UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

"POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EMPRESAS DEL SECTOR DE LOGÍSTICA Y TRANSPORTE DE CARGA DEL MUNICIPIO DE ANTIGUO CUSCATLÁN BASADAS EN LA NORMA TÉCNICA SALVADOREÑA ISO/IEC 27001:2013"

Trabajo de Investigación Presentado por:

Canizalez Hernández, Néstor Bladimir

Estrada, Irvin Osmaro

Mateo Cruz, Luis Mauricio

Para optar al grado de:

LICENCIADO EN CONTADURÍA PÚBLICA

Noviembre, 2017

San Salvador, El Salvador, Centroamérica

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES UNIVERSITARIAS

Rector:	Máster Roger Armando Arias Alvarado
Secretario General:	Licenciado Cristóbal Hernán Ríos Benítez
Decano de la Facultad de Ciencias Económicas:	Licenciado Nixon Rogelio Hernández Vásquez
Secretaria de la Facultad de Ciencias Económicas:	Licenciada Vilma Marisol Mejía Trujillo
Directora de la Escuela de Contaduría Pública:	Licenciada María Margarita de Jesús Martínez de Hernández
Coordinador General de Seminario de Graduación:	Licenciado Mauricio Ernesto Magaña Menéndez
Coordinación de Seminario de Procesos de Graduación de la Escuela de Contaduría Pública:	Licenciado Daniel Nehemías Reyes López
Docente director:	Máster Mario Hernán Cornejo Pérez
Jurado Examinador:	Licenciado Jorge Luis Martínez Bonilla Licenciado Carlos Ernesto Ramírez Master Mario Hernán Cornejo Pérez

Noviembre 2017

San Salvador, El Salvador, Centroamérica

AGRADECIMIENTOS

Dedico este logro a Dios, por su infinito amor para mí, y a la persona que siempre estuvo a mi lado dándome ánimos, brindándome su amor incondicional a mi madre María Esperanza Cruz, por ser mi todo en esta vida, por ayudarme siempre a salir adelante a siempre enseñarme que: “detrás de las nubes grises el cielo sigue siendo azul”, y también agradezco a cada una de las personas que me dieron animo hasta lograr mis metas.

Luis Mauricio Mateo Cruz

A Dios gracias por la oportunidad de culminar uno de los propósitos en mi vida, a mis padres por enseñarme que todo esfuerzo tiene su recompensa en especial a mi madre por su entrega incondicional, a mi hermano por su apoyo valioso en este proceso, a mis jefes por darme la oportunidad de estudiar en horarios de trabajo, a mis amigos por su paciencia en no contar conmigo en ciertas etapas por los estudios y en general a todas las personas por sus muestras de cariño y orgullo al verme triunfar académicamente.

Néstor Bladimir Canizalez Hernández

A Dios por haberme acompañado a lo largo de toda mi carrera, por ser mi fortaleza en los momentos de debilidad, por haberme guiado y brindado la sabiduría necesaria para cumplir mis metas con éxito, al alma mater por la oportunidad de estudio, mi familia por darme su apoyo incondicional en todo momento, así como también agradezco a una persona muy importante en mi vida que siempre me apoyo durante toda mi carrera, y mis compañeros Nestor Canizalez y Luis Mateo por su paciencia y por su valioso aporte para culminar esta etapa de educación a nivel profesional, y a todas las personas que desinteresadamente contribuyeron a este logro.

Irvin Osmaro Estrada

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

ANEXO 3 Análisis e interpretación de los resultados

ANEXO 4 Contrato de trabajo con cláusula de confidencialidad

ANEXO 5 Comprobante de entrega de políticas de seguridad informática a empleados

ANEXO 6 Acuerdo de intercambio de información

ANEXO 7 Contrato de confidencialidad

ANEXO 8 Cláusula para contrato de confidencialidad con proveedor

ANEXO 9 Entrevista al Ing. Fernando Martínez Gerente General del grupo empresarial Comca Internacional

RESUMEN EJECUTIVO

El sector de logística y transporte de carga es el encargado de desarrollar un proceso amplio y sistemático, que permite al comercio internacional o comercio exterior globalizarse, permite que las exportaciones de cada país fluyan y se comercialicen a nivel mundial, para esto es necesario que una empresa fabrique productos y otra empresa (extranjera o en otro país) requiera de éstos como parte de un elemento de materia prima o articulo final terminado; el comercio internacional depende directamente de las necesidades entre un vendedor y un comprador, indiferentemente del país, región o continente en el que se encuentren. En el país el sector logístico y transporte de carga ha hecho posible la intermediación de clientes y proveedores, extranjeros y nacionales.

Los avances tecnológicos brindan a las empresas del sector mayores herramientas para el desarrollo de negocios algunos de estos son: un sistema de gestión de clientes (CRM) en el cual es más fácil el control y seguimiento de los mismos, sistemas ERP que integran diferentes módulos y los cuales interactúan entre sí como planillas, contabilidad, operaciones, inventarios, facturación, y es necesario recalcar que cada uno de ellos administra datos y genera información importante para la organización a tal grado que con esta información se pueden tomar decisiones para la mejora de las estrategias, indicadores que se utilizan para el monitoreo de los resultados.

Las empresas del sector de logística en su mayoría no cuentan con políticas documentadas que les ayuden a proteger la información y garantizar la seguridad informática, dentro de sus instalaciones y para el personal, no tienen un programa de capacitaciones para la concientización y socialización de sus políticas, y para ello necesitan desarrollar y poner en marcha una cultura organizacional de protección a los activos informáticos que poseen.

Por lo que la presente investigación contiene políticas específicas que ayudarán a disminuir los riesgos en los sistemas de información, las cuales cumplen con requerimientos técnicos, contenidos en la Norma Técnica Salvadoreña ISO/IEC 27001:2013 "Tecnología de la Información. Técnicas de seguridad. Sistema de gestión de seguridad de la información. Requerimientos; desarrollada por la Organización Internacional de Normalización, (ISO, por sus siglas en inglés) y la Comisión Electrotécnica Internacional (IEC, por sus siglas en inglés); que es un estándar internacional adoptado por el Organismo Salvadoreño de Normalización (OSN), para su aplicación en el territorio salvadoreño y en caso particular para el sector logístico y de transporte de carga; ya que esto ayudará a dar mayor seguridad a los sistemas de información de las organizaciones que lo implementen.

Para la elaboración de las políticas de seguridad informática propuestas, se utilizó la técnica de investigación hipotética deductiva, utilizando la herramienta del cuestionario para la recolección de información, el cual brindó los conocimientos necesarios para realizar el análisis y la evaluación de la necesidad que tienen las empresas del sector, respecto de la aplicación de políticas de seguridad informática.

Las políticas de seguridad informática son un conjunto de reglas aplicadas a todas las actividades relacionadas al manejo adecuado de todos los activos de una empresa, teniendo el propósito de proteger la información, los recursos y la reputación de la misma.

INTRODUCCIÓN

El desarrollo de las nuevas tecnologías posibilita la obtención de mucha información, que en la mayoría de organizaciones no es considerada como un activo importante, en El Salvador, hay cierto reconocimiento para algunos bienes intangibles como la propiedad intelectual, las marcas o logos de las empresas; pero no se le toma mucha importancia a bienes considerados información como base de datos de clientes, conocimiento comercial, documentos legales como contratos en los que se establece términos de negociación y que en las manos incorrectas (competencia) pueden derivar en repercusiones negativas.

Es importante recalcar que en la actualidad el correcto manejo de sistemas de información posibilita mejorar los indicadores operativos y financieros de las organizaciones, determinando cierta ventaja entre las empresas del mismo sector y asegurándoles una posición estable en el mercado o industria en la cual se desarrollan.

Las empresas del sector de logística y transporte de carga son las encargadas de intermediar las relaciones comerciales entre empresas nacionales y extranjeras en todas las áreas de la economía, por lo que, considerando su importancia, se desarrolla la presente propuesta de políticas de seguridad informática, acorde a sus necesidades y condiciones de operación.

En el Capítulo I, se presenta el Marco de Referencia de la investigación, indicando la situación problemática objeto de estudio, el planteamiento del problema, la justificación de la investigación, los objetivos, la hipótesis de trabajo y las limitaciones de la investigación, a fin de contextualizar el desarrollo de la misma en sus diferentes fases.

En el capítulo II, se establece el Marco Teórico, indicando la situación actual de la seguridad informática en las empresas objeto de estudio, los antecedentes del sector analizado, la

importancia de aplicar la propuesta desarrollada, las principales definiciones y finalmente se describe el marco técnico y legal aplicable a la seguridad informática, todo esto con el fin de fundamentar de manera teórica la investigación.

En el capítulo III, se plantea la metodología implementada para la obtención de los resultados necesarios que dieron la pauta para proponer soluciones, además, en este capítulo, se conocen las unidades de estudio y los métodos utilizados para recabar la información suficiente para establecer los respectivos análisis a la problemática, además de analizar los resultados obtenidos de los datos recolectados en las empresas, para finalmente desarrollar el diagnostico.

Posteriormente en el capítulo IV, se desarrolla la propuesta que consiste en la elaboración de políticas de seguridad informática basadas en la Norma Técnica Salvadoreña ISO/IEC 27001:2013, que ayuden a mitigar los riesgos en los sistemas de información, dar seguimiento a los incidentes y controlar las nuevas vulnerabilidades que se generen en los mismos.

Y por último después de haber hecho un estudio de toda la información obtenida en toda la investigación, se redactaron conclusiones y recomendaciones, además en la bibliografía, se presentan las fuentes de información que se utilizó, y un detalle de anexos necesarios para una mejor comprensión de la investigación.

CAPÍTULO I-PLANTEAMIENTO DEL PROBLEMA

1.1 SITUACIÓN PROBLEMÁTICA DE LA SEGURIDAD INFORMÁTICA EN LAS EMPRESAS DEL SECTOR DE LOGÍSTICA Y TRANSPORTE DE CARGA

La seguridad informática tiene un especial valor en los tiempos actuales. Dado al auge del internet, la información privada de los usuarios cada vez tiende a ser más pública. El mundo se encuentra en un momento en que los niveles de información alcanzan límites históricos y en que la sociedad en general se ha dado cuenta del poder que genera la información; en un contexto tan interesante, la seguridad informática parece un tema realmente importante y es por eso que cuenta con el reconocimiento mundial. La seguridad informática en todo caso no es un tema reciente sino de mucha trayectoria.

Para el sector de logística y transporte de carga en el periodo del 2014 al 2016 también ha existido un crecimiento económico derivado de la adquisición de nuevas representaciones de sociedades extranjeras, con lo cual obtuvo más y mejores rutas de servicios logísticos de diferentes países del mundo y esto permitió una mayor cartera de clientes, a nivel local e internacional; esto generó mayor flujo de información entre clientes, proveedores, procesos internos y entidades gubernamentales, es por esta situación que fue necesaria la implementación de herramientas tecnológicas como computadoras portátiles, teléfonos inteligentes, equipos multifuncionales para la impresión, escaneo y almacenamiento de información, servidores locales, intranet, servicio de internet dedicado, memorias flash, correos electrónicos (principal medio de comunicación de las organizaciones) y creación de sistemas de planificación de recursos empresariales (ERP por sus siglas en ingles) para el registro, control y almacenamiento de información. El Banco Central de Reserva dice que:

> En el primer trimestre de 2016 el Producto Interno Bruto (PIB) creció 2.5%, siendo un resultado mayor al del mismo trimestre del año anterior (2.2%). En el trimestre, todas las ramas de actividad económica registraron crecimiento, siendo las más importantes transporte, almacenaje y comunicaciones (4.7%); comercio, restaurantes y hoteles (3.3%); bienes inmuebles y servicios prestados a las empresas (3.1%); industria manufacturera y minas (2.8%); y construcción (2.3%). (Banco Central de Reserva, 2016)

Con el uso de las herramientas descritas anteriormente y la implementación de otras alternativas o formas de laborar como lo es el trabajo en casa o fuera de las instalaciones de la organización, se vuelve necesario implementar políticas que permitan resguardar la información así como mantenerla disponible y de fácil acceso a los usuarios correctos; el robo de información de clientes, proveedores, empleados, rutas de tránsito, precios, costos y otra información empresarial, ha causado que las empresas carezcan de credibilidad y rentabilidad en el sector. Según el Organismo Salvadoreño de Normalización (OSN).

> En El Salvador, las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos. (Organismo Salvadoreño de Normalización [OSN], 2015)

Estas son las principales formas en las que las empresas pierden información de vital importancia para ellas mismas, y por ello se vuelve necesario crear políticas para evitar la pérdida de información y el uso inadecuado de sus sistemas de información.

El sector de logística y transporte de carga es de suma importancia en la economía nacional, por ser el encargado de la intermediación en las operaciones de exportaciones e importaciones de insumos para los diversos sectores económicos, influyendo en la generación de empleos directos e indirectos, contribuyendo así a la globalización de la economía.

Las entidades del sector están inmersas en la carencia de orientación adecuada sobre medidas de control de seguridad de sus sistemas de información que se deben implementar para protegerlo apropiadamente, como consecuencia no poseen políticas que ayuden a gestionar la seguridad informática, que con el desarrollo de la tecnología y medios de comunicación las fallas en la seguridad de los sistemas de información se convierten en una inseguridad. El entorno cambiante y las amenazas que representa requieren que se tomen acciones ante las vulnerabilidades que esto significa; en las empresas en las cuales no se ha tomado conciencia del valor de los activos informáticos.

Las empresas del sector de logística y transporte de carga que brindan servicios en diferentes áreas de la industria, actualmente no han implementado políticas para la seguridad informática, que garanticen el resguardo de la información, su seguridad y reserva; están expuestas a una diversidad de riesgos en sus sistemas de información, en base de datos de clientes, en costos y rutas de servicio en el área marítima y aérea, impactando en los ingresos y cartera de clientes, por lo que es necesario implementar políticas de seguridad informática con el objetivo de generar mayor confianza en el manejo de sus activos tecnológicos.

Dentro del contexto de activos, los sistemas de información son los de mayor importancia dentro de las organizaciones, razón por la cual es necesario protegerlos ante cualquier tipo de peligros que puedan afectar el negocio y perjudicar el cumplimiento de los objetivos estratégicos.

En el sector de logística de carga y transporte se han presentado algunos casos que es importante mencionar como pérdida de información o como distribución de información a los contactos o usuarios incorrectos:

En el año 2005 el gerente de operaciones de una de estas empresas fue despedido, dicho gerente tenía en su poder información valiosa de clientes y contratos con proveedores los cuales administraba y resguardaba en un disco duro externo que era de su propiedad, al momento del despido eliminó toda la información de su computadora asignada y la información que procesaba y resguardaba de la empresa, esto generó problemas dado que muchos embarques (carga que venía para diferentes clientes y de diferentes países) no fue notificada e informada a los clientes finales y se dieron demoras en el servicio *(Nota: esta información fue suministrada por uno de los gerentes, pero por motivos de seguridad no pueden ser revelados los nombres).*

Otro de los casos que sucedió en una de las empresas del sector de logística que distribuye y recibe carga, fue que uno de sus empleados de servicio al cliente, por medio del correo electrónico como uno de los principales medios de comunicación con las estaciones (oficinas en otros países que desarrollan el mismo trabajo que se hace en El Salvador) envió, notificaciones de carga a contactos que no correspondía, esto generó molestia en los clientes a quienes debía de haber llegado la información dado que a quien se le envió dicha información era uno de sus principales competidores, mostrándoles los materiales y costos de los mismos. *(Nota: esta información fue suministrada por uno de los gerentes, pero por motivos de seguridad no pueden ser revelados los nombres).*

1.2 ENUNCIADO DEL PROBLEMA

La problemática planteada anteriormente, causada por la ausencia de políticas de seguridad informática que ayuden a gestionar los riesgos, en los sistemas de información de las empresas del sector objeto de investigación, plantea la siguiente interrogante:

¿Cuáles son los riesgos en los sistemas de información de las empresas del sector de logística y transporte de carga del municipio de Antiguo Cuscatlán, por no contar con políticas de seguridad informática?

1.3 JUSTIFICACIÓN DE LA INVESTIGACIÓN

1.3.1 Novedoso

La facilidad para realizar cualquier tipo de negocios a través de internet y dispositivos inteligentes en las empresas no sólo ha traído beneficios, lógicamente también han surgido nuevos riesgos para el resguardo de la información; es por ello que las empresas tienen que tomar medidas que orienten a sus empleados sobre el uso adecuado de la tecnología que se posee y dar recomendaciones para evitar el uso indebido de la misma; además de hacer énfasis que la seguridad informática no solo es obligación de la gerencia de tecnologías de información, sino que es obligación de cada uno de los empleados que están relacionados con los clientes, proveedores y con toda la administración en general. Debido a que se carece de políticas de seguridad informática dirigidas a las empresas en el sector de logística y transporte de carga, ubicado en el municipio de Antiguo Cuscatlán, además que no existe una propuesta sobre esta problemática en la Universidad de El Salvador, ni en ningún otro centro de estudios de educación superior en El Salvador.

1.3.2 Factible

La seguridad informática posee un marco normativo y legal aplicable, basado en la norma técnica internacional aplicable adoptada por el Organismo Salvadoreño de Normalización, siendo

esta la Norma Técnica Salvadoreña ISO/IEC 27001:2013 “Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requerimientos”, además de COBIT 5 para la Seguridad de la Información (COBIT 5 for Information Security, en inglés), publicado por la Asociación de Auditoria y Control de Sistemas de Información (ISACA, por sus siglas en inglés) y la normativa legal salvadoreña aplicable que es la Ley especial contra delitos informáticos y conexos, Decreto Legislativo No. 260, de fecha 4 de febrero de 2016; publicado en el Diario Oficial No. 40 Tomo 410, del 26 de febrero de 2016.

1.3.3 Utilidad Social

La investigación tiene la finalidad de aportar a las empresas del sector de logística y transporte de carga, políticas de seguridad informática, para la prevención y reducción de los riesgos a los cuales son vulnerables tales empresas, garantizará la confidencialidad, integridad y disponibilidad de la misma. La implementación de políticas servirá a todos los empleados de las empresas, así como a las principales gerencias de tecnología, administrativas, generales, contadores públicos, departamentos de auditoría y demás entes relacionados con el sector de logística y transporte de carga, para resguardar activos tecnológicos de suma importancia, contribuyendo con el cumplimiento de los objetivos para este sector.

1.4 OBJETIVOS DE LA INVESTIGACIÓN

1.4.1 General

- Proponer políticas de seguridad informática basado en la Norma Técnica Salvadoreña ISO/IEC 27001:2013 “Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requerimientos”, para las empresas del sector de logística y transporte de carga del municipio de Antiguo Cuscatlán.

1.4.2 Específicos

- Diagnosticar la situación actual de la seguridad informática del sector de logística y transporte de carga del municipio de Antiguo Cuscatlán.
- Identificar los riesgos en los sistemas de información de las empresas del sector de logística y transporte de carga, para su posterior mejora.
- Formular políticas para mitigar los riesgos que se identifiquen en los sistemas de información de las empresas del sector de logística y transporte de carga.

1.5 HIPÓTESIS

1.5.1 Hipótesis de trabajo

- La aplicación de políticas de seguridad informática basadas en la Norma Técnica Salvadoreña ISO/IEC 27001:2013, en las empresas del sector logístico y transporte de carga, minimizaría los riesgos en los sistemas de información de las mismas.

1.6 LIMITACIONES

Las principales limitaciones que se presentaron en la ejecución de la investigación son las detalladas a continuación:

- A pesar de obtener información de hechos relacionados con la seguridad informática no se permitió divulgar en este trabajo de investigación el detalle específico de las personas que lo generaron.
- La implementación de políticas de seguridad informática en las organizaciones objeto de estudio, dependerá exclusivamente de las gerencias y altos mandos de cada entidad.
- La encuesta fue respondida por el personal a quienes se seleccionó como unidades de análisis, y las respuestas seleccionadas fueron de exclusiva responsabilidad de los mismos.

CAPÍTULO II-MARCO TEÓRICO, CONCEPTUAL, TÉCNICO Y LEGAL

2.1 ESTADO ACTUAL DE LA SEGURIDAD INFORMÁTICA EN LAS EMPRESAS DEL SECTOR DE LOGÍSTICA Y TRANSPORTE DE CARGA

En el 2017 los ataques a las plataformas virtuales de los grupos empresariales del sector de logística y transporte de carga se han vuelto muy común, a continuación, se presentan los casos más conocidos y las consecuencias que han tenido. El grupo MAERSK LINE publicó el siguiente comunicado el día 06 de julio del año 2017 como resultado de un ataque sufrido en dicha fecha en sus bases de datos y demás plataformas virtuales:

> "Estimado cliente, Esperamos que esté teniendo un buen día. Hoy queremos nuevamente compartir con usted los progresos que estamos haciendo para alcanzar la recuperación total. Esto ha demostrado ser un proceso largo con un progreso continuo, sin embargo, aún existen áreas donde necesitamos avanzar más.
>
> Los sistemas críticos para el negocio y canales *online* ya están funcionando. Esto permite que todos los negocios nuevos puedan continuar casi como siempre. Sin embargo, mientras seguimos poniéndonos al día con los pendientes acumulados, usted experimentará una respuesta más lenta de la normal. Si bien estamos complacidos con el progreso que hemos hecho para poder servir apropiadamente a nuestros clientes de exportación, estamos muy conscientes de que la experiencia en importaciones aún no ha logrado volver a los niveles que debiese estar. Sabemos que el no tener total visibilidad de la carga que está en nuestro poder le genera preocupación. Entendemos la importancia de esto, por lo que no nos tomamos a la ligera las preguntas que surgen al respecto.
>
> Mientras que muchas de las aplicaciones clave (reservas/bookings, instrucciones de entrega, impresión de BLs, etc.) ya se encuentran disponibles en My.Maerskline.com, no

hemos habilitado las aplicaciones de monitoreo de carga (track and trace) debido a un significativo número de estados de tránsito que aún están pendientes. Esto se debe al hecho de que, durante el periodo de disrupción, las operaciones de nuestras naves y movimiento de carga casi no se vieron afectadas, pero no pudimos cargar las ubicaciones de los envíos en el sistema. Es por esto que podría ser confuso para usted el monitorear su carga en esta etapa, previo a que hayamos ingresado manualmente el total de la data en el sistema. Nos encontramos trabajando arduamente para completar la actualización y habilitar la aplicación para darle total visibilidad.

