. ¿Existen zonas restringidas de acceso de personal?_____
_____
_____

12. ¿Se realiza mantenimiento preventivo y correctivo a la UPS?_____
_____
_____

13. ¿Existen sistemas de seguridad que impidan el acceso a lugares restringidos?_____
_____
_____

14. ¿Se cuenta con sistemas de alarma como detectores de humo, humedad?_____
_____
_____

15. ¿Existe vigilancia en la entrada del edificio?_____
_____
_____

16. ¿Los sitios donde están los equipos de cómputo cuenta con aire acondicionado?_____
_____
_____

17. ¿Se encuentra asegurados mediante pólizas los equipos de cómputo?_____
_____
_____

18. ¿Existe algún control para navegar en internet?_____
_____
_____

19. ¿Existe control sobre el uso del correo electrónico?_____
_____
_____

Apéndice 4. Lista de verificación.

NOMBRE DEL AUDITOR A EVALUAR	
DEPARTAMENTO	

A continuación encontrará una serie de preguntas cuya respuesta se debe señalar con una (X):

PREGUNTAS	**SI**	**NO**
1. ¿A sufrido accidentalmente pérdida de información en su puesto trabajo		
2. En caso de pérdida de información ¿Ha logrado recuperar total ó parcialmente la información?		
3. ¿Alguna persona ha divulgado información personal o privada?		
4. ¿Alguna vez ha insertado un Flash Memory en su puesto de trabajo?		
5. ¿Separa la información dependiendo de su importancia?		
6. ¿Existe un procedimiento o manual que ayude al manejo de información privada o restringida?		
7. ¿Alguna vez se le ha perdido algún dispositivo de almacenamiento, con información de la empresa?		
8. ¿Conoce usted el término de encriptación de archivos?		
9. ¿Se ha olvidado de cerrar su sesión?		

10. Cuando está ausente en su puesto de trabajo, ¿Su ordenador se queda prendido?		
11. ¿Ha instalado cualquier tipo de programa en su puesto de trabajo?		
12. ¿Ha intentado ingresar a documentos o archivos y se le ha denegado el acceso?		
13. ¿Ha grabado información en su puesto de trabajo desde algún dispositivo de almacenamiento?		
14. ¿Al terminar sus labores diarias apaga su computadora?		
15. En caso de ausencia en su puesto de trabajo y este prendido su computador ¿cierra usted su sesión?		
16. Cuando se instala un programa nuevo ¿Existe su debida capacitación?		
17. ¿Ha tenido alguna pantalla de advertencia en su monitor?		
18. ¿Ha comunicado al departamento de sistemas por algún mensaje de error de alguna aplicación?		
19. ¿Ha intentado ingresar a otras cuentas de usuario?		
20. Por cualquier motivo ¿Su puesto de trabajo ha sido reemplazado temporalmente por personal interno?		
21. ¿Ha recuperado algún archivo perdido?		
22. ¿Usted cree que la información dentro de la empresa está segura?		
23. ¿Comparten información con otros departamentos mediante carpetas compartidas?		

24. ¿Ha sufrido alguna pérdida de información?		
25. ¿Ha realizado alguna vez un cambio de clave en su computadora?		
26. ¿Graba la información que realiza cuando va a estar ausente?		
27. ¿Ha investigado información por medio de navegadores de búsqueda como Google en su puesto de trabajo?		
28. ¿Ha logrado alguna vez, por su cuenta, arreglar algún error en su computador?		
29. ¿Se ha denegado el acceso a datos o información de otro departamento?		
30. ¿Existe un área restringida en alguna carpeta de su computadora?		
31. ¿Realiza respaldos de su información diariamente en dispositivos de almacenamiento?		
32. ¿Se ha desconectado su computadora por apagones?		
33. ¿Ha llevado archivos digitales para terminar en su casa por falta de tiempo?		
34. ¿Tiene su ordenador información personal como fotos, videos, música, etc.?		
35. ¿El departamento de sistemas realiza el mantenimiento de su computador mensualmente?		
36. ¿Alguna vez le han cambiado su computadora por otra?		
37. ¿En los últimos 6 meses, le han cambiado su computadora?		
38. ¿Conoce usted el término de activos informáticos?		

39. ¿Separa por categorías los documentos públicos, privados, confidenciales, etc.?		
40. ¿Comparte su computador con otro compañero de trabajo?		
41. ¿Alguna vez se ha activado advertencias de antivirus?		
42. ¿Usted cree que la información que usted posee está segura?		
43. ¿Ha intentado arreglar su computadora por su propia cuenta?		
44. En su departamento ¿Tienen definido sus funciones y obligaciones?		
45. A parte de usted ¿Alguna otra persona conoce su contraseña de acceso a su computador?		
46. ¿Guarda información privada en distintas carpetas?		
47. Por cualquier motivo ¿Su puesto de trabajo ha sido reemplazado temporalmente por personal que no trabaja en la empresa?		
48. ¿Ha intentado ingresar a una página web y se ha bloqueado el acceso?		
49. ¿Ha tenido alguna capacitación para el mejor uso de las aplicaciones de su computadora, con el objetivo de mejorar su trabajo diario?		
50. ¿Ha llevado archivos o documentos informáticos fuera de la empresa en Flash Memory, CD, etc.?		
51. Su cuenta de usuario ¿Tiene la misma clave que la de su correo electrónico?		

52. Cuando sale un mensaje en su pantalla ¿Cierra el mensaje?		
53. ¿Ha rotado alguna vez una memoria flash para pasar información?		
54. ¿Se ha realizado algún cambio donde su computador le instalaron en otro departamento?		
55. ¿Ha observado archivos o información que no se relacionan con su departamento en su puesto de trabajo?		
56. ¿Tienen manuales todas las aplicaciones su computador?		
57. ¿Ha utilizado otra cuenta para ingresar a una sesión?		
58. ¿Su contraseña tiene como caracteres nombres de hijos, esposo, padres, mascotas, etc.?		
59. ¿Ha perdido información por apagones?		
60. ¿Se ha instalado alguna aplicación para el mejor manejo de la información?		
61. ¿Ha enviado archivos de la empresa desde su Hotmail o gmail?		
62. ¿Tiene acceso a internet en su puesto de trabajo?		
63. ¿Guarda su trabajo y cierra la aplicación cuando va a estar ausente?		
64. Sabe si su información, donde usted guarda ¿No es visible para otros usuarios?		