Por el momento, si usted tiene cualquier duda respecto al estado de los envíos, por favor contacte a su equipo local de servicio al cliente. Tenemos un ajustado y ambicioso plan que nos permitirá volver a estar funcionando casi como usted acostumbra en el servicio de importaciones para inicios de la próxima semana.

Tal como hemos compartido con usted en anterioridad, tenemos conexión telefónica en todos los mercados. Sin embargo, las líneas centrales de servicio al cliente por ahora no están operativas consistentemente alrededor del mundo. En lugares donde éste es el caso, usted debe haber recibido contactos telefónicos alternativos además de correos electrónicos.

Adicionalmente, lamentamos que aún no hayamos podido establecer un proceso de difusión de precios a aquellos clientes que embarcan con tarifas de corto plazo. Estamos trabajando diligentemente en resolver esto. Respetaremos todas las tarifas comunicadas y nos aseguraremos de que todos los cambios se vean reflejados, incluso retroactivamente. También esperamos estar operando totalmente en esta área a principios de la próxima

semana. Seguimos actualizando contenido en www.maersk.com/operationalupdate. Queremos poder guiarlo lo mejor posible en el estatus e implicaciones en los mercados locales hasta que volvamos a la total normalidad en todos lados.

Una vez más, algo que es de gran importancia para muchos, podemos compartir y confirmar que como parte del proceso de recuperación estamos aplicando las actualizaciones disponibles para los sistemas afectados de acuerdo con las recomendaciones de los proveedores de TI antes de la reactivación de cualquier sistema. El proceso de recuperación les permitirá a nuestros socios utilizar y comunicarse con los sistemas Maersk de nuevo sin ningún riesgo de ser afectados por el virus.

Finalmente – y no podemos repetirlo lo suficiente – muchas gracias una vez más por su continua paciencia y comprensión. Le podemos asegurar que estamos haciendo todo lo que está en nuestras manos para servir su negocio de manera efectiva y segura. ¡Muchas gracias! (MAERSK, 2017)"

Otro incidente sufrido por el mismo grupo el día 27 de junio del 2017 en sus plataformas virtuales se describe a continuación en el comunicado publicado por dicho grupo empresarial:

"A raíz de nuestras comunicaciones de ayer (27 de junio de 2017) sobre el impacto del ciberataque global Petya, en el grupo AP Moller-Maersk, podemos confirmar que algunas de nuestras infraestructuras de TI y comunicaciones han sido impactadas y algunos de nuestros sistemas permanecen cerrados proactivamente como una medida de seguridad.

Por ahora esto significa lo siguiente:

> Todas las operaciones de buques continuarán según lo programado, haciendo la mayoría de las llamadas portuarias planificadas. El acceso a la mayoría de los puertos no se ve afectado, sin embargo, algunas terminales de APM Terminals se ven afectados y las puertas están cerradas. La carga en tránsito será descargada según lo planeado. La carga de importación será liberada para clientes con crédito.
>
> Desafortunadamente no podemos ofrecer nuevas cotizaciones ni aceptar reservas futuras. Sin embargo, apreciamos mucho su paciencia y esperamos llevar su carga tan pronto como nos sea posible. Desafortunadamente, y debido al impacto en nuestros sistemas de TI y comunicaciones, estamos limitados en nuestra capacidad para comunicarnos con usted. Continuaremos enviándole correos electrónicos cuando sea apropiado y actualizaremos regularmente nuestros canales de redes sociales.
>
> Pedimos disculpas una vez más por cualquier inconveniente que esto pueda causar a su negocio y estamos trabajando duro para reanudar operaciones normales tan pronto como sea posible. El Equipo de Maersk (MAERSK, 2017)

2.2 PRINCIPALES DEFINICIONES

Las siguientes definiciones ayudaran a comprender de mejor forma los términos técnicos básicos relacionados con la investigación, así como los aspectos de seguridad y el sector empresarial en el que se implementaran.

- **Información:** la definición de información en el contexto empresarial es bastante amplio y complejo ya que lo que puede ser información para algunos para otros no es relevante, la definición más acertada de lo que es información la encontramos en la norma técnica

Norma Técnica Salvadoreña ISO/IEC 27001:2013 la cual define información de la siguiente manera:

Se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail y transmitida en conversaciones), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración. (NTS ISO/IEC 27001, 2013)

- **Normas ISO:** Son documentos que proporcionan especificaciones, requisitos, recomendaciones y guías que las organizaciones pueden emplear para afinar procesos, productos y servicios; de esta manera volverse más competitivas y eficientes, de las cuales se pueden obtener certificaciones para obtener reconocimiento a nivel mundial.
- **Políticas de seguridad informática:** son las que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. Un sistema informático puede ser protegido desde un punto de vista lógico (con el desarrollo de software) o físico (vinculado al mantenimiento eléctrico). Por otra parte, las amenazas pueden proceder desde programas dañinos que se instalan en la computadora del usuario (como un virus) o llegar por vía remota (los delincuentes que se conectan a Internet e ingresan a distintos sistemas).

  Entre las herramientas más usuales de la seguridad informática, se encuentran los programas antivirus, los cortafuegos o firewalls, la encriptación de la información y el uso de contraseñas (passwords). Herramientas todas ellas de gran utilidad como también lo son los conocidos sistemas de detección de intrusos, también conocidos como anti-spyware.

Un sistema seguro debe ser íntegro (con información modificable sólo por las personas autorizadas), confidencial (los datos tienen que ser legibles únicamente para los usuarios autorizados), irrefutable (el usuario no debe poder negar las acciones que realizó) y tener buena disponibilidad (debe ser estable). En otras palabras, puede decirse que las políticas de seguridad informática buscan garantizar que los recursos de un sistema de información sean utilizados tal como una organización o un usuario lo ha decidido, sin intromisiones.

- **Seguridad informática:** Se refiere a las características y condiciones de un sistema de procesamiento de datos y su forma de almacenamiento que garantizara su seguridad en base a los atributos de confidencialidad, integridad, y disponibilidad, que busca considerar los peligros que causa la vulnerabilidad a este activo, clasificar la información en pública y privada y protegerse de los daños por las amenazas.
- **Sector de logística y transporte de carga:** dentro de un contexto empresarial podemos mencionar que existen diferentes procesos que permiten a las empresas o fabricantes planear y gestionar una serie de actividades tales como la adquisición de materia prima, fabricación de productos terminados, comercialización, almacenaje de estos.

  Por lo que la logística y transporte de carga es la que se delega para la entrega de los productos o insumos necesarios en el lugar correcto y en el momento oportuno a fin de satisfacer las necesidades de quien requiere el producto movilizándolo desde un lugar de origen hasta un lugar de destino adecuado. (CASTRO, 2011)

2.3 GENERALIDADES DE LA SEGURIDAD INFORMÁTICA

2.3.1 Antecedentes de incidentes en la seguridad informática

Los ataques informáticos en los últimos años han sido más frecuentes algunos de los más sonados se listan a continuación:

En 2010 ocurrió el ataque conocido como *"operación Aurora"* se trató de un ataque proveniente de China, altamente sofisticado dirigido contra al menos dos docenas de compañías importantes, entre ellas Google quienes decidieron darlo a conocer, conforme a lo explicado por la firma de seguridad McAfee, identificaron una vulnerabilidad de tipo *"zero-day"* en Microsoft Internet Explorer, que sirvió como punto de entrada para que operación aurora afectara a Google y al menos a otras veinte empresas. Se sabe que la operación se saldó con robos de propiedad intelectual, obtención de acceso a cuentas de correo y un conflicto serio entre la empresa Google, el gobierno de EE. UU y el gobierno de China. La operación llamo mucho la atención porque fue un robo de inteligencia a las empresas de mayor tecnología del mundo. Una operación que duró meses y que hizo que las Amenazas Persistentes Avanzadas (APT por sus siglas en inglés) se tomara mucho más en serio.

En 2010 el robo de información protegida se hizo común, uno de los robos más sonado fue la sustracción de documentos cometida por *Aaron Swartz* de unos cuatro millones de documentos y aplicaciones bajo copyright del repositorio digital de publicaciones académicas Journal Storage (JSTOR, por sus siglas en inglés) a través de las redes del Instituto Tecnológico de Massachusetts. También fue conocido el hurto de certificados digitales a la empresa Realtek, de no mucho volumen, pero bastante serio, utilizando este certificado robado misteriosamente a Realtek se consiguió llevar a cabo el ataque de Stuxnet contra las centrales de centrifugación de uranio de Natanz Irán. (ELDIARIO ES, 2012)

El robo de información más sonado llegó con la publicación de 250,000 documentos del Departamento de Estado norteamericano por la organización *Wikileaks*, Estos documentos fueron obtenidos por el analista de inteligencia del ejército de los Estados Unidos Bradley Manning mediante los ordenadores que utilizaba cuando se encontraba de servicio en una base

militar de Bagdad, los mismo estaban conectados a la red *SIPRNet* que el Pentágono emplea para los documentos clasificados; este es el robo informático que más repercusión ha tenido puesto que aunque no ha sido un robo monetario, ha hecho tambalearse a Estados Unidos y otras naciones. Además de ser el principio de todo el movimiento de *Anonymus* y todas las demás evoluciones.

"Wikileaks desarrolla una versión no censurable de Wikipedia para la publicación masiva y el análisis de documentos secretos *("Leaks"),* manteniendo a sus autores en el anonimato." (WikiLeaks, 2010)

Tanto en 2011 como en 2012 se produjeron robos informáticos de información, uno de ellos apuntado por Sebastián Bortnik, gerente de educación y servicios de ESET LLC para Latinoamérica, este es el que sufrió la plataforma PlayStation Network de donde cibercriminales sustrajeron datos personales de 77 millones de usuarios.

Otro, de los robos de información sonados fue la denominada: " *Operation Anti-Security*", denominación bajo la que los grupos Anonymous y LulzSec lanzaron ataques contra gobiernos, empresas e instituciones a lo largo de meses y sustrajeron todo tipo de información que posteriormente publicaron en la red.

Anonymous y LulzSec, dos de los grupos de piratas informáticos y hackers más conocidos en todo el planeta, decidieron unir sus fuerzas con el objetivo de llevar a cabo una serie de ataques de ciberterrorismo contra las páginas web y sitios online del gobierno de Estados Unidos, contra sus entidades bancarias y financieras, así como filtrar información sensible sobre cuentas y datos en la Red. (Guzmán, 2011)

El Salvador no está ajeno a esta realidad ya que también en este territorio tan pequeño se cometen robos de información a gran y pequeña escala, como lo señalan periódicos locales como el que citamos a continuación:

> En 2011, las páginas web de diferentes dependencias de gobierno de El Salvador fueron blanco de ataque informático, páginas como la del Ministerio de Seguridad, Presidencia y Policía Nacional Civil sufrieron diversos ataques que obligaron a bajar los sitios, no sin antes haber tomado y divulgada información de usuarios y algunos passwords de cuentas importantes. También la página oficial del partido Alianza Republicana Nacionalista (ARENA) fue blanco de ataques durante ese año por parte del grupo *Anonymus.* (LA PAGINA, 2011)

> Los casos de clonación de tarjetas, de sitios web, venta ilegal de bases de datos son casos bien conocidos en El Salvador. Los correos fraudulentos ya no son exclusivos de bancos, sino han pasado a atacar aerolíneas, empresas de comunicaciones, de ropa, supermercados y ferreterías. El robo de información esconde cifras tenebrosas. El mayor problema es que las empresas no lo detectan, tienen daños y ataques, y ni se les imagina relacionarlo con robo de información. Las armas de los ladrones son las cámaras en sus móviles, memorias USB, copiadoras, emails y todo el TIC de una empresa. (EL DIARIO DE HOY [EDH], 2015)

A mediados del año 2016 se produjeron ataques cibernéticos a páginas web de empresas reconocidas como lo son el sitio web de La Prensa Gráfica, El Diario de Hoy y algunas dependencias del gobierno, para poder dar respuesta a este tipo de delitos se creó la ley especial contra los delitos informáticos y conexos, con la cual se pretendía dar una herramienta útil a las autoridades para erradicar o minimizar este tipo de delitos.

2.3.2 Importancia de aplicar políticas de seguridad informática en las empresas

A lo largo del tiempo la información siempre ha estado presente en todos los aspectos de la vida y en el desarrollo de las empresas ha obtenido un valor muy alto dentro de las mismas, es por ello que es considerada el mayor activo de una empresa porque es uno de los recursos fundamentales para el desarrollo normal de los procesos que manejen y los cuales son la razón de ser de la organización. Al respecto el libro sociedad de la información y educación nos narra que:

> La digitalización y la automatización han provocado una profunda revolución, caracterizada especialmente por la aparición de dispositivos multimedia y por una expansión espectacular de las redes telemáticas. Los sistemas expertos y la inteligencia artificial aumentan vertiginosamente la interactividad... La velocidad de procesamiento de la información crece constantemente, así como la capacidad casi ilimitada de almacenamiento. (Entonado, 2001)

La información en cierto modo es intangible y por esto es necesario contar con un soporte, entre las múltiples formas que existen se resalta que antiguamente la información se plasmaba en documentos y hoy en día por los avances en la tecnología, los procesos se están almacenando en sistemas informáticos los cuales se transmiten a través de las redes, siendo así como se empieza a establecer la sistematización.

Es innegable la importancia que tiene la información para una organización, bajo ese contexto se puede tomar como referente la definición siguiente: “La información es un activo que, como otros activos comerciales importantes, tiene valor para la organización y, en consecuencia, necesita ser protegido adecuadamente”. (NTS ISO/IEC 27001, 2013) De acuerdo a lo anterior es inevitable que las organizaciones tomen las medidas necesarias para mantener protegida la información y así mismo los medios en los que se encuentra soportada esta.

Por esta razón es importante que las empresas implementen políticas que les permita salvaguardar la información, creando controles efectivos que impidan que los perpetradores tengan acceso no controlado a los sistemas, con intereses malintencionados como el robo de la información o ejecutar acciones delictivas que puedan afectar la continuidad del negocio. Para evitar cualquier riesgo de pérdida, robo y manejo inadecuado de su información, las empresas deben implantar políticas de seguridad informática, con el fin de gestionar los riesgos y así minimizar la materialización de estos, la norma técnica salvadoreña define la gestión de riesgos como "las actividades coordinadas para dirigir y controlar una organización en relación con el riesgo." (NTS ISO/IEC 27001, 2013) Y a la vez establece la seguridad de la información como la preservación de la confidencialidad, la integridad y la disponibilidad de la información.

La gestión de la seguridad informática debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Para lograrlo el proceso debe de estar fundamentado en cuatro conceptos importantes, los cuales son:

- **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.

El aplicar políticas de seguridad, en la actualidad más que lujo de ha vuelto una necesidad con la que cuentan las organizaciones ya que su importancia radica en los beneficios que puede obtener una empresa que las implementen, tales beneficios a corto plazo son: la disminución del impacto de los riesgos por perdida, robo u malversación de información de vital importancia para la misma,

mayores garantías de continuidad del negocio basadas en la adopción de un plan de contingencias respecto del cuido de su información; la mejora de la imagen de la organización y el aumento del valor comercial de la empresa y sus marcas, una mayor confianza por parte de clientes, proveedores, accionistas y socios; una mejora del retorno de las inversiones, el cumplimiento de la legislación y normativa vigentes.

Además, con la implementación de políticas de seguridad, los clientes tienen acceso a la información mediante medidas de seguridad más eficientes, los riesgos y controles son continuamente evaluados y las organizaciones obtienen una mejor practica que la diferencia de la competencia, ya que es mejor hacer negocios con empresas que se conoce que están creando mecanismos de control y resguardo de información que con las empresas que no poseen medidas ni controles de resguardo de la misma.

2.4 GENERALIDADES DEL SECTOR DE LOGÍSTICA Y TRANSPORTE DE CARGA

2.4.1 Antecedentes del sector de logística y transporte de carga

Con el auge del comercio internacional el sector de la logística y transporte de carga se convierte en una poderosa herramienta que se utiliza para potenciar el traslado de los bienes, las formas principales de transporte de carga son marítimo, terrestre y aéreo. En El Salvador los primeros avances del sector logístico se puede ver en la construcción del puerto de Acajutla para ello el 28 de mayo de 1952 se creó la Comisión Ejecutiva del Puerto de Acajutla y en 1961 se logra la inauguración del denominado muelle “A” lo cual dio apertura al intercambio comercial y a desarrollar la competencia económica en el país, debido a la demanda y al éxito obtenido en los años 1970 se construyó el muelle “B” y en 1975 se finalizó el muelle “C”.

En virtud de la creciente demanda del tráfico portuario y al propio desarrollo de la Comisión Ejecutiva del Puerto de Acajutla, en 1965 el Gobierno decidió ampliarle sus facultades,

> concediéndole la administración, explotación y dirección de los Ferrocarriles Nacionales de El Salvador (FENADESAL), incluido el Puerto de Cutuco; convirtiéndose de esta manera en la actual Comisión Ejecutiva Portuaria Autónoma (CEPA). En el año de 1976 se le confió la construcción, administración y operación del Aeropuerto Internacional El Salvador el cual iniciaría a brindar servicios al público en general a partir de enero de 1980, con esto el país abría las puertas a más y mejores relaciones comerciales a nivel global. (CEPA, 2010)

El comercio internacional como tal es regido bajo ciertos términos de compra establecidos por la International Chamber of Commerce (ICC) o Cámara de Comercio Internacional en español. Los INCOTERMS que significan Términos Internacionales de Comercio, en los cuales el comprador y el vendedor establecen sus obligaciones, tanto del lugar de entrega del producto convenido como de los costos que ellos asumirán, en la figura 1 se podrán ver el resumen de los mismos.

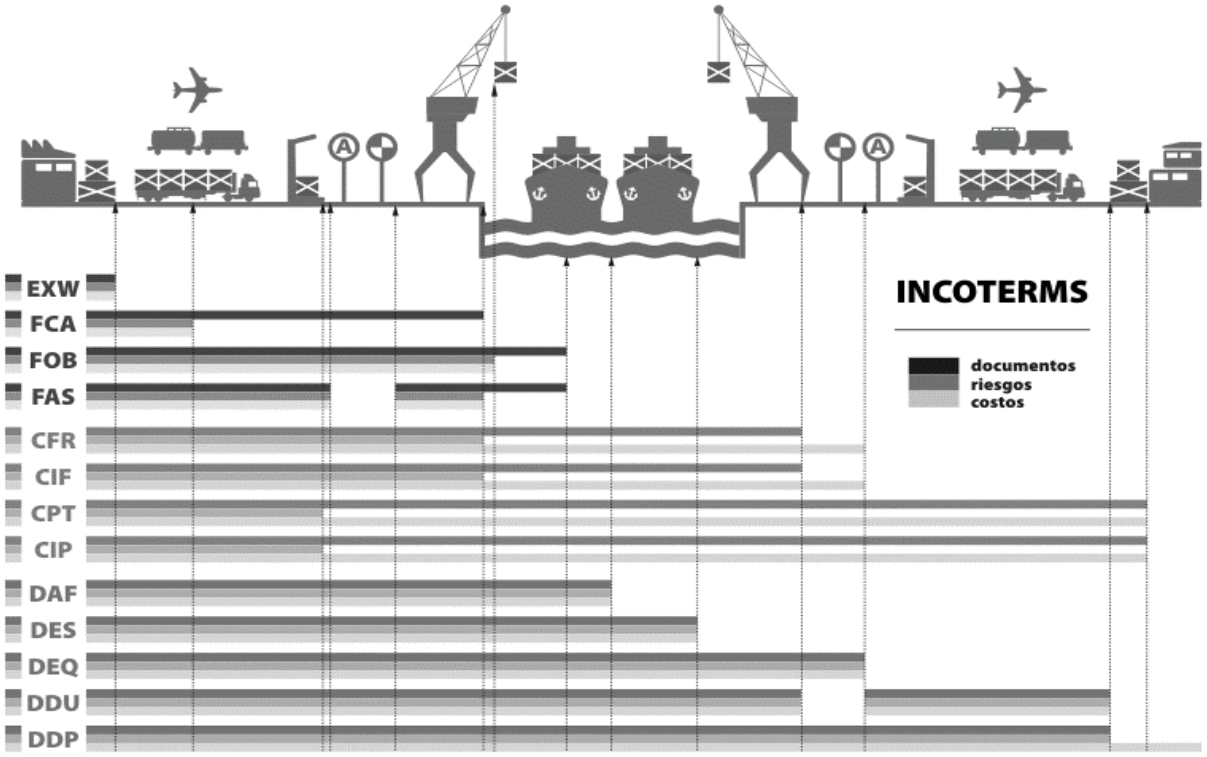


Figura 1 Esquema de INCOTERMS
Fuente: www.comercioyaduanas.com.mx

El esquema anterior muestra los diferentes tipos de INCOTERMS que existen en el comercio internacional y las obligaciones del comprador y el vendedor dependiendo del termino de compra que se utiliza, en todos es necesario la intervención del sector logístico para transportar los bienes de un origen a un destino o de un país a otro, estableciendo así la importancia del sector de logística y transporte de carga, en el cual las empresas de la cadena de logística adquieren compromisos documentales y económicos para que el producto se movilice eficazmente.

La balanza comercial de El Salvador muestra que las variaciones entre exportaciones e importaciones del 2013 al 2016 son mínimas aunque existe un porcentaje mayor de las exportaciones por lo que la brecha o déficit de la balanza ha disminuido porcentualmente, comparando el 2014 las exportaciones fueron de $4,021.80 millones vs 2015 que fueron de

$4,224.5 millones lo cual representa un incremento del 5% y esto significa mayor participación del sector de logística y transporte de carga para la distribución de estos productos a nivel mundial.

Inversiones importantes que CEPA estará realizando en el Aeropuerto Internacional de El Salvador Monseñor Oscar Arnulfo Romero y Galdámez y en el Puerto de Acajutla, podría significar para el país una mayor eficiencia en la cadena de suministros que el país necesita y con esto se iniciara la búsqueda del camino hacia el futuro en el cual las estrategias articuladas de los diferentes sectores tanto gobierno, empresa privada, organizaciones internacionales, población se verán beneficiados por los cambios, y desarrollo que esto representara en el país.

> Es necesario incentivar la inversión extranjera en el país y esto solo se puede lograr con un ambiente más atractivo y competitivo para los inversionistas que conlleve al desarrollo sostenido de la economía, como parte fundamental de este desarrollo el comercio internacional necesita de costos operativos bajos los cuales pueden lograrse con una logística y transporte de carga adecuada que les permita obtener servicios de estándares de calidad mundial a precios razonables alcanzando un movimiento de la cadena de suministros ágil y funcional a medida que se entreguen los bienes en forma oportuna y correcta. (PROESA, 2013)

Toda empresa local que exporte sus productos o inversionista extranjero que necesite crear fábricas y mantener costos bajos necesitara de un suministro diversificado de logística de carga y no solo para el movimiento del producto terminado o materia prima sino también para su almacenamiento y distribución.

Las estrategias articuladas que influyen en la eficiencia de los puertos, aeropuertos, fronteras, estructuras viales contemplan la integración del gobierno a través del Ministerio de

Hacienda y su división de Dirección General de Aduanas (DGA) como fiscalizador pero también como facilitador del comercio en paralelo con las empresas del sector de logística y transporte de carga que son los que velan por el cumplimiento de los requisitos de los importadores y exportadores tanto documental como en pago de impuestos para dar continuidad a los procesos establecidos por la DGA para liquidación de carga.

2.4.2 Antecedentes de empresas representativas del sector de logística y transporte de carga en El Salvador

A continuación, se presenta una breve reseña histórica de las empresas que gestionaron el crecimiento del sector de logística y transporte de carga en los últimos años en El Salvador:

- Mudanzas Internacionales S.A. (MUDISA): se definen según su página Web como la empresa de carga y mudanzas internacionales más grande de El Salvador. Fue fundada en el año de 1,963 como parte de una iniciativa familiar, con la finalidad de brindar servicios con los más altos estándares de calidad en el área de las mudanzas y carga general. MUDISA cuenta con bodegas de 22,500 pies cuadrados y oficinas de 6,500 pies cuadrados, ubicados sobre la carretera que conduce al aeropuerto internacional de Comalapa y el puerto de Acajutla.

  Dentro de las bodegas de MUDISA se encuentra la sección de carpintería, que facilita la elaboración de cajas, vanes y jabas de madera de acuerdo a los requerimientos del cliente para el acomodo de sus pertenencias. El transporte terrestre dentro de El Salvador es proveído a través de su propia flota de camiones. (MUDISA, S.A. DE C.V., 2005)

- Comercial Centroamérica (COMCA) Internacional es una empresa de soluciones logísticas en transporte y distribución que opera en El Salvador desde 1967. Se consolida como la

empresa de capital nacional líder en el servicio de transporte, almacenaje y mudanzas. Actualmente cuenta con más de 48 años de experiencia en el mercado salvadoreño, gracias a las alianzas estratégicas con empresas de primer nivel y afiliación a diversas instituciones internacionales, que han permitido ofrecer un servicio de primer nivel con tarifas sumamente competitivas.

COMCA Internacional es representante exclusivo para El Salvador de DB Schencker, empresa líder en su campo, con presencia en más de 120 países a nivel mundial y que permite ofrecer tarifas competitivas. La excelencia de los servicios ha permitido alcanzar a este grupo empresarial el reconocimiento a la calidad ISO 9001-2008. La renovación de esta certificación es producto del esfuerzo que la empresa, colaboradores y proveedores realizan para satisfacer a sus clientes y mantener una mejora continua en sus procesos administrativos y operativos.

COMCA Internacional ha logrado posicionarse como una agencia de carga, representante de Líneas Navieras y proveedor de servicios de Mudanzas Internacionales y locales; con el personal, la infraestructura y el conocimiento necesario que le permite ofrecer servicios de clase mundial (COMCA EL SALVADOR, 2012)

- En El Salvador, DHL Global Forwarding inició operaciones a partir de 1,995 ofreciendo una amplia gama de servicios logísticos, dentro de los cuales destacan la distribución terrestre hacia todo Centroamérica, Panamá y México, contando para ello con una flota de más de 100 furgones (45, 48 y 53 pies de largo) tanto propios como subcontratados. Actualmente entre sus principales clientes podemos mencionar a: Livsmart, Grupo CYBSA, Grupo Sigma, Laboratorios Biogalenic, etc.; cuyos productos son entregados a clientes radicados en cada uno de los países mencionados anteriormente.

Otro servicio ofrecido por DHL GF El Salvador es la distribución marítima a diferentes destinos en el Caribe, Norte, Centro y Sur América, haciendo uso de contenedores herméticamente sellados de 20 y 40 pies de largo, que garantizan la seguridad en la entrega y la inocuidad del producto que se transporta en éstos. Para lograr tales propósitos, DHL GF posee alianzas estratégicas con las principales navieras existentes en el mercado de las exportaciones o importaciones. (DHL, 2007)

- Crowley Logistics: En julio de 2005, inauguró un Centro de Distribución en Colón, La Libertad, inversión estimada en un poco más de un millón de dólares; consistente en una bodega de 18 mil pies cuadrados, la cual sirve de apoyo a las empresas maquiladoras de ropa que operan en la zona. ¨Este centro de distribución está orientado a recibir cargamentos de insumos y productos para el sector textil¨ (Crowley Maritime Corporation, 2017)
- En noviembre del 2006 la empresa Represa Algodonera y Almacén Nacional (RANSA) como parte de la apuesta por desarrollar el país como un centro logístico regional invirtió alrededor de $10 millones en las bodegas de almacenaje de más de 17 mil metros cuadrados en una primera etapa, ubicados sobre la Nueva Carretera Panamericana, CA-1, Cantón Joya Galana. Instalaciones en las cuales son almacenados productos para clientes reconocidos tales como Kellogg, Nestlé y Mabe. Actualmente, RANSA ofrece soluciones especializadas para atender los requerimientos logísticos de los clientes en las áreas de minería y energía, consumo masivo, industria y logística refrigerada, contando para ello con modernos sistemas de información y soluciones tecnológicas. (RANSA, 2017)

2.4.3 Empresas del sector de logística y transporte de carga, ¿cómo funcionan?

Las empresas del sector de logística y transporte de carga son aquellas que, realizan los procesos para la importación y exportación de artículos, mercadería y/o productos desde un origen hasta un destino, tanto local como internacional; el transporte de la mercadería puede ser aéreo, marítimo o terrestre, este último a través de tren, furgones, camiones o contenedores.

Las empresas de logística deben de estar legalmente constituidas y registradas ante el ministerio de hacienda y forman parte de la red de auxiliares de la administración aduanera, ya que estas empresas deben velar por el cumplimiento de los tramites y procesos para la importación y exportación de las mercaderías, y con esto contribuir al cumplimiento de todos los requisitos que la administración aduanera estipula, alguno de estos son el pago de impuestos y aranceles especiales, permisos y autorizaciones para productos especiales o restringidos, entre otros.

En El Salvador existen empresas que brindan servicios de logística integral, esto se refiere en la importación: contratar el servicios de transporte que se apegue a las necesidades del cliente (importador o exportador) y producto a transportar los cuales pueden ser aéreos o marítimos, realizar los trámites en origen (directamente o a través de la red de agentes de carga que posean en el país de origen) para la importación del producto, pre-alertar al consignatario de la carga en destino del arribo de la carga, realizar los trámites necesarios ante la aduana para el pago de impuestos y liberación de la carga, movilización de la carga desde el puerto o aeropuerto hasta la bodega del cliente, o almacenaje de la carga si el consignatario no tiene espacio de bodega en el momento de la descarga.

En el caso de la exportación: contratar el servicio de transporte que más se apegue a las necesidades del cliente, aéreo, marítimo o terrestre, realizar los documentos que respalden el proceso de exportación y elaborar el trámite respectivo (elaboración de declaración de mercancía,

pago de impuestos, revisión física ante la aduana), colocar el medio de transporte en el lugar convenido para la carga del producto, hacer el despacho de este medio de transporte e informar al exportador que su carga ha sido despachada, brindar fechas de llegada a destino y notificar al cliente o consignatario en destino del arribo de la carga, si dentro de las negociaciones incluye la entrega en bodega final se hace el servicio de trámite en el país o lugar de destino y el transporte desde el aeropuerto o puerto para e lugar de descarga.

Las empresas de logística forman parte de una red de empresas del sector a nivel mundial a través de marcas registradas (DB Shenker, Zim Integrated Shipping Services) o asociaciones (International Association of Movers IAM, Asociación Salvadoreña de Agentes de Carga, ASAC), con esto cada empresa puede brindar servicios en otros países sin tener su empresa radicada en ese país, ya que atreves de convenios con estas marcas o asociaciones, la empresa que radica en ese país y forma parte de esa red brinda los servicios.

Las empresas del sector elaboran contratos de servicios con empresas internacionales para poder representarles en el país y brindar (vender, administrar, controlar y promover los servicios o rutas que las empresas internacionales poseen) los servicios que estas multinacionales ofrecen tal es el caso de ZIM Integrated Shipping Services, que es una Naviera Israelí y necesitaba que una empresa del sector de logística le representara en El Salvador, fue así que en negociaciones con Triton Logistics S.A. de C.V. (empresa legalmente constituida en El Salvador, conocida también como Trilog) llegaron al convenio y firmaron contrato en el cual Trilog promovería los servicios navieros (transporte marítimo de carga en contenedores y barcos) y ZIM retribuiría a través de comisiones y pagos de porcentajes de la operación.

Trilog con la firma de este contrato forma parte de la red de empresas del sector que brindan los servicios de ZIM en el mundo y es el único en El Salvador autorizado para brindar estos

servicios, con lo anterior al buscar un servicio en la página web de ZIM (www.zim.com) para El Salvador se muestra Triton Logistics como la empresa en el país que ayudara a los clientes con los servicios que requieran, es por ello que Trilog es la encargada de informar a todos los clientes de la carga que es transportada en los barcos y contenedores de ZIM, que provienen de diferentes puertos y países del mundo y que su destino final es en El Salvador, con esto dar el servicio, seguimiento y hacer los trámites necesarios para movilizar la carga del puerto de destino hacia las bodegas de los clientes o el lugar convenido en el documento de transporte, cotización o contrato.

Adicional a los servicios de logística también es el encargado de hacer los cobros respectivos que pertenecen a ZIM y los cargos locales que pertenecen a Trilog, los cuales son reportados en ventas propias y ventas a cuentas de terceros para los cuales deben de pagarse los impuestos respectivos.

Las empresas del sector de logística y transporte de carga pueden entonces brindar servicios de importación aérea, marítima y terrestre de cualquier tipo de producto, desde una pastilla (laboratorios) hasta una maquina industrial (manufactura o proyectos industriales) por lo que representan un factor importante para la economía de las empresas privadas y sector público.

2.5 GENERALIDADES DE LA NORMA TÉCNICA SALVADOREÑA ISO/IEC 27001:2013

2.5.1 Antecedentes de la Norma Técnica Salvadoreña ISO/IEC 27001:2013

La ISO/IEC 27001:2013, es la norma que establece los requisitos para implantar, mantener y mejorar un SGSI. Fue publicada por primera vez en el año 2005, como una norma certificable y es la única norma aceptada a nivel internacional para la gestión de la seguridad de la información. Aunque esta norma tiene sus orígenes en Europa a mediados de los años 90, siendo su evolución la que se presenta en la figura 2.

En El Salvador, a partir de la creación del OSN en el 2011 como el organismo competente para realizar las actividades de Normalización, y con el auge de las tecnologías de información, es necesario aplicar una normativa técnica internacional vigente la cual es la Norma Técnica Salvadoreña ISO/IEC 27001:2013.

En el 2014, la OSN desarrolla un taller de interpretación de la Norma Técnica Salvadoreña ISO/IEC 27001, con el objetivo de dar a conocer los requisitos y alcances de la norma, para el establecimiento y certificación de un sistema de gestión de seguridad de la información.

En el 2015, el OSN realiza un evento de difusión de normas en tecnología de la información, entre las cuales se encuentran la Norma Técnica Salvadoreña ISO/IEC 27001:2013, Norma Técnica Salvadoreña ISO/IEC 27003:2010, Norma Técnica Salvadoreña ISO/IEC 27004:2009 y Norma Técnica Salvadoreña ISO 27006:2011. Esto con el fin de dar a conocer al público en general, las normas técnicas que son aplicables a las tecnologías de información en El Salvador.

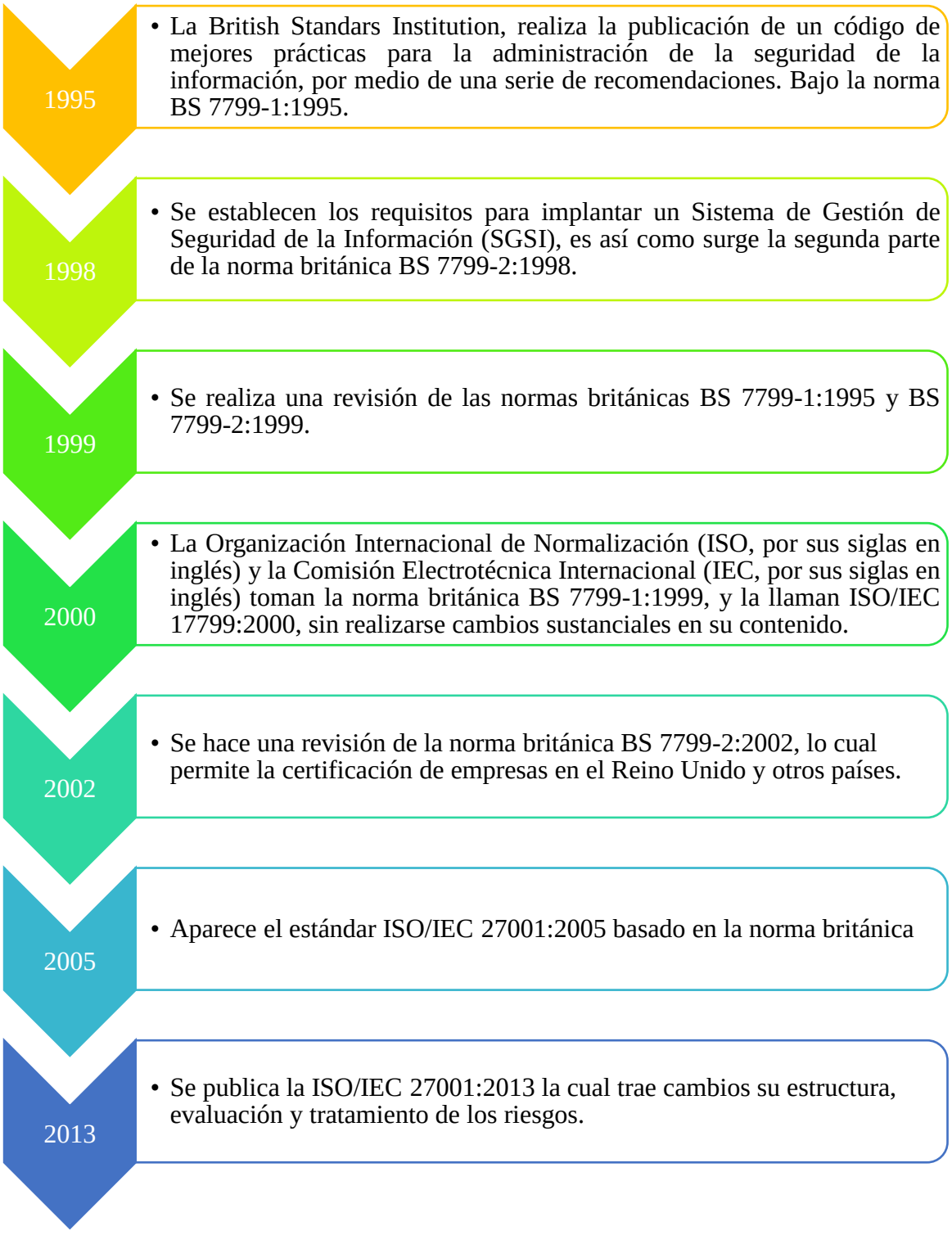


Figura 2 Historia de la NTS ISO/IEC 27001: 2013

Fuente: http://www.pmg-ssi.com/2013/12/iso27001-origen

2.5.2 Descripción de la NTS ISO/IEC 27001:2013

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

Puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma. Se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento.

El eje central es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información por medio de la evaluación de riesgos, y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan mitigando los riesgos. Por lo tanto, la filosofía principal se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

2.5.3 Ventajas en la implementación de La NTS ISO/IEC 27001:2013 en las empresas

Las ventajas comerciales esenciales que una empresa puede obtener con la implementación de la ISO 27001:2013, son las siguientes:

- Cumplir con requerimientos legales: cada vez hay más y más leyes, normativas y requerimientos contractuales relacionados con la seguridad de la información. La mayoría de ellos se pueden resolver implementando ISO 27001, ya que esta norma proporciona una metodología perfecta para cumplir con todos ellos.
- Obtener una ventaja comercial: si la empresa obtiene la certificación y sus competidores no, es posible que obtenga una ventaja sobre ellos ante los ojos de los clientes a los que les interesa mantener en forma segura su información.
- Menores costos: la filosofía principal de ISO 27001 es evitar que se produzcan incidentes de seguridad, y cada incidente, ya sea grande o pequeño, cuesta dinero; por lo tanto, evitándolos la empresa ahorra mucho dinero. La inversión en ISO 27001 es mucho menor que el ahorro que obtendrá.
- Una mejor organización: en general, las empresas de rápido crecimiento no tienen tiempo para hacer una pausa y definir sus procesos y procedimientos; como consecuencia, muchas veces los empleados no saben qué hay que hacer, cuándo y quién debe hacerlo. La implementación de ISO 27001 ayuda a resolver este tipo de situaciones ya que alienta a las empresas a escribir sus principales procesos (incluso los que no están relacionados con la seguridad), lo que les permite reducir el tiempo perdido de sus empleados.
- Garantía de los controles internos y cumplimiento de requisitos de gestión corporativa y de continuidad de la actividad comercial.
- Poner de manifiesto el respeto a las leyes y normativas que sean de aplicación.

- Fiabilidad de cara al cliente, demostrar que la información está segura.
- Identificación, evaluación y gestión de riesgos.
- Evaluaciones periódicas que ayudan a supervisar el rendimiento y las posibles mejoras.
- Se integra con otros sistemas de gestión
- Reducción de costos y mejora de procesos
- Aumento de la motivación y satisfacción del personal al contar con unas directrices claras.

2.6 MARCO TÉCNICO APLICABLE

La Organización Internacional de Normalización (ISO por sus siglas en inglés) como forma de estandarizar soluciones y procedimientos aplicables a las organizaciones, ha creado las normas técnicas internacionales que ayuden a la disminución o control de riesgos informáticos, para lo cual ha establecido lineamientos y guías que permitan el correcto tratamiento, así como incluir todas las áreas críticas de una organización.

2.6.1 Norma Técnica Salvadoreña ISO/IEC 27001:2013 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos

La norma define los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información en el contexto de organización. Los requisitos establecidos son genéricos y pueden ser aplicables a cualquier tipo de organizaciones, sin importar su tipo, tamaño o naturaleza.

El eje principal de la norma es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo realiza indagando cuáles son los problemas que pueden afectar la información por medio de la evaluación de riesgos y la aplicación de controles para mitigar el riesgo.

El OSN, ha adoptado el estándar internacional ISO/IEC 27001:2013 como Norma Técnica Salvadoreña ISO/IEC 27001:2013 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. Para ser aplicado por todas las empresas que deseen certificarse en seguridad de la información. Algunos de los controles que sugiere la norma en su anexo A se describen en la tabla 1:

Tabla 1: controles sugeridos por la Norma Técnica Salvadoreña ISO/IEC 27001:2013

ÁREA	CONTROL
Organización de la seguridad de la información	
Organización interna	
Dispositivos móviles y trabajo remoto	
Política de dispositivos móviles	Una política y medidas de soporte de seguridad deben ser adoptadas para gestionar los riesgos introducidos por el uso de dispositivos móviles.
Trabajo remoto	Una política y medidas de soporte de seguridad deben ser implementadas para proteger la información accedida, procesada o almacenada en sitios de trabajo remoto.
Seguridad de los recursos humanos	
Antes del empleo	
Selección de personal	Los controles de verificación de los antecedentes de todos los candidatos para el empleo deben llevarse a cabo en concordancia con las leyes, regulaciones y normas de ética pertinentes y, deben ser proporcionales al requerimiento del negocio, la clasificación de la información a ser accedida y los riesgos percibidos.
Términos y condiciones de empleo	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las responsabilidades de la organización para la seguridad de la información.
Durante el empleo	
Responsabilidades de la Dirección	La Dirección debe requerir que los empleados y contratistas apliquen la seguridad de la información en concordancia con las políticas y procedimientos establecidos por la organización.
Capacitación, educación y concientización sobre la seguridad de la información	Todos los empleados de la organización y, cuando sea pertinente, los contratistas, deben recibir una apropiada concientización, capacitación y actualización periódica de las políticas y procedimientos organizacionales, que sean relevantes a su función laboral.
Proceso disciplinario	Debe existir un proceso disciplinario formal y comunicado de forma que se tomen acciones en contra de empleados que han cometido una violación en la seguridad de la información.
Terminación y cambio del empleo	
Responsabilidades de terminación o cambio de empleo	Deben ser definidas las responsabilidades y funciones de la seguridad de la información que permanezcan validas después de una terminación o cambio de empleo, comunicadas y remarcadas al empleado o contratista.
Gestión de activos	
Responsabilidad sobre los activos	
Inventario de activos	Activos asociados con información e instalaciones de procesamiento de la información deben ser identificados y un inventario de estos activos debe ser levantado y mantenido.
Propiedad de los activos	Los activos dentro del inventario deben ser asignados.

Uso aceptable de los activos	Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información, los activos asociados y las instalaciones para procesamiento de la información.
Devolución de los activos	Todos los empleados y usuarios externos deben devolver todos los activos de la organización que se encuentran en su posesión una vez dada la terminación de su empleo, contrato o acuerdo.
Clasificación de la información	
Clasificación de la información	La información debe ser clasificada en términos de su valor, requerimientos legales, sensibilidad y criticidad a modificaciones o divulgación no autorizada.
Etiquetado de la información	Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar la información en concordancia con el esquema de clasificación de información adoptado por la organización.
Manejo de activos	Se debe desarrollar e implementar procedimientos para manejo de activos en concordancia con el esquema de clasificación de información adoptado por la organización.
Control de acceso	
Requerimiento del negocio para el control de acceso	
Política del control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requerimientos de seguridad de la información y del negocio.
Acceso a redes y servicios de red	Se debe proveer a los usuarios únicamente con acceso a la red y servicios de red que hayan sido específicamente autorizados.
Gestión del acceso de usuarios	
Registro y anulación de usuarios	Para habilitar la asignación de derechos de acceso se debe implementar un procedimiento formal para la creación y anulación de usuarios.
Provisión de accesos de usuarios	Se debe implementar un proceso formal de provisión de accesos de usuario para asignar o revocar derechos de acceso para todos los tipos de usuario a todos los sistemas y servicios.
Gestión de privilegios de derechos de acceso	Se debe restringir y controlar la asignación y uso de los privilegios de derechos de acceso.
Gestión de la información de autenticación secreta de los usuarios	Se debe controlar a través de un proceso formal de gestión la asignación de información de autenticación secreta.
Revisión de los derechos de acceso	Los dueños de los activos deben revisar periódicamente los derechos de acceso de los usuarios.
Remover o ajustar los derechos de acceso	Se deben remover los derechos de acceso de todos los empleados y usuarios externos a la información e instalaciones de procesamiento de la información una vez dada la terminación de su empleo, contrato o acuerdo, o ser ajustados cuando se dé un cambio.
Responsabilidades del usuario	

Uso de información de autenticación secreta	Se debe requerir a los usuarios seguir las prácticas de la organización en el uso de la información de autenticación secreta.
Control de acceso a sistemas y aplicaciones	
Restricción del acceso a la información	Se debe restringir el acceso a la información y a funcionalidades de los sistemas de aplicación en concordancia con la política de control de acceso.
Procedimientos seguros de inicio de sesión	Cuando sea requerido por la política de control de acceso, se deben controlar por un procedimiento seguro de inicio de sesión el acceso a los sistemas y aplicaciones.
Sistema de gestión de la contraseña	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.
Uso de programas utilitarios privilegiados	Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden estar en capacidad de sobrescribir los controles de aplicaciones y sistema.
Control de acceso al código fuente de los programas	Se debe restringir el acceso al código fuente de los programas.
Criptografía	
Controles criptográficos	
Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y duración de las llaves criptográficas durante todo el ciclo de vida.
Seguridad física y ambiental	
Áreas seguras	
Perímetro de seguridad física	Se deben definir y utilizar perímetros de seguridad para proteger áreas que contienen información, ya sea sensitiva o crítica, e instalaciones de procesamiento de la información.
Controles de entrada físicos	Las áreas seguras deben estar protegidas por controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
Seguridad de oficinas, habitaciones e instalaciones	Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones e instalaciones.
Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
Trabajo en áreas seguras	Se debe diseñar y aplicar procedimientos para trabajar en áreas seguras.
Áreas de carga y descarga	Se deben controlar los puntos de acceso como las áreas de carga y descarga y otros puntos donde personas no autorizadas puedan ingresar a las instalaciones, y cuando fuese posible, se deben aislar de los medios de procesamiento de la información para evitar un acceso no autorizado.

Equipo	
Ubicación y protección del equipo	El equipo debe estar ubicado y protegido para reducir los riesgos de amenazas y peligros ambientales, y de las oportunidades de accesos no autorizados.
Herramientas de soporte	El equipo debe ser protegido contra fallas de energía y otras interrupciones causadas por fallas en las herramientas de soporte.
Seguridad en el cableado	El cableado de la energía y las telecomunicaciones que transportan datos o soportan servicios de información, deben ser protegidos de intercepción, interferencia o daño.
Mantenimiento de equipo	El equipo debe recibir un correcto mantenimiento para asegurar su continuidad, disponibilidad e integridad.
Retiro de activos	El equipo, información o software no debe ser extraído de las instalaciones sin previa autorización.
Seguridad del equipo y activos fuera de las instalaciones	Al trabajar con equipos y activos fuera de las instalaciones de la organización, se deben aplicar medidas de seguridad considerando los riesgos que esto implica.
Seguridad en la reutilización o eliminación de equipos	Todos los elementos del equipo que contengan medios de almacenamiento deberán ser verificados para asegurar que los datos sensibles y el software con licencia hayan sido eliminados o sobrescrito con seguridad antes de su reutilización o eliminación.
Equipo desatendido de usuario	Los usuarios deben asegurarse que el equipo desatendido tiene protección apropiada.
Política de escritorio y pantalla limpia	Se debe adoptar una política de escritorio limpio para documentos y medios de almacenamiento removibles y una política de pantalla limpia en las instalaciones de procesamiento de la información.
Seguridad de las operaciones	
Procedimientos y responsabilidades operacionales	
Procedimientos de operación documentados	Los procedimientos de operación deben documentarse y estar disponibles a todos los usuarios que lo necesiten.
Gestión de cambios	Cambios en la organización, procesos de negocios, instalaciones de procesamiento de la información y sistemas que afecten la seguridad de la información deben ser controlados.
Gestión de la capacidad	El uso de los recursos debe ser monitoreado, optimizado y se deben realizar proyecciones de la capacidad futura necesaria para asegurar el desempeño requerido por el sistema.
Separación de los ambientes de desarrollo, prueba y producción	Los ambientes de desarrollo, prueba y producción, deben estar separados para reducir los riesgos de acceso no autorizado o cambios en el ambiente en producción.
Protección contra software malicioso	
Controles contra software malicioso	Se deben implementar controles de detección, prevención y recuperación para protegerse contra software malicioso, combinándolos con una apropiada concientización del usuario.
Copias de seguridad	

Copia de seguridad de la información	Se debe hacer copias de seguridad de la información, software e imágenes del sistema y probarlas periódicamente de acuerdo a la política de respaldo.
Registro y monitoreo	
Registro de eventos	Se deben producir, mantener y revisar periódicamente registros de los eventos de las actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
Protección de la bitácora de información	Las instalaciones de registro y la bitácora de la información deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.
Bitácoras del administrador y operador	Se deben llevar bitácoras de las actividades del administrador y operador del sistema y éstas deben ser protegidas y revisadas regularmente.
Sincronización de reloj	Los relojes de los sistemas de procesamiento de información relevantes de una organización o dominio de seguridad deben estar sincronizados con una única fuente de tiempo de referencia.
Control de software operacional	
Instalación de software en sistemas operacionales	Se deben implementar procedimientos para controlar la instalación de software en sistemas operacionales.
Seguridad de las comunicaciones	
Gestión de seguridad de red	
Controles de red	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
Seguridad de los servicios de red	Mecanismos de seguridad, niveles de servicio y requisitos de la gestión de todos los servicios de red, deben ser identificados e incluidos en cualquier acuerdo de servicios de red, ya sea si estos servicios son provistos por la misma organización o se subcontratan.
Segmentación de redes	Se deben segmentar en redes los grupos de servicios de información, usuarios y sistemas de información.
Transferencia de información	
Procedimientos y políticas de transferencia de información	Se deben establecer políticas, procedimientos y controles formales para proteger la transferencia de información a través de todos los tipos de recursos de comunicación.
Acuerdos de transferencia de información	Los acuerdos deben abordar la seguridad de la transferencia de información del negocio entre la organización y entidades externas.
Mensajes electrónicos	Se debe proteger adecuadamente la información contenida en los mensajes electrónicos.
Acuerdos de confidencialidad o no divulgación	Se deben identificar, revisar periódicamente y documentar los requerimientos para acuerdos de confidencialidad o no divulgación, reflejando las necesidades de la organización para la protección de la información.
Gestión de incidentes de seguridad de la información	

Gestión de incidentes de seguridad de la información y mejoras	
Informar sobre los eventos de seguridad de la información.	Se debe requerir que los empleados y contratistas que utilizan los sistemas y servicios de información de la organización tomen nota e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios de la organización.
Informar sobre las debilidades de seguridad de la información.	Se debe evaluar los eventos de seguridad de la información y decidir si éstos se clasificarán como incidentes de seguridad de la información.
Respuesta a incidentes de seguridad de la información.	Se debe responder a los eventos de seguridad de la información en concordancia con los procedimientos documentados. (NTS ISO/IEC 27001, 2013)

Fuente: *Norma Técnica Salvadoreña ISO/IEC 27001:2013*

2.6.2 COBIT 5 Procesos catalizadores

Este modelo de gestión de seguridad propone dos procesos catalizadores, que al aplicarlos de manera adecuada contribuyen con la seguridad informática de las empresas. En la tabla 2 se describe el contenido de dichos procesos.

Tabla 2: procesos catalizadores relacionados a la seguridad informática.

PROCESO	DESCRIPCIÓN	PRÁCTICAS CLAVES DEL PROCESO
DSS05 Gestionar Servicios de Seguridad	Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.	**DSS05.01** Proteger contra software malicioso. **DSS05.02** Gestionar la seguridad de la red y las conexiones. **DSS05.03** Gestionar la seguridad de los puestos de usuario final. **DSS05.04** Gestionar la identidad del usuario y el acceso lógico. **DSS05.05** Gestionar el acceso físico a los activos de TI.

		DSS05.06 Gestionar documentos sensibles y dispositivos de salida. **DSS05.07** Supervisar la infraestructura para detectar eventos relacionados con la seguridad
APO13 Gestionar la seguridad **(ISACA, 2012)**	Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.	**APO13.01** Establecer y mantener un SGSI. **APO13.02** Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información. **APO13.03** Supervisar y revisar el SGSI.

Fuente: *COBIT 5 Procesos catalizadores*

2.7 LEGISLACIÓN APLICABLE

La seguridad informática posee un marco legal que la regula, permitiendo desarrollar y aplicar lineamientos para el resguardo de la información que se genera dentro de las organizaciones. En la tabla 3, se muestran las leyes y artículos que se relacionan con la seguridad informática.

Tabla 3: legislación aplicable a la seguridad informática

LEY APLICABLE	ARTÍCULO	DESCRIPCIÓN
Ley especial contra los delitos informáticos y conexos.	Art. 1 Objeto de la ley.	La ley en su contenido posee como objeto proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación, así como la prevención y sanción de los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, intimidad e imagen de las personas naturales o jurídicas en los términos aplicables y previstos en la presente Ley.
	Art. 8 Posesión de equipos o prestación de servicios para la vulneración de la seguridad.	La ley establece prisión para la posesión de equipos prestación de servicios para la vulneración de la seguridad. El que utilizando las Tecnologías de la Información y la Comunicación posea, produzca, facilite, venda equipos, dispositivos, programas informáticos, contraseñas o códigos de acceso; con el propósito de vulnerar, eliminar ilegítimamente la seguridad de cualquier sistema informático, ofrezca o preste servicios destinados a cumplir los mismos fines para cometer cualquiera de los delitos establecidos en la presente Ley, será sancionado con prisión de tres a cinco años.
	Art. 9 Violación de la seguridad del sistema.	La persona que sin poseer la autorización correspondiente transgreda la seguridad de un sistema informático restringido o protegido con mecanismo de seguridad específico, será sancionada con prisión de tres a seis años. En igual sanción incurrirá quien induzca a un tercero para que de forma involuntaria, ejecute un programa, mensaje, instrucciones o secuencias para violar medidas de seguridad. No incurrirá en sanción alguna quien ejecute las conductas descritas en los Arts. 8 y 9 inciso primero de la presente Ley, cuando con autorización de la persona facultada se realicen acciones con el objeto de conducir pruebas técnicas o auditorías de funcionamiento de equipos, procesos o programas.
	Art. 10 Estafa informática.	El que manipule o influya en el ingreso, el procesamiento o resultado de los datos de un sistema que utilice las Tecnologías de la Información y la Comunicación, ya sea mediante el uso

		de datos falsos o incompletos, el uso indebido de datos o programación, valiéndose de alguna operación informática o artificio tecnológico o por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial indebido para sí o para otro, será sancionado con prisión de dos a cinco años. Se sancionará con prisión de cinco a ocho años, si las conductas descritas en el inciso anterior se cometieren bajo los siguientes presupuestos: a) En perjuicio de propiedades del Estado; b) Contra sistemas bancarios y entidades financieras; y, c) Cuando el autor sea un empleado encargado de administrar, dar soporte al sistema, red informática, telemática o que en razón de sus funciones tenga acceso a dicho sistema, red, contenedores electrónicos, ópticos o magnéticos.
	Art. 11 Fraude informático.	El que por medio del uso indebido de las Tecnologías de la Información y la Comunicación, valiéndose de cualquier manipulación en sistemas informáticos o cualquiera de sus componentes, datos informáticos o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho para sí o para un tercero en perjuicio ajeno, será sancionado con prisión de tres a seis años.
	Art. 12 Espionaje informático.	El que con fines indebidos obtenga datos, información reservada o confidencial contenidas en un sistema que utilice las Tecnologías de la Información y la Comunicación o en cualquiera de sus componentes, será sancionado con prisión de cinco a ocho años. Si alguna de las conductas descritas en el inciso anterior se cometieren con el fin de obtener beneficio para sí o para otro, se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas, resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de la información de carácter reservada, confidencial o sujeta a secreto bancario, la sanción será de seis a diez años de prisión.
	Art. 13 Hurto por medios informáticos.	El que, por medio del uso de las Tecnologías de la Información y la Comunicación, se apodere de bienes o valores tangibles o intangibles de carácter personal o patrimonial, sustrayéndolos

		a su propietario, tenedor o poseedor, con el fin de obtener un provecho económico para sí o para otro, será sancionado con prisión de dos a cinco años.
	Art. 15 Manipulación de registros.	Los Administradores de las Plataformas Tecnológicas de instituciones públicas o privadas, que deshabiliten, alteren, oculten, destruyan, o inutilicen en todo o en parte cualquier información, dato contenido en un registro de acceso, uso de los componentes de éstos, será sancionada con prisión de cinco a ocho años. Si las conductas descritas en el inciso anterior, favorecieren la comisión de otro delito, la sanción se agravará hasta en una tercera parte del máximo señalado.
	Art. 19 Alteración, daño a la integridad y disponibilidad de los datos.	El que violando la seguridad de un sistema informático destruya, altere, duplique, inutilice o dañe la información, datos o procesos, en cuanto a su integridad, disponibilidad y confidencialidad en cualquiera de sus estados de ingreso, procesamiento, transmisión o almacenamiento, será sancionado con prisión de tres a seis años.
	Art. 20 Interferencia de datos.	El que interfiera, obstruya o interrumpa el uso legítimo de datos o los produzca nocivos e ineficaces, para alterar o destruir los datos de un tercero, será sancionado con prisión de tres a seis años. Si alguna de las conductas descritas en el inciso anterior recae sobre datos, documentos, programas o sistemas informáticos públicos o sobre datos destinados a la prestación de servicios de salud, de comunicaciones, sistemas bancarios, entidades financieras, de provisión y transporte de energía, de medios de transporte u otro servicio público, la sanción de prisión será de cinco a ocho años.
	Art. 23 Divulgación no autorizada.	El que sin autorización da a conocer un código, contraseña de acceso o cualquier otro medio de acceder a un programa o datos almacenados en un equipo o dispositivo tecnológico, con el fin de lucrarse así mismo, a un tercero o para cometer un delito, será sancionado con prisión de cinco a ocho años. Igual sanción tendrá el que sin autorización revele o difunda los datos o información, contenidos en un sistema informático que utilice las Tecnologías de la Información y la Comunicación o en cualquiera de sus componentes, con el fin de obtener algún tipo de beneficio para sí o para otro.

		Si alguna de las conductas descritas en los incisos anteriores pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas, como consecuencia de la revelación de las informaciones de carácter reservado, será sancionado con prisión de seis a doce años.
	Art. 25 Obtención y transferencia de información de carácter confidencial.	El que deliberadamente obtenga y transfiera información de carácter confidencial y que mediante el uso de esa información vulnere un sistema o datos informáticos apoyándose en cualquier clase de las Tecnologías de la Información y la Comunicación, incluidas las emisiones electromagnéticas, será sancionado con prisión de cinco a ocho años. (Asamblea Legislativa de El Salvador, 2016)
Ley de propiedad intelectual.	Art. 1 objeto de la ley.	Las disposiciones contenidas en la presente ley tienen por objeto asegurar una protección suficiente y efectiva de la propiedad intelectual, estableciendo las bases que la promuevan, fomenten y protejan.
	Art. 32 programas informáticos.	Programa de ordenador, ya sea programa fuente o programa objeto, es la obra literaria constituida por un conjunto de instrucciones expresadas mediante palabras, códigos, planes o en cualquier otra forma que, al ser incorporadas en un dispositivo de lectura automatizada, es capaz de hacer que un ordenador, o sea, un aparato electrónico o similar capaz de elaborar informaciones, ejecute determinada tarea u obtenga determinado resultado. Se presume que es productor del programa de ordenador, la persona que aparezca indicada como tal en la obra de la manera acostumbrada, salvo prueba en contrario.
	Art. 33 contrato de programas informáticos.	El contrato entre los autores del programa de ordenador y el productor, implica la cesión ilimitada y exclusiva a favor de éste de los derechos patrimoniales reconocidos en la presente ley, así como la autorización para decidir sobre su divulgación y la de ejercer los derechos morales sobre la obra, en la medida que ello sea necesario para la explotación de la misma, salvo pacto en contrario. (Asamblea Legislativa de El Salvador , 1993)

Fuente: *Ley especial contra los delitos informáticos y conexos; ley de propiedad intelectual.*

CAPÍTULO III-METODOLOGÍA DE LA INVESTIGACIÓN

3.1 ENFOQUE Y TIPO DE INVESTIGACIÓN

El enfoque bajo el cual se realizó la investigación es el cuantitativo, ya que permitió la recolección de datos utilizando el instrumento del cuestionario para poder medir las variables de investigación, y realizar un análisis estadístico de los resultados obtenidos para poder inferir sí todos los elementos de la población cumplen con la hipótesis formulada, y dar así una solución a la problemática identificada.

La investigación se basó en un estudio de tipo hipotético-deductivo partiendo del conocimiento general del problema al conocimiento específico, debido a que se observó el problema en estudio, por medio de esto se presentó un diagnóstico de la situación problemática y por último se elaboró una propuesta de solución.

3.2 DELIMITACIÓN ESPACIAL Y TEMPORAL

3.2.1 Espacial

El estudio se realizó en 20 empresas del sector de logística y transporte de carga ubicadas en el municipio de Antiguo Cuscatlán, departamento de La Libertad, las cuales fueron seleccionadas por la importancia que poseen cada una de ellas en el sector objeto de estudio, el tamaño de sus operaciones fue otra de las características por las cuales se seleccionaron las empresas ubicadas en dicho municipio, aparte de que es este municipio donde existe la mayor actividad comercial del sector.

3.2.2 Temporal

Para efectos de la investigación se consideró como objeto de estudio toda la información de las empresas del sector desde el año 2014 al año 2016, ya que tres años de información se consideran suficientes para realizar un análisis exhaustivo de la problemática de la seguridad

informática de las empresas, y para determinar los riesgos a los cuales están expuestas al no aplicar políticas de seguridad informática adecuadas; además , que en este período fue donde incrementó la actividad económica de las empresas del sector de logística y transporte de carga ya que existen más representaciones de empresas.

3.3 SUJETOS Y OBJETO DE ESTUDIO

3.3.1 Unidades de análisis

Las unidades de análisis que se consideraron en el estudio son los jefes o encargados del área de sistemas informáticos y alternativamente también la gerencia general de las empresas del sector de logística y transporte de carga del municipio de Antiguo Cuscatlán, La Libertad, ya que ambos poseen una injerencia importante en la implementación de políticas de seguridad informática, las cuales se proponen para su aplicación.

3.3.2 Población y marco muestral

A) Población

La población que se tomó como objeto de estudio para esta investigación se encuentra conformada por un total de 20 empresas del sector de logística y transporte de carga, legalmente constituidas y registradas en el municipio de Antiguo Cuscatlán, según listado obtenido de la Dirección General de Aduanas (DGA), el cual fue confirmado por el equipo de investigación para verificar la existencia de dichas empresas y su ubicación geográfica. ***(ver anexo 1)***

B) Muestra

No existe muestra, dado que la población es menor a 30 elementos.

3.3.3 Variables e indicadores

Las variables e indicadores relacionados con la problemática en las empresas del sector de logística y transporte de carga, son las siguientes:

Tabla 4: variables e indicadores

Variables	Indicadores
Independiente: Políticas de seguridad informática.	▪ Controles de seguridad en las redes. ▪ Gestión adecuada de activos informáticos. ▪ Control de acceso a las instalaciones de las empresas. ▪ Seguridad física y ambiental. ▪ Seguridad en las operaciones. ▪ Seguridad en las comunicaciones. ▪ Seguridad lógica. ▪ Gestión de incidentes de seguridad de la información. ▪ Robos de información. ▪ Acceso a la información.
Dependiente: Minimizar los riesgos en los sistemas de información.	

Fuente: *resultado de la investigación en las empresas del sector en estudio.*

3.4 TÉCNICAS, MATERIALES E INSTRUMENTOS

3.4.1 Técnicas para la recolección de la información

Las técnicas utilizadas para la recolección de información fueron las siguientes:

- Entrevista, realizada al Gerente General del grupo empresarial Comca Internacional, una de las empresas con gran trayectoria en este sector para conocer más de cerca la problemática en estudio, desde una perspectiva más amplia ***(ver anexo 9).***
- Encuesta, se realizaron una serie de preguntas a los jefes de informática de las empresas con la finalidad de recoger información en cuanto al tema en estudio.

3.4.2 Instrumentos de medición

El instrumento que se utilizó para la recopilación de información fue el cuestionario que se presentó a las unidades de análisis para que sea completado, dicho cuestionario está elaborado

por diversas preguntas, esto con el fin de determinar los riesgos de inseguridad en el sistema de información que poseen las empresas objeto de estudio, de esta manera se obtuvo otra perspectiva sobre la problemática para la creación de la propuesta que consiste en políticas de seguridad informática ***(ver anexo 2).***

3.5 PROCESAMIENTO Y ANÁLISIS DE LA INFORMACIÓN

Para el procesamiento y análisis de la información se eligió el software en línea SurveyMonkey, la razón, como se trata de tecnologías de la información, que mejor opción para realizar encuestas de una forma innovadora y segura como esta. Dicha aplicación permite diseñar de forma personalizada encuestas y enviarlas a través de correos electrónicos, enlaces en páginas web propias o por medio de las redes sociales.

SurveyMonkey consta de 3 módulos básicos que se detallan a continuación: diseñar, recopilar y analizar. En el módulo de diseñar se ingresó la encuesta con las opciones de respuesta establecidas previamente, se realizó de forma personalizada para que fuera atractiva al encuestado. En el módulo de recopilar se definió que la mejor forma de recolectar los datos de la encuesta sería por medio de correo electrónico, además de gestionar el proceso de envío y control de porcentaje de respuesta de los encuestados, en el mismo modulo se enviaron recordatorios a los encuestados que no habían respondido aun la encuesta o que la habían respondido de forma parcial en el tiempo estipulado para contestarla, finalmente se enviaron agradecimientos por la colaboración al llenar la encuesta a través de su email. Por último, el módulo de analizar permitió observar los resultados de cada encuestado, y generar un resumen automático de la encuesta llenada por las unidades de análisis con tablas y gráficos estándar propios de la aplicación.

Los resultados de las encuestas generados por la aplicación fueron exportados a un archivo de Microsoft Excel y Adobe Reader, para realizar un mejor análisis de los resultados. Los gráficos

de la información recopilada en la encuesta se diseñaron en los programas Microsoft Power Point y Adobe Photoshop (infografía), ***(ver anexo 3)***.

Para mayor comprensión de los mismos y para el cruce de variables se utilizó el software de análisis estadístico International Business Machines (IBM) Statistical Package for the Social Sciences (SPSS) versión 24.

3.6 CRONOGRAMA DE ACTIVIDADES

ACTIVIDAD	AÑO 2017																															
	MARZO				ABRIL				MAYO				JUNIO				JULIO				AGOSTO				SEPTIEMBRE				OCTUBRE			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
CAPÍTULO I PLANTEAMIENTO DEL PROBLEMA																																
Situación problemática																																
Enunciado del problema																																
Justificación de la investigación																																
Objetivos de la investigación																																
Hipótesis																																
Limitaciones																																
CAPÍTULO II MARCO TEÓRICO																																
Estado actual de la seguridad informática en las empresas en estudio																																
Antecedentes																																
Importancia de aplicar políticas de seguridad informática en las empresas																																
Principales definiciones																																
Legislación aplicable																																
Normativa técnica aplicable a la seguridad informática																																
CAPÍTULO III METODOLOGÍA DE LA INVESTIGACIÓN																																
Enfoque y tipo de investigación																																
Delimitación espacial y temporal																																
Sujetos y objeto de estudio																																
Técnicas, materiales e instrumentos																																
Procesamiento y análisis de la información																																
Cronograma de actividades																																
Presentación de resultados																																
CAPÍTULO IV PROPUESTA CASO PRÁCTICO																																
Planteamiento del caso																																
Estructura del plan de solución																																
Beneficios y limitantes																																
Desarrollo de caso práctico																																
CONCLUSIONES Y RECOMENDACIONES																																
Conclusiones																																
Recomendaciones																																
DEFENSA DEL TRABAJO DE GRADUACIÓN																																

3.7 PRESENTACIÓN DE RESULTADOS

3.7.1 Tabulación y análisis de los resultados

Tabla 5: cruce preguntas 4 y 3

PREGUNTAS		3. ¿Cuáles de los siguientes controles aplica la empresa a los empleados que trabajan de forma remota y fuera de las instalaciones de la empresa?								Total
		A. Validación de datos.	B. Software antivirus en las unidades externas.	C. Accesos restringidos desde IP externa.	D. Asignación de ID únicos para establecer responsabilidades.	E.Monitoreo de la información que se genera.	F. Bloqueo de impresión de documentos y/o almacenamiento en unidades externas.	G. No aplicamos ninguna.	H. No se permite el trabajo de forma remota	
4. Cuando se contrata a un nuevo empleado; ¿se incluye una cláusula de confidencialidad en su contrato para garantizar la seguridad de la información?	SI	11	11	10	6	3	5	0	1	**16**
		55.0%	55.0%	50.0%	30.0%	15.0%	25.0%	0.0%	5.0%	**80.0%**
	NO	1	2	0	1	0	0	0	2	**4**
		5.0%	10.0%	0.0%	5.0%	0.0%	0.0%	0.0%	10.0%	**20.0%**
Total		**12**	**13**	**10**	**7**	**3**	**5**	**0**	**3**	**20**
		60.0%	**65.0%**	**50.0%**	**35.0%**	**15.0%**	**25.0%**	**0.0%**	**15.0%**	**100.0%**

Fuente: *resultado de encuesta realizada a las unidades de análisis.*

Análisis: Las empresas del sector toman como medida para garantizar la seguridad de la información una cláusula de confidencialidad en los contratos de trabajo, sin embargo, no se monitorea la información que se genera de forma remota y los bloqueos de impresión y almacenaje de información está permitida en la mayoría de casos**.**

Tabla 6: cruce de preguntas 5 y 14

PREGUNTAS		14. ¿Cuáles de las siguientes características utiliza la empresa para autentificar las contraseñas de usuario?					Total
		A. Asignación de ID únicos para establecer responsabilidades.	B. Técnicas de cifrado.	C. Bloqueo de accesos por intentos fallidos.	D. Cambio de contraseña cada determinado periodo.	E. No se utiliza ninguna.	
5. De las siguientes medidas de seguridad; ¿Cuáles aplica la empresa para el uso adecuado de los activos informáticos?	A. Los empleados devuelven los activos informáticos al finalizar su contrato de trabajo.	10	3	5	9	2	16
		50.0%	15.0%	25.0%	45.0%	10.0%	80.0%
	B. Se asignan activos informáticos de acuerdo a las funciones de cada empleado.	9	3	5	8	2	14
		45.0%	15.0%	25.0%	40.0%	10.0%	70.0%
	C. No se permite a los empleados el uso de dispositivos de almacenamiento móviles.	6	1	4	6	0	6
		30.0%	5.0%	20.0%	30.0%	0.0%	30.0%
	D. Asigna claves de acceso único para fotocopia, impresión y escaneo.	9	2	5	6	1	11
		45.0%	10.0%	25.0%	30.0%	5.0%	55.0%
	E. No aplica ninguna.	9	2	5	6	1	11
		45.0%	10.0%	25.0%	30.0%	5.0%	55.0%
Total		14	4	8	12	2	20
		70.0%	20.0%	40.0%	60.0%	10.0%	100.0%

Fuente: *resultado de encuesta realizada a las unidades de análisis.*

Análisis: De las medidas de seguridad para el uso adecuado de activos, prevalece la asignación de claves de acceso únicos y no permitir el uso de dispositivos de almacenamientos móviles, pero a su vez se ha comprobado que las técnicas de cifrado son poco utilizadas, así como el bloqueo de accesos por intentos fallidos.

Tabla 7: cruce de preguntas 10 y 11

PREGUNTAS		11. Si realiza copias de seguridad de seguridad de la información ¿Cuál es la frecuencia con la cual lo realiza?					Total
		Diario	Semanal	Mensual	Trimestral	Anual	
10. ¿Realiza copias de seguridad de toda la información sensible de la empresa?	SI	6	7	10	1	1	19
		31.6%	36.8%	52.6%	5.3%	5.3%	95.0%
	NO						1
							5.0%
Total		6	7	10	1	1	20
		31.6%	36.8%	52.6%	5.3%	5.3%	100.0%

Fuente: *resultado de encuesta realizada a las unidades de análisis.*

Análisis: A pesar de contar con copias de seguridad de la información, estas son realizadas en su mayoría mensualmente, es importante determinar la necesidad de elaborar copias con mayor frecuencia.

Tabla 8: cruce de preguntas 18 y 13

PREGUNTAS		13. ¿Cuáles de las siguientes medidas aplican en la empresa para garantizar la seguridad de la información generada por los sistemas?								Total
		A. Autentificación de usuarios (Contraseñas).	B. Control de acceso a los datos.	C. Encriptación de datos sensibles o confidenciales.	D. Socialización a los usuarios de normas o políticas de seguridad Informática.	E. Actualización de Software.	F. Validación de datos.	G. Software antivirus.	H. No aplicamos ninguna medida.	
18. ¿Considera que la aplicación de políticas de seguridad informática le ayudaría a la empresa a proteger la información y generar credibilidad y confianza ante terceros?	SI	19	11	2	5	15	5	19	0	**20**
		95.0%	55.0%	10.0%	25.0%	75.0%	25.0%	95.0%	0.0%	**100.0%**
	NO									
Total		**19**	**11**	**2**	**5**	**15**	**5**	**19**	**0**	**20**
		95.0%	**55.0%**	**10.0%**	**25.0%**	**75.0%**	**25.0%**	**95.0%**	**0.0%**	**100.0%**

Fuente: *resultado de encuesta realizada a las unidades de análisis.*

Análisis: Se ha podido determinar que las empresas del sector ya aplican algunas medidas o buenas prácticas para garantizar la seguridad de la información, pero a su vez estas empresas consideran que la aplicación de políticas de seguridad informática les ayudaría a generar credibilidad y confianza ante terceros, esto se puede entender debido a que estas políticas estarán sustentadas en normas de estándar internacional con éxito a nivel mundial.

Tabla 9: cruce de preguntas 12 y 16

PREGUNTAS		16. De los ataques informáticos sufridos por la empresa ¿Cuáles fueron las causantes del ataque?									Total
		A. Ataques de hackers.	B. Uso inadecuado de internet.	C. Modificación de mensajes.	D. Acceso no autorizado (áreas físicas).	E. Correo spoofing (remitentes falsos).	F. Virus informáticos.	G. Ataque interno de empleados.	H. Puertos USB abiertos.	I. Utilización de claves y usuarios de otros empleados.	
12. ¿La empresa cuenta con un software antivirus para la detección y prevención de los ataques de software maliciosos?	SI	0	2	1	0	4	3	0	0	0	5
		0.0%	40.0%	20.0%	0.0%	80.0%	60.0%	0.0%	0.0%	0.0%	100.0%
Total		0	2	1	0	4	3	0	0	0	5
		0.0%	40.0%	20.0%	0.0%	80.0%	60.0%	0.0%	0.0%	0.0%	100.0%

Fuente: *resultado de encuesta realizada a las unidades de análisis.*

Análisis: Al indagar si las empresas del sector cuentan con un software antivirus para la prevención de ataques de software maliciosos, se comprobó que el 100% de ellas cuentan con esta protección, pero 7 de los ataques informáticos sufridos fue producto de virus informáticos y correo spoofing, lo que demuestra que la protección con los antivirus actuales no es bien administrada o la herramienta no es la mejor.

Tabla 10: cruce de preguntas 15 y 19

PREGUNTAS		19. ¿Cree que la empresa estaría interesada en aplicar políticas de seguridad informática basadas en la Norma Técnica Salvadoreña ISO/IEC 27001:2013?		Total
		SI	NO	
15. ¿Ha sufrido la empresa ataques informáticos los últimos 3 años?	SI	5	0	5
		25.0%	0.0%	25.0%
	NO	13	2	15
		65.0%	10.0%	75.0%
Total		18	2	20
		90.0%	10.0%	100.0%

Fuente: *resultado de encuesta realizada a las unidades de análisis.*

Análisis: Las empresas que han sufrido ataques informáticos en los últimos años han sido pocas, sin embargo, la mayoría de las empresas estarían interesadas en aplicar políticas de seguridad informática en su empresa, esto con el objetivo de prevenir cualquier ataque o corregirlo en el caso de las que ya han sufrido uno.

3.7.2 Diagnóstico

Las empresas del sector de logística y transporte de carga que brindaron información a través del cuestionario (100%) consideran que la aplicación de políticas de seguridad informática les ayudaría a minimizar los riesgos en los sistemas de información, el 90% confirman que las políticas de seguridad informática basadas en la Norma Técnica Salvadoreña ISO/IEC 27001:2013 serían aplicadas en sus empresas, lo anterior producto a diferentes debilidades y necesidades que se han podido detectar tales como la permisibilidad de conexión a sus redes por parte de colegas, clientes, proveedores que necesitan hacer uso de las redes internas de las empresas en el momento de una conferencia, reunión de negocios o eventos como cocteles o lanzamientos de nuevos servicios en la región.

Las empresas del sector confirmaron que permiten el acceso a sus redes y con esto generar confianza y buen servicio a sus clientes y proveedores que les visitan así como a los agentes y empresas multinacionales que representan, para ello la aplicación de medidas de seguridad para contribuir a disminuir los riesgos son básicas ya que se pudo detectar que los cifrados de información en tránsito es mínima , es decir, no se protege la información que ven, generan y sustraen de los sistemas y redes de las empresas, no se realizan muy constante pruebas de intrusión para determinar la adecuación de la protección de la red y con esto identificar accesos específicos de usuarios externos, con dispositivos móviles a los cuales previamente se les ha asignado una clave y confirmar que son ellos los usuarios que están utilizando realmente la red y no que alguien más posee la clave.

El 85% de las empresas permite el acceso remoto de sus empleados a las redes (correos electrónicos, documentos compartidos, sistemas informáticos) con el objetivo de permitir avanzar con los trabajos y brindar servicios a los clientes que manejan carga de otros continentes y la

coordinación es necesaria con esos países que tienen horarios diferenciados, adicional en fechas festivas donde la oficina permanece cerrada pero los servicios continúan en tránsito y es importante brindar status de los embarques, ante esto no existe un monitoreo exhaustivo de la información que se utiliza ni que se genera de forma remota, el bloqueo de impresión así como almacenamiento de información es bajo y esto representa un riesgo de fuga de información o de perdida de la misma.

Las empresas que no permiten el uso de unidades de almacenamiento móviles (memorias flash, discos duros portátiles, memorias SD, teléfonos celulares) también es bajo, y esto significa que existe el riesgo de sustracción de información de los sistemas y de los registros, y utilizarlas para diferentes fines tanto personales como laborales en otras áreas, es por ello que la necesidad de políticas que les permitan a las empresas del sector minimizar este riesgo son necesarias e imprescindibles.

La seguridad lógica y física son otros de los aspectos que pocas veces son contemplados para la protección de los activos de las empresas del sector por ejemplo solo el 20% de las empresas aplica bloqueos a usuarios por intentos fallidos, es decir si el usuario ha olvidado su clave y la digita mal no hay bloqueo de usuario, que pasaría si otro usuario está utilizando el código y clave para accesar a módulos de los sistemas que no tiene autorización, no habría forma de percatarse ni de alertar al usuario que alguien más utiliza su clave de acceso ni al departamento de tecnología que alguien está intentando infiltrarse al sistema con usuarios que no corresponden.

Algunas empresas no aplican ningún método de seguridad para el acceso a sus instalaciones, esto representa un riesgo que cualquier persona puede entrar y salir de las instalaciones con algún objeto sin ser revisado ni detenido; mas sin embargo algunas aplican normas que su empresa representada (empresa internacional que necesita de los servicios de una

empresa local para culminar la cadena logística y por ello le retribuye una comisión o un monto especifico de dinero por el servicio).

Un porcentaje considerable de las empresas del sector han mencionado haber sido víctimas de ataques informáticos debido a diferentes factores entre ellos: correos spoofing y virus informáticos, la falta de políticas que les alerte a los empleados respecto a cómo actuar al recibir un correo sospechoso y no accesar a los links, y sobre todo ingresar información solicitada es una de las principales causas para lo cual la propuesta de políticas de seguridad informática ayudara a disminuir en gran medida esta causa de riesgo, respecto a los software antivirus estos al ser en su mayoría gratuitos no poseen las herramientas completas para brindar una protección de alto nivel y tomando en cuenta que esta es una de las principales herramientas para controlar los accesos de forma remota, así como una de las principales medidas de seguridad para la información generada por los sistemas, es decir mucha de las medidas actuales de seguridad están basadas en software gratuito.

Las repercusiones o consecuencias generadas por estos ataques van en contra de la continuidad del negocio de las empresas del sector, dado que genera atrasos en las operaciones del negocio y fuga de información de base de datos de clientes, vendedores que usualmente se retiran de la empresa y dejan de laborar e inician a trabajar en otra empresa similar (competencia), en donde tratan de retomar su cartera de clientes, debido a que esto es una práctica usual las empresas del sector deberían incluir en los contratos laborales de los empleados cláusulas de confidencialidad, para tratar de disminuir esta práctica; pérdida de credibilidad ante terceros es otra de las consecuencias, lo cual afecta la imagen de la empresa, el servicio de calidad como tal y posibles nuevos negocios que no podrá concretar.

Los sistemas de información son una herramienta fundamental para el desarrollo y desempeño de las empresas del sector y esto es comprobado aún más cuando el estar informando a los clientes de sus embarques es una actividad principal, además cuando es necesario coordinar embarques y enviar documentos escaneados que son resguardados en los sistemas, como archivos adjuntos y se ha comprobado que las medidas para garantizar toda esta información es básica ya que solo utilizan una autentificación de usuarios, software antivirus y actualización de software, dejando en última instancia normas importantes como la validación de datos para verificar que es el usuario correcto desde la IP correcta.

Dado que algunas de las empresas del sector de logística y transporte de carga aplican buenas prácticas impuestas por las empresas multinacionales que representan, y estas no están sustentadas en normas técnicas de estándares internacionales como lo es la Norma Técnica Salvadoreña ISO/IEC 27001:2013 ni en algunas buenas prácticas de bibliografías especializadas en el tema, sino más bien en lo que consideran prudente o necesario para controlar los riesgos, así como acciones correctivas por situaciones que han vivido y que repercute en consecuencias para las empresas; es importante el uso e implementación de políticas de seguridad informática basadas en la Norma Técnica Salvadoreña ISO/IEC 27001:2013 que les permita minimizar los riesgos en los sistemas de información, y con ello solventar la problemática planteada dado que se constató que actualmente tiene muchas áreas en las que necesitan mejorar la seguridad y vulnerabilidad que poseen.

CAPÍTULO IV-POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EMPRESAS DEL SECTOR DE LOGÍSTICA Y TRANSPORTE DE CARGA

4.1 PLANTEAMIENTO DEL CASO

La propuesta de solución de políticas de seguridad informática para empresas del sector de logística y transporte de carga del municipio de Antiguo Cuscatlán, se realizó con el objetivo de sugerir una herramienta útil que ayude a garantizar la seguridad informática dentro de las organizaciones, desde la dirección ejecutiva hasta los niveles operativos, se trabajó con referencia al anexo A de la Norma Técnica Salvadoreña ISO/IEC 27001:2013, esta es una guía que permite establecer, implementar, operar, revisar, mantener y mejorar la gestión de la seguridad de la información dentro de las empresas que lo deseen.

Esta herramienta detalla las políticas de seguridad informática y la forma como deben implementarse para dar cumplimiento a los controles establecidos en la Norma antes mencionada, que se refiere a los requisitos que debe contener un Sistema de Gestión de Seguridad de la información (SGSI). Las empresas deben comprometerse a dar a conocer a todos sus miembros lo establecido en las políticas, con el propósito de cuidar y garantizar las buenas prácticas para la protección de los sistemas de información.

4.2 ESTRUCTURA DEL PLAN DE SOLUCIÓN

La estructura de solución se muestra en la figura 3, la cual fue diseñada tomando como base la estructura del Anexo A de la norma antes mencionada. Cada uno de los grupos de políticas descritos en la figura 3, fue incluido para garantizar la seguridad informática en las distintas áreas de la empresa.

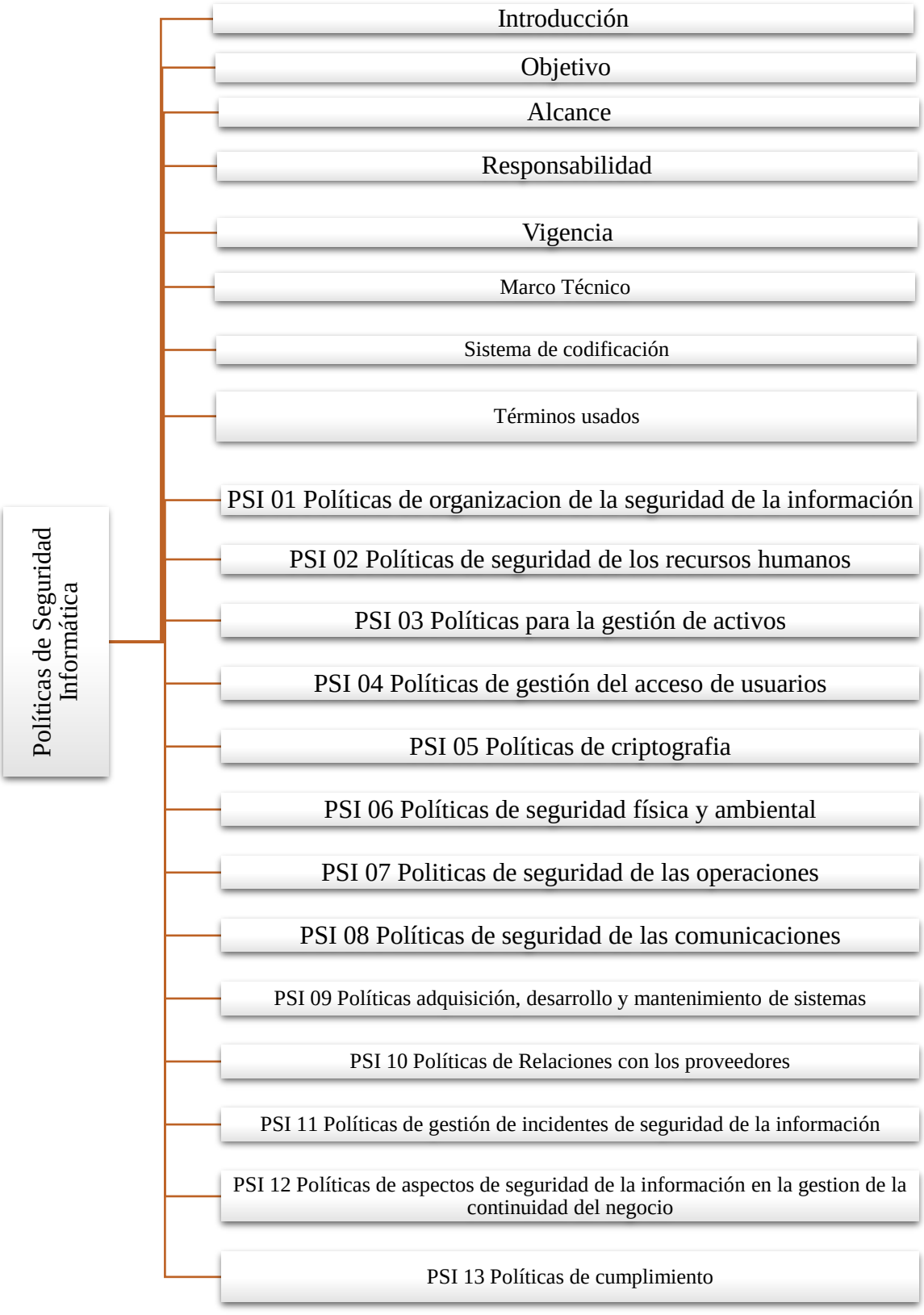


Figura 3 Estructura de las políticas de seguridad informática

4.3 BENEFICIOS Y LIMITANTES

4.3.1 Beneficios de aplicar políticas de seguridad informática

La aplicación de políticas es un elemento necesario cuando se pretende gestionar la seguridad informática en una empresa, cuyos beneficios son:

- Respaldan la seguridad de la información; es decir, ayudan a designar todas aquellas responsabilidades y prácticas que ejerce la alta dirección en cuanto a la seguridad.
- Ayudan en la protección de los activos; es decir, todo aquello que es importante para la organización, incluyendo la información considerada como sensible, y que en la mayoría de los casos no debería ser del dominio público.
- Contribuyen en la creación de un entorno para que las medidas de seguridad que han sido aplicadas en la industria y han generado buenos resultados, puedan ser aplicadas dentro de las empresas. En otras palabras, permiten adoptar y al mismo tiempo adaptar a las necesidades propias, las mejores prácticas en materia de seguridad.
- Ayudan en determinar la conducta esperada de los miembros de la empresa, a través de la definición de funciones y responsabilidades.
- Crean conciencia al personal sobre la importancia de la información a la cual tiene acceso, los riesgos de seguridad que pueden afectarlos y principalmente sobre la manera de minimizar sus consecuencias o la frecuencia con la que se presentan.
- Establecen lo necesario para estar en apego con las leyes aplicables de acuerdo con el negocio de la empresa, así como con las regulaciones y obligaciones contractuales directamente relacionadas con seguridad.

4.3.2 Limitantes en la aplicación de políticas de seguridad informática

Algunas de las limitantes en la aplicación de políticas de seguridad informática en las empresas son:

- Deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la empresa, cambio o diversificación del área de negocios entre otros. Estas actualizaciones pueden aumentar los costos de las empresas.
- No se puede obtener una garantía en la colaboración de todo el personal en la aplicación correcta de las políticas de seguridad informática, lo que podría causar deficiencia en algunas áreas críticas de seguridad.

4.4 DESARROLLO DE CASO PRÁCTICO

4.4.1 Conocimiento de la empresa

Para el desarrollo de la propuesta de solución fue necesario seleccionar una de las empresas listadas en la población, para evaluar sus operaciones y diseñar políticas específicas para el sector, la empresa fue el grupo:

A. **COMCA Internacional,** es una empresa de soluciones logísticas en transporte y distribución que opera en El Salvador desde 1967. Se consolida como la empresa de capital nacional líder en el servicio de transporte, almacenaje y mudanzas. Actualmente, cuenta con más de 50 años de experiencia en el mercado salvadoreño, gracias a las alianzas estratégicas con empresas de primer nivel y afiliación a diversas instituciones internacionales, que han permitido ofrecer un servicio de primer nivel con tarifas sumamente competitivas. COMCA Internacional es representante exclusivo para El

Salvador de DB Schencker, empresa líder en su campo, con presencia en más de 120 países a nivel mundial; además es representante de ZIM Integrated Shipping una de las 5 Navieras con profit a nivel mundial y servicios marítimos especializados.

B. Visión

- Ser la mejor opción como facilitadores del comercio internacional en la región centroamericana.

C. Misión

- Brindamos soluciones logísticas con servicios de clase mundial

D. Valores

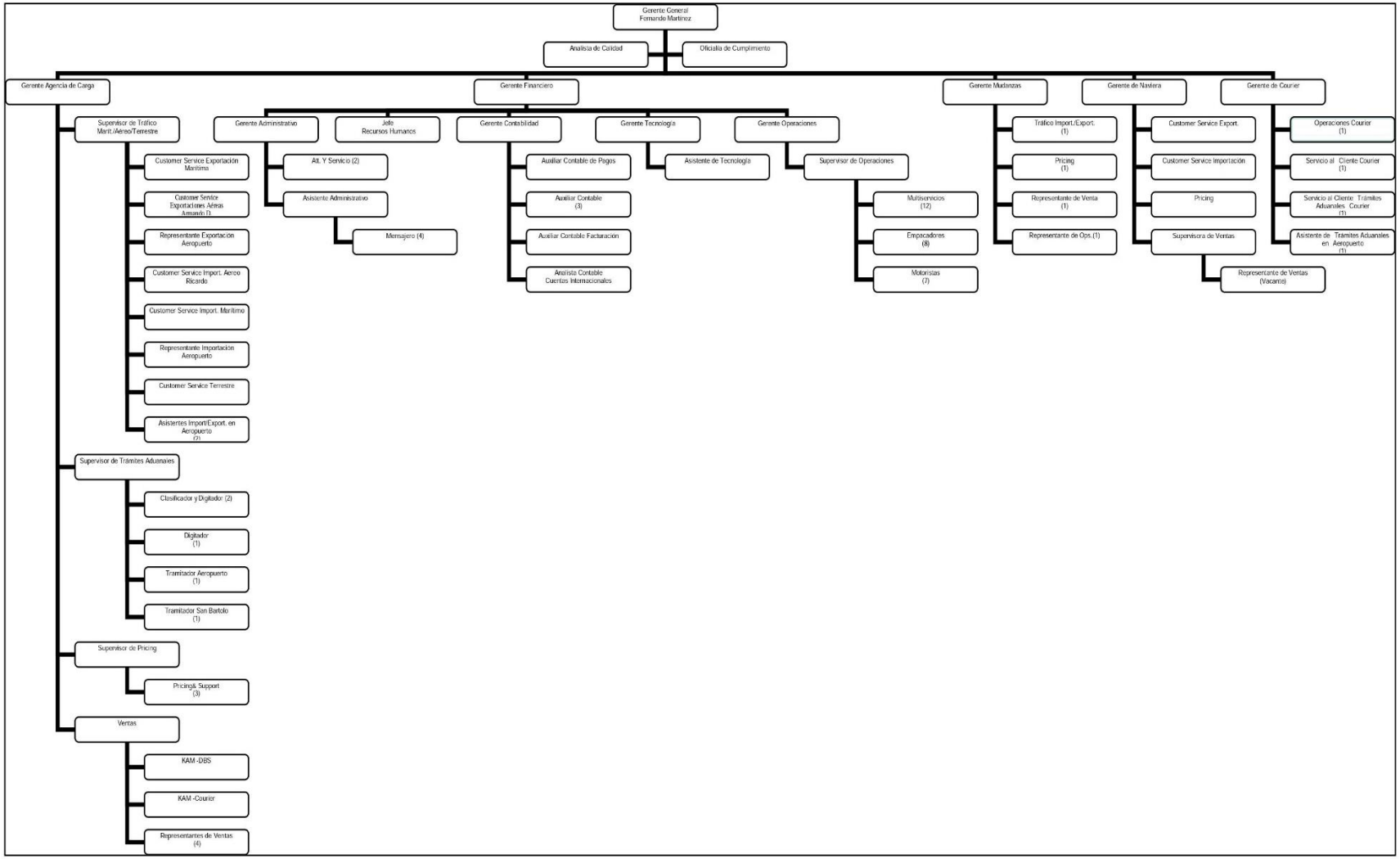
- **Respeto:** nos desempeñamos en un ambiente agradable y en armonía, valorando a nuestros compañeros, clientes y proveedores.
- **Compromiso con la Calidad:** dar siempre lo mejor de nosotros mismos.
- **Honestidad:** siempre hacemos buen uso de los que se nos confía.
- **Servicio:** el cliente es y será la razón de ser de nuestra empresa.
- **Responsabilidad:** cumplimos con nuestras decisiones, compromisos y obligaciones para con nuestros clientes, empresa familia y sociedad.

E. Servicios que ofrece

Algunos de los servicios que ofrece COMCA Internacional son:

- Agencia de carga: transporte aéreo, marítimo y terrestre
- Mudanza local e internacional.
- Servicios de almacenaje.
- Naviera con transporte marítimo especializado.

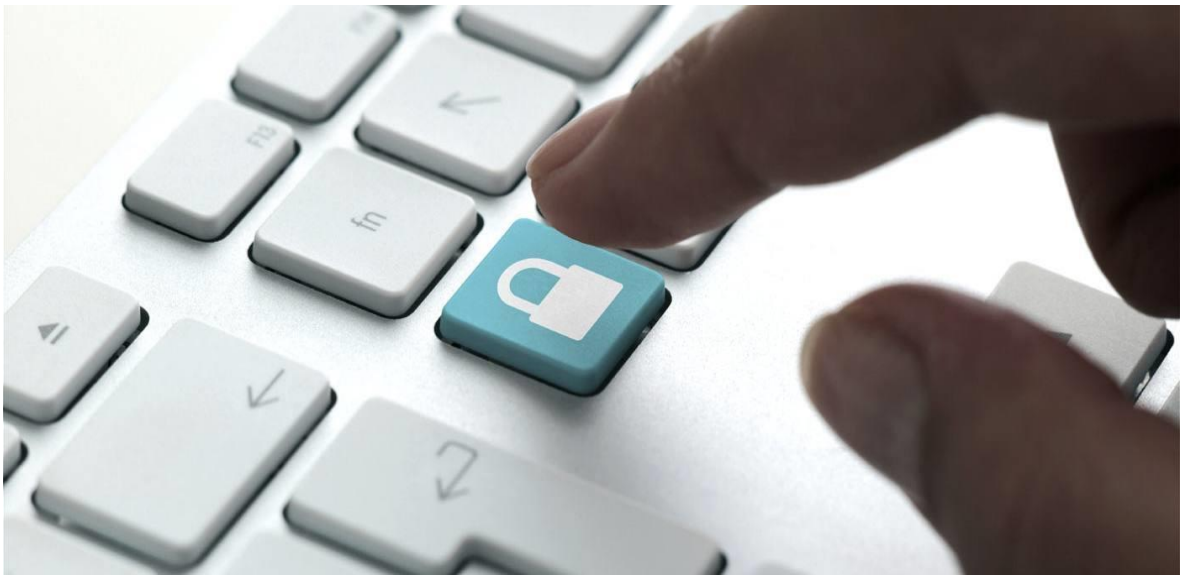
F. Estructura organizacional



Fuente: *Departamento de Recursos Humanos COMCA Internacional*

4.4.2 Políticas de seguridad informática basadas en la Norma Técnica Salvadoreña ISO/IEC 27001:2013

A continuación, se presentan las políticas de seguridad informática basadas en la Norma Técnica Salvadoreña ISO/IEC 27001:2013, las cuales podrán ser aplicadas por todas las empresas del sector de logística y transporte de carga del municipio de Antiguo Cuscatlán, para minimizar los riesgos en sus sistemas de información.



POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EMPRESAS DEL SECTOR DE LOGÍSTICA Y TRANSPORTE DE CARGA DEL MUNICIPIO DE ANTIGUO CUSCATLÁN.

Índice

Introducción

El objetivo de la seguridad informática es proteger los recursos informáticos valiosos de las empresas, tales como la información, el hardware o el software. A través de la adopción de las medidas adecuadas, la política de seguridad informática ayuda a las empresas a cumplir sus objetivos, protegiendo sus recursos financieros, sus sistemas, su reputación, su situación legal, y otros bienes tanto tangibles como intangibles.

El documento que se presenta como políticas de seguridad, pretende, ser el medio de comunicación en el cual se establecen las reglas, normas, controles y procedimientos que regulen la forma en que la empresa, prevenga, proteja y maneje los riesgos de seguridad en diversas circunstancias. Las normas y políticas expuestas en este documento sirven de referencia, en ningún momento pretenden ser normas absolutas, las mismas están sujetas a cambios realizables en cualquier momento, siempre y cuando se tengan presentes los objetivos de seguridad de la información y los servicios prestados por la empresa y sus objetivos estratégicos.

Las políticas de seguridad informática establecen el marco formal de seguridad que debe aplicar la empresa, integrando el recurso humano con la tecnología, denotando responsabilidades y actividades complementarias como respuesta ante situaciones anómalas a la seguridad. También establece responsabilidades en cuanto a la aplicación de las mismas por parte de empleados y terceros relacionados con las empresas.

Objetivo: Propiciar y asegurar condiciones adecuadas que permitan proteger los activos informáticos en su integridad, confidencialidad y disponibilidad en las empresas del sector de logística y transporte de carga del municipio de Antiguo Cuscatlán, con el fin de contribuir en buena gestión y generar confianza en los clientes internos y externos, así como ante terceros relacionados.

Alcance: Las políticas de seguridad de la información aquí diseñadas, contemplan los aspectos administrativos y de control que deben ser cumplidos por los colaboradores y terceros que laboren o tengan relación con las empresas del sector de logística y transporte de carga del municipio de Antiguo Cuscatlán, para conseguir un adecuado nivel de protección de sus activos informáticos.

Responsabilidad: Es responsabilidad de todo el personal de las empresas la adecuada aplicación de políticas de seguridad informática, para reducir al mínimo los riesgos que por falta de aplicación de las mismas se puedan generar, la mala aplicación o aplicación parcial de las presentes políticas no aseguran la reducción de los riesgos en un 100%. Es responsabilidad de la dirección la divulgación y cumplimiento de las políticas dentro de las empresas.

Vigencia: Las presentes políticas entrarán en vigencia cuando sean aprobadas por la dirección de las empresas para su aplicación inmediata. Esta normativa deberá ser revisada y actualizada conforme a las exigencias de la empresa o en el momento en que haya la necesidad de realizar cambios sustanciales en la infraestructura tecnológica.

Marco técnico: El marco técnico de referencia usado en la elaboración de las presentes políticas de seguridad informática es el siguiente:

- **Anexo A, de la Norma Técnica Salvadoreña ISO/IEC 27001:2013**: el cual establece los controles específicos que una organización debe aplicar para garantizar la seguridad de la información.
- **COBIT 5: procesos catalizadores:** el cual establece practicas claves que la organización puede aplicar para garantizar la seguridad informática en diferentes áreas.

Sistema de codificación: el sistema de codificación utilizado para identificar las presentes políticas de seguridad informática es el siguiente:

- **PSI:** código para identificar las políticas de seguridad informática
- **PSI 01:** código para identificar el grupo de políticas
- **PSI 01.1:** código para identificar el sub grupo de políticas
- **PSI 01.1.1:** código para identificar las políticas especificas
- **DSS Y APO**: Se refieren a los procesos catalizadores de COBIT 5
- **"A"**: Se refiere al anexo A objetivos de control y controles de referencia de la Norma Técnica Salvadoreña ISO/IEC 27001:2013

Términos usados: todos los términos usados en el presente documento tienen el significado que se define a continuación**:**

- **Amenaza**: es un evento que puede desencadenar un incidente en la empresa, produciendo daños materiales o pérdidas inmateriales en sus activos.
- **Ataque**: evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.
- **Centro de Comunicaciones:** cualquier oficina dentro de las empresas que cuenten con equipamiento de cómputo, telecomunicaciones o servidores.
- **Confidencialidad:** proteger la información de su revelación no autorizada. Esto significa que la información debe estar protegida de ser copiada por cualquiera que no esté explícitamente autorizado por el propietario de dicha información.
- **Contraseña:** conjunto de caracteres que permite el acceso de un usuario a un recurso informático (passwords).
- **Cuenta:** mecanismo de identificación de un usuario, llámese de otra manera, al método de acreditación o autenticación del usuario mediante procesos lógicos dentro de un sistema informático.
- **Encriptación:** es el proceso mediante el cual cierta información o "texto plano" es cifrado de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación. Es una medida de seguridad utilizada para que al momento de almacenar o transmitir información sensible ésta no pueda ser obtenida con facilidad por terceros.
- **Firewall:** sistema de defensa basado en que el tráfico de entrada o salida a la red pasa por un sistema de seguridad que autoriza, deniega y registra todo evento en función de una política de seguridad; controlando la comunicación interna y externa de la red.
- **Impacto**: consecuencia de la materialización de una amenaza.

- **Incidente de seguridad de la información:** se considera un Incidente de Seguridad de la Información a cualquier evento que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).
- **Integridad:** proteger la información de alteraciones no autorizadas por la organización.
- **Red:** equipos de cómputo, sistemas de información y redes de telemática de las empresas.
- **Riesgo**: posibilidad de que se produzca un Impacto determinado en un activo, en un dominio o en toda la empresa.
- **Usuario:** cualquier persona (empleado o no) que haga uso de los servicios de las tecnologías de información proporcionadas por las empresas tales como equipos de cómputo, sistemas de información, redes de telemática.
- **Virus informático:** programa ejecutable o pieza de código con habilidad de ejecutarse y reproducirse, regularmente escondido en documentos electrónicos, que causan problemas al ocupar espacio de almacenamiento, así como destrucción de datos y reducción del desempeño de un equipo de cómputo
- **Vulnerabilidad**: posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.

PSI 01 Políticas de organización de la seguridad informática

Objetivo: instaurar dentro de la organización un método que permita el control y operación de la seguridad informática.

PSI 01.1 Organización Interna

PSI 01.1.1 Roles y responsabilidades de la seguridad de la información

La alta dirección de las empresas debe establecer perfiles de puestos claros para los directores de seguridad informática, en los que se les atribuyan sus responsabilidades incluyendo la seguridad de la información, indicadores y puntos de control que debe de monitorear en todo el proceso de su gestión.

La gerencia general en conjunto con recursos humanos y el departamento de TI debe establecer los roles y responsabilidades relacionados con la seguridad de la información en todos los niveles tanto directivos como operativos.

La seguridad informática tendrá la siguiente estructura:

Figura 4 estructura organizativa de la seguridad informática

PSI 01.1.2 Segregación de funciones

El director de seguridad informática, encargado de la operación y administración de los recursos tecnológicos que apoyan los procesos de la organización, asignará funciones específicas a sus usuarios o empleados, quienes deben efectuar la operación y administración de dichos recursos tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades. Así mismo, velará por la eficiencia de los controles implantados en los procesos operativos asociados a los recursos tecnológicos con el objeto de proteger la confidencialidad, la integridad y la disponibilidad de la información manejada y asegurará que los cambios efectuados sobre los recursos tecnológicos, serán adecuadamente controlados y debidamente autorizados.

PSI 01.1.3 Seguridad de la información en la gestión de proyectos

La Dirección de seguridad informática en conjunto con la Gerencia General deben participar activamente en los proyectos de nuevas rutas, clientes o servicios de las empresas del sector de logística de carga y transporte para proveerlos de las seguridades adecuadas, gerenciando principalmente los de seguridad informática, y estableciendo controles específicos a los usuarios de estos proyectos para evitar la fuga de información previo a su realización, y que esto perjudique en la obtención del proyecto.

PSI 01.2 Dispositivos móviles y trabajo remoto

PSI 01.2.1 Política de dispositivos móviles

Los usuarios que cuenten con la herramienta de dispositivos móviles otorgados por la organización deben evitar la descarga de software o aplicaciones que no sean necesarias para

el cumplimiento de sus funciones, así como su instalación y uso en las estaciones de trabajo o dispositivos móviles.

Los departamentos a los cuales se les asignarán un dispositivo móvil por parte de la empresa, debido a la necesidad en el trabajo que desarrollan son los empleados de los siguientes departamentos:

- Contabilidad
- Área de operaciones portuarias
- Área de agencias de carga
- Área de ventas
- Trámites aduanales
- Operaciones Courier
- Mudanzas
- Área de Naviera

La dirección de seguridad informática realizara las siguientes actividades para asegurar la correcta aplicación de dispositivos móviles de los empleados.

- Establecer un listado con el software, aplicaciones y sistemas de información que se encuentran permitidos en las estaciones de trabajo o equipos móviles para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo o equipos móviles corresponda únicamente al permitido para un mejor control.

- Establecer un método de bloqueo (contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles institucionales que serán entregados a los usuarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad automáticamente ingresen a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.
- Cifrar la memoria de almacenamiento de los dispositivos móviles de tal forma que no permita la copia o extracción de datos si se desconoce el método de desbloqueo.
- Configurar una opción de borrado remoto de información en los dispositivos móviles, a fin de poder eliminar los datos de estos dispositivos cuando se encuentren en riesgo (robo o hurto del dispositivo móvil), evitando así la divulgación no autorizada de información.
- Diseñar un plan de back up para la información contenida en los dispositivos móviles, con la frecuencia oportuna para mantener siempre una copia en los servidores de la organización.
- Contar con códigos de seguridad de la tarjeta SIM para los dispositivos móviles antes de entregarlos a los usuarios finales y almacenar estos códigos en su base de datos de información restringida y/o confidencial.
- Monitorear toda la información que a través de redes sociales o aplicaciones permitidas por la organización (WhatsApp, Facebook, etc.) para su uso en cada una de las funciones de los usuarios y con esto cumplir con sus labores sean transmitidas, esto contempla las conversaciones o chats y los archivos que en estos se comparten a

fin de evitar la fuga de información confidencial de la empresa a destinatarios no autorizados o relaciones con el servicio.

- Elaborar un documento que entregará a cada usuario que utilice un dispositivo móvil de la organización en el cual deberá de establecer las normas y reglas de uso del dispositivo móvil, así como dejar establecido que este dispositivo es de uso exclusivo para actividades relacionadas a la prestación de servicios de la organización y que por tal motivo es monitoreada la información que desde este se genera, así como la que se almacena en él.

Los empleados de los departamentos a los cuales se les asigne un dispositivo móvil, deben aplicar las siguientes medidas para garantizar la seguridad:

- Evitar al máximo el uso de los dispositivos móviles en lugares que no ofrezcan las garantías de seguridad necesarias para evitar pérdidas tanto físicas (robo) como lógicas (redes de acceso públicas, uso de bluetooth, infrarrojos).
- Evitar conectar los dispositivos móviles a puertos USB de computadoras públicas o que no pertenezcan a la organización, así como en hoteles, restaurantes, otras organizaciones similares en las cuales no se cuenta con la seguridad o respaldo necesario.
- No deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.
- No deben de modificar ninguna de las configuraciones de seguridad instaladas y utilizadas en los dispositivos móviles ya que estos son los que permiten la seguridad,

al hacer esto estarían realizando una actividad en contra de la organización y esto repercutirá en una sanción o amonestación al empleado que lo haga.

PSI 01.2.2 Trabajo remoto

La gerencia general en conjunto con la dirección de seguridad informática deben analizar y aprobar los métodos de conexiones remotas que estarán en interacción con la plataforma tecnológica interna de la organización así como los usuarios que se autorizan para el trabajo remoto ya sea por su perfil de puesto o por sus actividades a desarrollar que lo requieran, debe de restringir las conexiones remotas a los recursos de la plataforma tecnológica; y solamente permitir los accesos al personal autorizado y por los tiempos necesarios establecidos. Debe implementar controles que permitan monitorear la seguridad de la información que se interactúe de forma remota, así como verificar la efectividad de los controles aplicados a los recursos de la plataforma tecnológica.

Todo dispositivo que se utilice para la conexión de forma remota debe estar previamente identificada en una base de datos de la dirección de seguridad informática (Laptop, dispositivo móvil, IP) además deben cada uno de estos contar con software antivirus que permita escanear la información y evitar contagios o posibles invasiones de software malicioso que dañe la información generada o almacenada.

Los usuarios que utilicen la conexión remota deben previamente estar autorizados y deben acatar las condiciones de uso establecidas para estos propósitos, si ellos no cumplieran con estos protocolos y ponen en riesgo la información de la organización pueden ser sujetos a

una amonestación o llamado de atención por su jefe inmediato superior, así como por el Director de Seguridad Informática.

Los empleados a los cuales se les permiten trabajar de forma remota son, por ejemplo:

- Gerentes de línea
- Tramitadores
- Jefes de líneas de apoyo
- Supervisores de trámites aduanales
- Representantes de ventas
- Servicio al cliente de Importaciones y exportaciones
- Supervisor de tráfico aéreo/marítimo/terrestre
- Analista contable de cuentas internacionales

PSI 02 Políticas de seguridad de los recursos humanos

Objetivo: asegurar que todos los empleados conozcan y apliquen de manera adecuada las políticas de seguridad informática, en todos niveles de responsabilidad, dentro de las empresas.

PSI 02.1 Antes del empleo

PSI 02.1.1 Selección de personal

El departamento de Recursos Humanos, al contratar a un nuevo empleado se asegurara de verificar que tal persona cumpla con los requisitos del puesto para el cual ha sido contratado y en cuanto sea posible verificara que la persona no haya estado involucrado en incidentes de seguridad de la información en trabajos anteriores, la selección de personal se hará de acuerdo a los establecido por El Código de Trabajo, y como mínimo se requerirá de cada empleado la siguiente documentación para crear su archivo personal:

- Acción de Personal, en la cual se formaliza la decisión de contratación y el sueldo a devengar.
- Solicitud de Empleo debidamente completada por el aplicante, Fotocopia de DUI, NIT, Tarjeta de AFP e ISSS, de Libreta de ahorro o cuenta corriente vigente del Banco con quien se maneje la Cuenta Planillera.
- Solvencia de la Policía y constancia de NO antecedentes penales (con antigüedad máxima de 2 meses).
- Referencias personales y de trabajo.
- Resultados de las entrevistas y pruebas.
- Currículum Vitae.

- Constancias de Estudios.
- Boleta de Seguro de Vida (*) y/o Médico (en caso aplique).
- Original del contrato.
- Contrato de confidencialidad.

PSI 02.1.2 Términos y condiciones de empleo

En los contratos de los empleados, se incluirá una cláusula de confidencialidad que será comunicada a cada empleado contratado; para garantizar que los empleados cumplan con la seguridad de la información de la empresa, dicha cláusula será leída al empleado antes de firmar su contrato de trabajo para garantizar que entiende la importancia de la confidencialidad en la empresa. La cláusula de confidencialidad en los contratos será como se muestra en el ***anexo 4.***

PSI 02.2 Durante el empleo

PSI 02.2.1 Responsabilidades de la dirección

Cuando se contrate a un nuevo empleado el director de seguridad informática en coordinación con el departamento de Recursos Humanos, entregarán una copia de las políticas de seguridad informática aplicadas dentro de la empresa y serán explicadas en un lenguaje entendible, para dejarle claro al empleado la importancia de aplicarlas desde su lugar de trabajo, para comprobar que el empleado ha recibido su copia de las políticas de seguridad informática, se hará firmar un acuse de recibido del documento, como se muestra en el ***anexo 5.***

PSI 02.2.2 Capacitación, educación y concientización sobre la seguridad de la información

El director de seguridad informática en coordinación con el departamento de Recursos Humanos programara capacitaciones por departamentos, acerca de seguridad informática y temas relacionados en la empresa al menos 4 veces por año, el director deberá llevar una bitácora de dichas capacitaciones que contenga al menos: lugar y fecha, departamento capacitado, tema de la capacitación, lista de asistentes con su respectiva firma, responsable de la capacitación, entre otros.

PSI 02.2.3 Proceso disciplinario

La falta de aplicación y/o cumplimiento de las políticas de seguridad informática por parte del personal, tendrá acciones disciplinarias en contra de los mismos la cuales se dividirán en:

- **Faltas leves:** cuando el empleado no aplicare una política de seguridad informática, que no causare daños económicos ni riesgos de importancia material para la empresa.
- **Faltas graves:** cuando el empleado no aplicare una o varias políticas de seguridad informática**,** que causare daños económicos no significativos para la empresa y pusiere en riesgo a la empresa y la seguridad informática de la misma**.**
- **Faltas muy graves:** cuando el empleado no aplicare una o varias políticas de seguridad informática, que causare daños económicos significativos a la empresa y la empresa se viere afectada por tal razón, y esto causare daño a la imagen de la misma ante terceros relacionados.

Las siguientes sanciones disciplinarias serán aplicadas a los empleados que cometan las faltas descritas anteriormente:

- Amonestación verbal.
- Amonestación escrita.
- Suspensión de labores, de un día sin goce de sueldos.
- Destitución de su trabajo.

PSI 02.3 Terminación y cambio del empleo

PSI 02.3.1 Responsabilidades de terminación o cambio de empleo

Cuando se dé por terminada la relación laboral de un empleado, ya sea por retiro voluntario o con causa justificada, el director de seguridad informática deberá velar que el empleado despedido entregue todos los activos informáticos asignados propiedad de la empresa, y toda la información que en ellos haya, y cuidar que el empleado no pueda llevar información en discos extraíbles de tipo personal, la entrega de los activos informáticos se hará constar en un acta que firmaran tanto el empleado que los entrega, como también la persona que los recibe, también deberán entregarse los accesos físicos y lógicos asignados al empleado. Cuando el empleado sea promovido de su cargo a otro, entregara los activos informáticos que tiene en su poder, para asignarle los nuevos, de acuerdo a su nuevo cargo, dicha entrega también se hará constar en un acta.

PSI 03 Políticas de gestión de activos

Objetivo: identificar los activos informáticos de la empresa para definir el buen uso y seguridad de los mismos.

PSI 03.1 Responsabilidad sobre los activos

PSI 03.1.1 Inventario de activos

El director de seguridad informática, deberá llevar un inventario de activos informáticos clasificando a cada uno de las siguientes clasificaciones:

- **Recursos de información:** bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, disposiciones relativas a sistemas de emergencia para la reposición de información perdida (“fallback”), información archivada.
- **Recursos de software:** software de aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios.
- **Activos físicos**: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PBXs, máquinas de fax, contestadores automáticos), medios magnéticos (USB y discos), otros equipos técnicos (suministro de electricidad, unidades de aire acondicionado) y mobiliario.
- **Servicios**: servicios informáticos y de comunicaciones, utilitarios generales. Calefacción, iluminación, energía eléctrica, aire acondicionado, mantenimientos.

Par cada uno de ellos deberá llevar un registro en el cual especifique lo siguiente:

- Código

- Tipo de activo de acuerdo a la clasificación anterior
- Formato en que se guarda
- Área que lo utiliza
- Fecha de compra
- Fecha de caducidad (si aplica)
- Descripción del activo
- Ubicación del activo (si aplica)
- Precio del activo
- Responsable del activo

El inventario de activos será actualizado ante cualquier modificación de la información registrada, y revisado con una periodicidad semestral por el encargado de llevar el inventario.

PSI 03.1.2 Propiedad de los activos

El encargado de la custodia de los activos consolidados será el director se seguridad informática, sin embargo, cada área, y empleado de la organización será responsable de los activos que utiliza en el desarrollo de sus funciones laborales diarias.

A cada empleado se le deberá asignar los activos que utilizará en su puesto de trabajo, para controlar dicho proceso el jefe de seguridad informática deberá de llevar una bitácora de registros que deberá llevar como mínimo los siguientes campos:

- Nombre del empleado.
- Área a la que pertenece.
- Cargo que desempeña.

- Activos necesarios en su función laboral.
- Activos entregados.
- Fecha de entrega.
- Condiciones de los activos entregados.
- Firma de entrega.

PSI 03.1.3 Uso aceptable de los activos

Los empleados que reciban activos informáticos deben utilizarlos de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la empresa. Los recursos tecnológicos de la empresa provistos a funcionarios y personal, son proporcionados con el único fin de llevar a cabo las labores de su puesto de trabajo; por consiguiente, no deben ser utilizados para fines personales o ajenos a este. Todos los dispositivos móviles y demás recursos tecnológicos serán asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos. El director de seguridad informática deberá explicar al empleado el correcto uso de cada recurso asignado, y velará por el uso correcto de cada uno de ellos.

PSI 03.1.4 Devolución de los activos

Cuando un empleado cese de laborar en la empresa ya sea por despido o por retiro voluntario o cambio de puesto, dentro de la empresa, deberá entregar al director de seguridad informática todos los equipos tecnológicos que le fueron asignados, quien es el responsable de recibir los equipos de trabajo fijo y/o portátil, para su reasignación o disposición final, y generar copias de seguridad de la información contenida en dichos equipos. También deberá

llenar un acta en que se haga constar la entrega de los equipos por parte del empleado, dicha acta contendrá como mínimo lo siguiente:

- Nombre del empleado
- Cargo desempeñado
- Área a la que pertenece
- Fecha
- Razón de entrega de los equipos asignados
- Lista de equipos entregados
- Estado de los equipos entregados
- Otras notas adicionales para explicar la entrega de equipos
- Firmas

PSI 03.2 Clasificación de la información

PSI 03.2.1 Clasificación de la información

Toda la información de la empresa debe de ser clasificada como Restringida, Confidencial, Uso Interno o General, de acuerdo al criterio de cada uno de los propietarios o usuarios, los cuales deberán informar la clasificación al director de seguridad informática para su posterior etiquetado. La clasificación asignada a un tipo de información, solo puede ser cambiada por el propietario de la información, luego de justificar formalmente el cambio en dicha clasificación. La información que existe en más de un medio (por ejemplo, documento fuente, registro electrónico, reporte o red) debe tener la misma clasificación sin importar el formato. La información debe de ser examinada para determinar el impacto que causaría en la empresa

si dicha información fuere divulgada o alterada por medios no autorizados las clasificaciones se definen a continuación:

- **Restringida:** Información con mayor grado de sensibilidad; el acceso a esta información debe de ser autorizado caso por caso. Ejemplos de este tipo son: contratos con las representaciones internacionales, comisiones que se pagan por los servicios prestados, transferencia de dinero mensual, planes estratégicos de la compañía, estados financieros de la compañía, costos, entre otros.
- **Confidencial:** Información sensible que solo debe ser divulgada a aquellas personas que la necesiten para el cumplimiento de sus funciones.

  Ejemplos de este tipo de información son: Contratos con clientes y empleados, costos de venta, estatus de la carga importaciones y exportaciones (aérea, marítima y terrestre), condiciones de ventas, bases de datos de clientes, base de datos de proveedores.
- **Uso Interno:** Datos generados para facilitar las operaciones diarias; deben de ser manejados de una manera discreta, pero no requiere de medidas elaboradas de seguridad.

  Ejemplos de este tipo de información son: Comprobantes de crédito fiscal y facturas de ventas, conocimientos de embarque, carta de porte, guía aérea, declaraciones de mercadería de clientes, estados de las mercaderías de clientes, rutas de comercio.
- **General:** Información que es generada específicamente para su divulgación a la población general de usuarios.

Ejemplos de este tipo de información son: Precios de los servicios que se prestan con tarifas de referencia, servicios que se ofrecen, promociones y descuentos con clientes, nuevos servicios (marketing).

PSI 03.2.2 Etiquetado de la información

El jefe de seguridad informática deberá diseñar un sistema de codificación para etiquetar la información de acuerdo a la clasificación anterior, dicho identificador puede estar en el encabezado del documento, en el nombre del archivo, en la etiqueta del medio de almacenamiento o en una nota anexa. El procedimiento para etiquetado y archivo será elaborado por el jefe de seguridad informática y comunicado a todos los empleados.

PSI 04 Política de control de acceso

Objetivo: asegurar el acceso a la información y sistemas solo a los usuarios autorizados y así prevenir accesos a las redes, sistemas, aplicaciones que dañen o pongan en riesgo a la organización y su continuidad.

PSI 04.1 Requerimientos del negocio para el control de acceso

PSI 04.1.1 Política del control de acceso

Todas las personas que trabajen para la organización y/o aquellas que son designadas para trabajar en actividades específicas (consultores, auditores, proveedores) son responsables del adecuado uso de la información suministrada para tal fin, por lo que deben velar por su integridad, confidencialidad y disponibilidad, dicha información si se considera de carácter secreta o restringida debe estar provista de seguridad necesaria por quien la maneja para evitar el uso indebido de personal no autorizado

Al finalizar las jornadas laborales, el personal deberá archivar todo documento sensible que pueda comprometer los intereses de la organización, es recomendable que se archiven bajo llave, cajas fuertes o demás medios de almacenamientos físicos que proporcionen seguridad; así como las áreas donde información confidencial o critica es manipulada debe de contar con cámaras que registren las actividades desarrolladas en esos sectores. Estas políticas son aplicables a las áreas de:

- Ventas
- Agencia de carga
- Área de ventas

- Área de contabilidad
- Área de mudanzas
- Área de naviera
- Área de Courier
- Área de operaciones
- Área de trámites aduanales

PSI 04.1.2 Acceso a redes y servicio de red

El director de seguridad informática como responsable de las redes de datos y los recursos informáticos de la organización, vigilará porque dichas redes estén debidamente protegidas contra accesos no autorizados a través de controles de accesos lógicos establecidos como:

- Establecer un procedimiento de autorización y controles que permita la protección de acceso a las redes de datos.
- Las redes inalámbricas de la organización contaran con métodos de autenticación para evitar los accesos no autorizados.
- Controlar la autenticación de los usuarios provistos por terceras partes en las redes, así como velar por la aceptación de las responsabilidades de dichos terceros para lo cual se debe formalizar la aceptación de las políticas de seguridad de información.
- Elaborar un formato de creación de cuentas de usuarios el cual deberá de ser autorizado por el director de seguridad informática, así como el gerente general en el cual se incluirá el acuerdo de confidencialidad, ambos debidamente firmados.
- Autorizar la creación o modificación de cuentas de acceso a las redes o recursos de tecnología de la organización.

- Periódicamente verificar los controles de accesos con el objetivo de revisar que los usuarios autorizados posean los permisos únicamente a los recursos de red y servicios de la plataforma tecnológica para los que se han autorizado.

PSI 04.2 Gestión del acceso de usuarios

PSI 04.2.1 Registro y anulación de los usuarios

El director de seguridad informática establecerá un procedimiento formal para la administración de los usuarios en las redes de datos, recursos tecnológicos y sistemas de información a los que tendrán accesos el cual contemplara la creación, modificación, bloqueo o eliminación de las cuentas del usuario.

En coordinación con los jefes inmediatos de los solicitantes de las cuentas de usuario se deberán de aprobar la creación, modificación, bloqueo y/o eliminación sobre las redes de datos, recursos tecnológicos y sistemas de información acorde al procedimiento establecido.

Definir lineamientos para la correcta configuración de contraseñas los cuales deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso entre otros.

PSI 04.2.2 Gestión de privilegios de derechos de acceso

Es responsabilidad del director de seguridad de informática en conjunto con los gerentes de líneas de negocio y líneas de apoyo dentro de la organización, definir los perfiles de usuario y autorizar las solicitudes de acceso a los recursos de la organización de acuerdo a los perfiles previamente establecidos.

Se velará por que los recursos de la plataforma tecnológica y los servicios de red de la organización sean operados y administrados en condiciones controladas y de seguridad el cual permita un monitoreo posterior de la actividad que cada usuario realice (incluyendo a los administradores y aquellos usuarios poseedores de los más altos privilegios sobre dicha red y sistemas).

La necesidad de crear cuentas personalizadas con altos privilegios es fundamental por lo que los directores de seguridad en conjunto con el gerente general establecerán dichas cuentas para los administradores de los recursos tecnológicos, servicios de red y sistemas de información, para lo cual se generará un listado y se mantendrá actualizado con el detalle de las cuentas con privilegios de los recursos de la plataforma tecnológica.

Los gerentes de líneas de negocios y líneas de apoyo tendrán acceso de acuerdo a las funciones que cada uno desarrolla.

PSI 04.2.3 Revisión de los derechos de acceso

Periódicamente se revisaran los accesos otorgados a usuarios y se monitoreara que cada cuenta de usuario haya realizado accesos a la plataforma asignada según el formato aprobado, si existiera una variación entre los accesos otorgados, y a los que han acceso se deberá de investigar como el usuario obtuvo ese acceso, y tomar las medidas correctivas para solventar el problema, adicional a esto luego de detectada la causa raíz de esta infracción se podrá interponer una amonestación o llamado de atención al personal involucrado.

PSI 04.2.4 Remover o ajustar los derechos de acceso

En las revisiones periódicas se determinará aquellos accesos a módulos o redes que los usuarios no han utilizado a fin de verificar la necesidad de privilegios otorgados con el objetivo de poder eliminar todos los que no sean necesarios para el perfil o para el usuario.

Se deberá de utilizar un formato el cual proporcionara el director de seguridad informática para remover o ajustar los privilegios de los usuarios, estos serán de carácter obligatorio cuando un empleado sea rotado (cambio de puesto) dentro de la organización o cuando exista finalización de contrato laboral, a manera de que los usuarios sean desactivados y no se puedan utilizar nunca más.

PSI 04.3 Responsabilidades del usuario

PSI 04.3.1 Uso de información de autenticación secreta

Para evitar el uso indebido de usuarios a módulos de sistemas, áreas restringidas, información confidencial, se prohíbe a los usuarios compartir sus claves de acceso y es responsabilidad de cada usuario el correcto uso de esta información, cualquier acceso indebido con un usuario será responsabilidad del personal que no resguardo de forma segura su información de acceso.

Los usuarios asignados para los servicios de red y sistemas son los responsables de las acciones que se realicen con las contraseñas para accesos, así como la información generada y procesada en los sistemas.

El personal provisto por entidades externas (clientes, proveedores, colegas extranjeros) que posean accesos a la plataforma tecnológica de la organización debe acogerse a los lineamientos para la configuración de contraseñas y no divulgarlas a personal interno.

PSI 04.4 Control de acceso a sistemas y aplicaciones

PSI 04.4.1 Restricción del acceso a la información

El director de seguridad informática en conjunto con los gerentes de cada línea en la organización, velaran por el control de acceso así como asignación, modificación y revocación de privilegios de accesos a los sistemas y aplicaciones de manera controlada, el objetivo principal es proteger a los sistemas y aplicativos de accesos no autorizados a través de herramientas de control de acceso lógico, es importante incluir en esta sección a los desarrolladores de sistemas tanto internos como externos para que se ejecuten buenas prácticas de desarrollo en los sistemas o aplicaciones generados.

El director de seguridad informática será el encargado de establecer ambientes separados tanto físicos como lógicos para el desarrollo, producción y pruebas de los sistemas y aplicativos solicitados por la alta gerencia, contando cada uno con su plataforma, servidores, dispositivos y versiones independientes de los otros ambientes o sistemas ya en funcionamiento, evitando con esto que el desarrollo y pruebas de módulos o sistemas puedan generar un riesgo en la integridad de la información.

A nivel de aplicativos y sistemas se restringirá el acceso a los archivos, así como otros recursos tales como, dirección URL protegidas, funciones protegidas, servicios, información

relevante a las aplicaciones o sistemas, atributos y políticas utilizadas por los controles de acceso, así como información relevante a la configuración de estos.

PSI 04.4.2 Procedimientos seguros de inicio de sesión

Todos los sistemas y aplicativos utilizados por la organización ya sea en ordenadores personales, centros de cómputo, laptops, dispositivos móviles deben de solicitar un inicio de sesión para su acceso en el cual deberán de incluir nombre de usuario y password, para esto será necesario el sistema proporcione una bitácora que muestre al menos el detalle de usuarios conectados, tiempo de conexión, IP desde donde se efectuó la conexión.

Los sistemas y aplicativos deben de mostrar y certificar a los usuarios el ultimo acceso (ya sea exitoso o fallido) en cada acceso exitoso que realicen a los sistemas, esto como un punto de control de validación y que el usuario pueda detectar si alguien más está utilizando sus credenciales.

PSI 04.4.3 Sistema de gestión de la contraseña

Los sistemas y aplicativos deben de contar con un registro de los usuarios y sus contraseñas así como aquellos cambios y solicitud de regeneración de contraseñas, es necesario asegurarse que cuando se genera o reasigna una contraseña se enviara un link o enlace de contraseña temporal a cuentas de correos con dominios de la organización (está prohibido él envió de contraseñas a cuentas personales de correo electrónico como Yahoo! o Hotmail etc.) las cuales deben de tener un perdió de validez establecido; y se debe de forzar al usuario a realizar el cambio cuando se utilice por primera vez esta nueva contraseña.

PSI 04.4.4 Control de acceso al código fuente de los programas

Se debe de asegurar que el acceso al código fuente de los sistemas y aplicativos está asignado al personal capacitado y según perfiles asignados por la alta gerencia y que estos códigos fuentes están protegidos para evitar que sea descargado y modificado.

PSI 05 Políticas de seguridad en la Criptografía

Objetivo: garantizar controles efectivos de cifrado de información para proteger la confidencialidad, autenticad e integridad de la información.

PSI 05.1 Controles criptográficos

PSI 05.1.1 Políticas sobre el uso de controles criptográficos

El director de seguridad informática velará porque la información de la empresa, clasificada como reservada o restringida, sea cifrada al momento de almacenarse y/o transmitirse por cualquier medio, a un tercero dentro o fuera de la empresa.

Esta política es aplicable a todos los sistemas de información de apoyo a procedimientos y actividades que realiza la empresa y de gestión electrónica, y también a las relaciones por medios electrónicos con terceros que no forman parte de los empleados tales como proveedores y clientes.

PSI 05.1.2 Gestión de llaves

Los mecanismos de cifrado de la información confidencial o reservada al momento de almacenarse o transmitirse son las siguientes:

- Si la información se transmite a un tercero no relacionado con la empresa, se utilizará una llave de tipo asimétrica (llaves diferentes para cifrar y descifrar), y se le compartirá al tercero la clave para tener acceso a la información, la contraseña cumplirá al menos las siguientes características: un mínimo de 8 caracteres en los cuales se combinarán números, mayúsculas, minúsculas y caracteres especiales.
- Si la información se transmite a un tercero relacionado con la empresa, se utilizará una llave de tipo simétrica (la misma llave para cifrar y descifrar), y se le compartirá

al tercero la clave para tener acceso a la información, la contraseña cumplirá al menos las siguientes características: un mínimo de 8 caracteres en los cuales se combinarán números, mayúsculas, minúsculas y caracteres especiales.

- El director de seguridad informática deberá llevar una bitácora de contraseñas y personal a quien se les comparte la información de tipo reservada o confidencial.

PSI 06 Políticas de seguridad física y ambiental

Objetivo: asegurar las instalaciones físicas de la empresa contra accesos no autorizados, daños e interferencia, que puedan causar riesgos en la continuidad del negocio.

PSI 06.1 Áreas seguras

PSI 06.1.1 Perímetro de seguridad física

Los perímetros de seguridad deben estar claramente definidos, la ubicación y la resistencia de cada uno de los perímetros dependerá de los requisitos de seguridad de los activos dentro del perímetro. El perímetro de los edificios o lugares que contengan instalaciones de procesamiento de información, debe tener solidez física (por ejemplo, no tendrá zonas que se puedan derribar fácilmente); los muros externos deben ser sólidos y todas las puertas exteriores deben estar protegidas contra accesos no autorizados, mediante mecanismos de control, por ejemplo: vallas, alarmas, cerradura y cámaras de video vigilancia. Las puertas y ventanas deben ser bloqueadas cuando se encuentren descuidadas y se debe contar con protección externa para las ventanas ubicadas en niveles bajos.

Los perímetros de seguridad definidos por la empresa son:

- Área de control de equipos
- Áreas de trámite en puerto y en frontera
- Áreas de importación y exportación por las 3 vías
- Área de mudanzas
- Área de contabilidad
- Área de recursos humanos

- Área de TI
- Área de calidad
- Área de administración

Las áreas de venta están controladas con cámaras de seguridad, pero no deben poseer controles restrictivos de ingreso.

PSI 06.1.2 Controles de entrada físicos

Las visitas autorizadas a ingresar al perímetro de seguridad con información sensible deben quedar registradas en recepción, detallando nombre, empresa, motivo de ingreso, fecha y hora de ingreso y egreso. Durante su permanencia debe estar siempre acompañado por personal debidamente autorizado, a menos que su acceso se haya aprobado previamente.

El acceso a las áreas donde se procesa o almacena información sensible debe ser controlado y restringido sólo a personas autorizadas algunos medios de restricción de acceso físico que se pueden usar son:

- Carnet de identificación.
- Medios magnéticos con uso de clave.
- Huella digital o tarjeta electrónica.
- Guardias de seguridad.
- Acceso restringido por llave.
- Cámaras de video vigilancia.

Cuando un empleado dé por terminada su relación laboral con la empresa se debe de revocar todos los permisos de acceso físico que posea.

PSI 06.1.3 seguridad de oficinas, habitaciones e instalaciones

Todas las oficinas e instalaciones de la empresa deberán contar con las siguientes medidas de seguridad, para evitar pérdida o robo de equipos e información por personas no autorizadas.

- Aire acondicionado.
- Suministro de energía eléctrica.
- Alarma contra incendio.
- Extintores de fuego.
- Mascarías.
- Puertas de acceso controladas.
- Oficina de recepción para evitar el flujo incontrolado de personas no autorizadas.
- Cámaras de video vigilancia.
- Vigilantes de seguridad.

PSI 06.1.4 Protección contra amenazas externas y ambientales

Dado que cualquier tipo de desastre natural o accidental ocasionado por el hombre puede afectar el nivel de servicio y la imagen de la empresa, se deba prever que los equipos de procesamiento y comunicaciones se encuentren localizados en áreas aseguradas y debidamente protegidas contra inundaciones, robos, interferencias electromagnéticas, fuego, humo y demás amenazas que puedan interferir con el buen uso de los equipos y la continuidad

del servicio. La empresa deberá contratar seguros por cualquier desastre natural que suceda en las instalaciones de la misma.

PSI 06.1.5 Trabajo en áreas seguras

Todo lugar de trabajo en que exista algún riesgo de incendio, ya sea por la estructura del edificio o por la naturaleza del trabajo que se realiza, debe contar con extintores de incendio, del tipo adecuado a los materiales combustibles o inflamables que en él existan o se manipulen en las diferentes áreas.

Cualquier área que sea definida como crítica, debe ser protegida bajo las directrices definidas en esta política, contar con un acceso restringida y controlado, que sólo permita el acceso a personal autorizado. El responsable de cada área debe mantener un registro actualizado con los funcionarios autorizados a ingresar de forma permanente a las áreas críticas. El acceso de personal no habitual o personas externas, debe ser autorizado por la Jefatura respectiva o quien ésta faculte para ello. En este caso, el acceso debe quedar registrado, detallando nombre, empresa, motivo del ingreso, fecha y hora del ingreso y egreso.

PSI 06.1.6 Áreas de carga y descarga

El acceso a la entrega y carga desde fuera del edificio debe ser restringido a personal debidamente identificado y autorizado. Donde sea aplicable, las puertas externas deben ser aseguradas cuando se abran las puertas internas. Cuando sea aplicable, el material que ingrese debe ser inspeccionado para evitar posibles amenazas antes de que sea ingresado a su lugar de utilización.

PSI 06.2 Equipo

PSI 06.2.1 Ubicación y protección del equipo

La ubicación de los equipos es fundamental para garantizar la protección y reducir los riesgos asociados al uso inadecuado de los mismos. Para disminuir las amenazas y peligros se debe:

- No situar equipos en sitios altos para evitar caídas.
- Separar los equipos cercanos a las ventanas para evitar caídas o que objetos lanzados desde el exterior de la organización los dañen.
- Evitar comer o beber cerca de los medios de procesamiento de la información.
- Alejar los equipos de lugares que pueden ocasionar un riesgo ambiental, como incendios, explosiones, agua polvo, entre otros.
- Suministrar soporte adecuado a los servidores donde se encuentra la información, para evitar fallas y pérdidas de la información.
- Alejar los equipos de la exposición al sol o a temperaturas altas para evitar daños en los mismos.
- No ubicarlos en el suelo o piso de la empresa.
- Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida. Y adoptar controles adecuados para minimizar el riesgo de amenazas potenciales, por: robo o hurto, incendio, explosivos, humo, inundaciones o filtraciones de agua (o falta de suministro), polvo, vibraciones, efectos químicos, interferencia en el suministro de energía eléctrica (cortes de suministro, variación de tensión), radiación electromagnética, derrumbes.

PSI 06.2.2 Seguridad en el cableado

El cableado de la empresa debe ser instalado y mantenido por personas calificados con el fin de garantizar su integridad. Conectores de pared no utilizados deben ser sellados y su estado debe ser formalmente notificado. Para el cableado se deben tomar las siguientes medidas de seguridad:

- Las conexiones de potencia deben tener su respectivo polo a tierra.
- El cableado de la red debe ser protegido de intercepción o daño, por ejemplo, usando canaletas que lo protejan.
- Los cables de potencia deben estar separados de acuerdo a las normas técnicas, de los de comunicaciones.
- Para el caso de conexiones muy críticas (Transporte de mucha información o aplicaciones especiales) se debe considerar el uso de fibra óptica.
- Considerar el uso de enlaces redundantes.
- Diferencias los tipos de cables de acuerdo a colores establecidos por las normas técnicas relacionadas a esta área.

PSI 06.2.3 Mantenimiento de Equipo

Se debe realizar el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

- Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del jefe de TI de la empresa. El jefe de seguridad informática

mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.

- Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
- Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
- Registrar el retiro de equipamiento de las instalaciones de la empresa para su mantenimiento. Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

PSI 06.2.4 Retiro de equipo

El equipamiento, la información y el software no serán retirados de la sede de la empresa sin autorización formal. Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos de la Institución, las que serán llevadas a cabo. El personal será puesto en conocimiento de la posibilidad de realización de dichas comprobaciones.

PSI 06.2.5 Política de escritorio y pantalla limpia

Se adopta una política de escritorios limpios para proteger documentos en papel y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo. Se aplicarán las siguientes medidas:

- Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
- Guardar bajo llave la información sensible o crítica de la empresa (preferentemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina.
- Desconectar de la red / sistema / servicio las computadoras personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso (como por ejemplo la utilización de protectores de pantalla con contraseña). Los responsables de cada área mantendrán un registro de las contraseñas o copia de las llaves de seguridad utilizadas en el sector a su cargo. Tales elementos se encontrarán protegidos en sobre cerrado o caja de seguridad para impedir accesos no autorizados, debiendo dejarse constancia de todo acceso a las mismas, y de los motivos que llevaron a tal acción.
- Proteger los puntos de recepción y envío de correo electrónico y postal y las máquinas de fax no atendidas.

PSI 07 Políticas de seguridad de las operaciones

Objetivo: velar por la eficiencia de las operaciones de los recursos tecnológicos que sirven de apoyo a los diferentes procesos de la organización.

PSI 07.1 Procedimientos y responsabilidades operacionales

PSI 07.1.1 Procedimientos de operación documentados

Se establecerán los procedimientos por parte del director de seguridad informática en donde se asignarán funciones específicas a los diferentes empleados (encargados de áreas o recursos tecnológicos) quienes deberán efectuar la operación y administración de los recursos tecnológicos con el principal fin de que los procesos operativos estén accesibles y actualizados para la ejecución de las actividades. De igual forma se velará por la eficiencia de los controles establecidos en los procesos operativos asociados a los recursos tecnológicos de las organizaciones con el principal objeto de proteger la confidencialidad, integridad y disponibilidad de la información.

PSI 07.1.2 Gestión de cambios

El director de seguridad informática es el encargado de verificar que todos los cambios en la organización que afecten la seguridad estén documentados y actualizados en los procedimientos gestionando para ello:

- Que los cambios generados por la alta gerencia sean claros y se actualicen en las áreas pertinentes por los encargados asignados a esta función.
- Que los procesos de los negocios que están directamente relacionados con las operaciones y funcionalidad que las plataformas tecnológicas brindan estén disponibles con todos los cambios actualizados y sean comunicados al personal.

- Que los cambios que se solicitan por la alta gerencia a los desarrolladores de los sistemas ya sean internos o externos se verifiquen, prueben y actualicen antes de implementarlos a manera que todo aquello que afecte la operacionalidad y la seguridad de la información este controlado.

PSI 07.1.3 Gestión de la capacidad

Las operaciones de las organizaciones se deben de monitorear y es responsabilidad del director de seguridad informática realizar las siguientes actividades para asegurar la capacidad tecnológica:

- Realizar revisiones del uso de los sistemas, su funcionalidad y su utilización efectiva al menos de forma trimestral, con el objetivo de determinar si la plataforma tecnológica es suficiente para las operaciones de la organización.
- Hacer reuniones con los gerentes de áreas críticas en la organización a fin de determinar futuros requisitos tecnológicos y si la plataforma actual cubre las necesidades futuras.
- De ser necesario la ampliación de la plataforma tecnológica de la organización gestionar dicha ampliación con la gerencia general y establecer el porqué de las necesidades de incrementarla.

PSI 07.2 Protección contra software malicioso

PSI 07.2.1 Controles contra software malicioso

La gerencia general a través de la dirección de seguridad informática proporcionará herramientas que garanticen la protección de la información y los recursos de la plataforma

tecnológica en la cual se procesa y almacena; contribuyendo con esto a evitar la divulgación y/o daño ocasionados por el contagio por medio de software malicioso, adicional proporcionara los mecanismos para generar una cultura de seguridad entre sus empleados y usuarios en general tanto internos como externos frente a los ataques de software malicioso para lo cual se definen las siguientes actividades:

- Proveer herramientas tales como sistemas antivirus, antispyware, antispam, antimalware, contribuyendo a la disminución del riesgo de contagio y así respaldar la seguridad de la información contenida y almacenada en los servidores y ordenadores de la organización.
- Asegurarse que el software antivirus posee las licencias de uso requeridas, verificando su autenticidad y brindando la posibilidad de actualización periódica de las últimas bases de datos para contrarrestar los nuevos software maliciosos que son generados y que pueden perjudicar la operación de la organización.
- Asegurarse que toda la información generada desde un ordenador hasta la que es almacenada en los servidores de la organización es escaneada por el software antivirus, incluyendo la de los servicios que están contenidos y son transmitidos a través del servicio de correos electrónicos.
- Verificar que los usuarios generales no puedan hacer cambios en la configuración del software antivirus ocasionando así falta de actualizaciones o desinstalar el software.
- Cerciorarse que los usuarios ejecutan como una actividad principal el escaneo por medio del software antivirus a los documentos que son abiertos o ejecutados por

primera vez especialmente aquellos que se encuentran en unidades de almacenamiento externos o que su procedencia es por correo electrónico.

- Establecer como acción para los usuarios que cuando detecten alguna infección por software malicioso lo notifiquen al director de seguridad informática o su personal para que implementen las medidas de control que proceden en casos de infección.

PSI 07.3 Copias de seguridad

PSI 07.3.1 Copia de seguridad de la información

El director de seguridad informática proporcionara la confiabilidad que se generan copias de respaldo y almacenamiento de la información catalogada como crítica para la organización, a través de las siguientes actividades:

- Proporcionar las herramientas necesarias para el almacenamiento periódico de la información.
- Realizar copias de seguridad de la información crítica estableciendo una periodicidad adecuada según los criterios de la organización.
- Almacenar en una ubicación diferente a las instalaciones de la organización donde realizan las operaciones los medios magnéticos que contengan las copias de la información.
- Asegurar la disponibilidad de la información a través de procedimientos que especifiquen la generación, almacenamiento, tratamiento y restauración.

- Realizar pruebas de respaldo para comprobar que en casi de ser necesario se podrá contar con la información de esta forma comprobar la integridad y posibilidad de recuperación de la información.
- Establecer el tiempo que las copias de seguridad deben de ser almacenadas y con esto no saturar la base de datos de copias, pero siempre contemplando que toda la información necesaria esté disponible en el momento que sea necesaria para no eliminar copias que en un futuro sean de utilidad.
- Identificar en conjunto con los usuarios y gerentes de áreas de la organización la información que es crítica y que por lo tanto debe de respaldarse y con esto posibilitar el almacenamiento según el nivel de clasificación de información.

PSI 08 Políticas de Seguridad de las comunicaciones

Objetivo: velar por la seguridad de la información en las redes de la empresa cuando se procesa o se transfiera información.

PSI 08.1 Gestión de seguridad de red

PSI 08.1.1 Controles de red

El director de seguridad informática deberá aplicar los controles de red necesarios para garantizar que la seguridad de las redes y las comunicaciones cumple con las necesidades del negocio. También se determinará de cada red lo siguiente:

- Elementos de la red que pueden ser accedidos.
- El procedimiento de autorización para la obtención de acceso.
- Controles para protección de la red.

PSI 08.1.2 Seguridad de los servicios de red

El jefe del departamento de informática deberá revisar los contratos con las empresas proveedoras de servicios de redes para garantizar la seguridad de la información transmitida a través de dichas redes y establecer controles para mitigar al mínimo dichos riesgos.

PSI 08.1.3 Segmentación de redes

Las redes de la empresa se dividirán como sigue a continuación:

- Red LAN.
- Red WLAN.
- Red WIFI.
- Red WAN.

- Red MAN.
- Red WMAN.
- Red PAN.
- Red SAN.

El director de seguridad informática verificara que todas las redes estén adecuadas a las operaciones que se realizan dentro de la empresa, y la seguridad de cada una de las mismas.

PSI 08.2 Transferencia de información

PSI 08.2.1 Procedimientos y políticas de transferencia de información

El director de seguridad informática asegurará la protección de la información en el momento de ser transferida o intercambiada con terceros y establecerá los procedimientos y controles necesarios para el intercambio de información; así mismo, debe ofrecer servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información, que permitan el cumplimiento del procedimiento para el intercambio de información (digital o medio magnético), con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.

PSI 08.2.2 Acuerdos de transferencia de información

Además de aplicar controles para el intercambio de información, es necesario dejar documentado un acuerdo de intercambio que permita determinar responsabilidades, notificación de la transmisión, despacho y recepción de los documentos que se entregan, el modelo de documento de acuerdo de intercambio de información será como se muestra en el ***anexo 6.***

PSI 08.2.3 Mensajes electrónicos

El director de seguridad informática velara por el uso del correo electrónico como herramienta para facilitar la comunicación entre funcionarios y terceras partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

Todos los empleados de las áreas de la empresa de las líneas de negocio y las líneas de apoyo, se les asignara una cuenta de correo electrónico empresarial.

La cuenta de correo electrónico asignada es de carácter individual; por consiguiente,

- Ningún empleado de la empresa, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.
- Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones dentro de la empresa.
- Los usuarios de correo electrónico institucional tienen prohibido él envió de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los funcionarios del instituto y el personal provisto por terceras partes.
- No es permitido el envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por la empresa y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

PSI 08.2.4 Acuerdos de confidencialidad o no divulgación

El director de seguridad informática junto con el departamento legal debe definir los modelos de Acuerdos de Confidencialidad entre la empresa y los terceros incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos. Entre los aspectos a considerar se debe incluir la prohibición de divulgar la información entregada por la empresa a los terceros con quienes se establecen estos acuerdos y la destrucción de dicha información una vez cumpla su cometido. Se debe establecer en los contratos que se establezcan con terceros, los acuerdos de confidencialidad, dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información. El modelo de dichos acuerdos de confidencialidad se presenta a en el ***anexo 7.***

PSI 09 Adquisición, desarrollo y mantenimiento de sistemas

Objetivo: asegurar que se haga un adecuado análisis e implementación de los requerimientos del software desde su diseño, ya sea interno o adquirido, que incluya garantías de validación de usuarios y datos de entrada y salida, así como de los procesos mismos, de acuerdo con la clasificación de los activos a gestionar en la herramienta.

PSI 09.1 Requisitos de seguridad de los sistemas de información

PSI 09.1.1 Análisis y especificación de requerimientos de seguridad de la información

El director de seguridad de la información junto con la dirección de TI de la empresa deben establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando requerimientos de seguridad de la información, deben definir qué información sensible puede ser eliminada de sus sistemas y solicitar que estos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos, y los requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones.

PSI 09.2 Seguridad en los procesos de desarrollo y soporte

PSI 09.2.1 Política de desarrollo seguro

La empresa deberá tener una metodología formal para el desarrollo de software de los sistemas de información de misión crítica y prioritaria, desarrollos rápidos del mismo y las actividades de mantenimiento, las cuales cumplirán con las políticas, normas, procedimientos, controles y otras convenciones estándares aplicables en el desarrollo de

sistemas. Adicionalmente, toda solicitud de modificación al software deberá contar con estudios de factibilidad y de viabilidad.

PSI 09.2.2 Procedimientos de control de cambios en sistemas

Para de minimizar los riesgos de alteración de los sistemas de información, se implementarán controles estrictos durante la implementación de cambios imponiendo el cumplimiento de procedimientos formales. Éstos garantizarán que se cumplan los procedimientos de seguridad y control, respetando la división de funciones. El jefe de seguridad informática será responsable de lo siguiente:

- Verificar que los cambios sean propuestos por usuarios autorizados y respete los términos y condiciones que surjan de la licencia de uso.
- Mantener un registro de los niveles de autorización acordados.
- Solicitar la autorización del propietario de la información, en caso de tratarse de cambios a sistemas de procesamiento de la misma. Identificar todos los elementos que requieren modificaciones (software, bases de datos, hardware).
- Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios.
- Obtener aprobación formal por parte del responsable del Área Informática para las tareas detalladas, antes que comiencen las tareas.
- Solicitar la revisión del Responsable de Seguridad Informática para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.
- Efectuar las actividades relativas al cambio en el ambiente de desarrollo.

- Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.
- Mantener un control de versiones para todas las actualizaciones de software.
- Garantizar que la implementación se llevará a cabo minimizando la discontinuidad de las actividades y sin alterar los procesos involucrados.
- Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operatoria.

PSI 09.2.3 Desarrollo subcontratado

Cuando la empresa necesite desarrollar sistemas propios el jefe de seguridad informática deberá garantizar que los desarrolladores cumplan como mínimo lo siguiente:

- Los desarrolladores deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.
- Los desarrolladores deben certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas y reconocidas en el mercado.
- Los desarrolladores deben deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.
- Los desarrolladores deben establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.

- Los desarrolladores deben asegurar que no se permitan conexiones recurrentes a los sistemas de información construidos con el mismo usuario.
- Los desarrolladores deben certificar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros.

PSI 09.2.4 Pruebas de seguridad del sistema

Las pruebas sobre el software desarrollado tanto interna como externamente deberán contemplar aspectos funcionales, de seguridad y técnicos. Adicionalmente, se incluirá una revisión exhaustiva a la documentación mínima requerida, así como la revisión de los procesos de retorno a la versión anterior. En caso que se requirieran las claves de producción para ejecutar pruebas, su inserción y mantenimiento se deberá efectuar de manera segura. Se deberá poseer un cronograma para la ejecución de las pruebas con el fin de cumplir con los compromisos institucionales acordados. Éste podrá verse afectado en su calendarización por aquellos eventos en que se tengan que atender desarrollos rápidos únicamente por exigencias mandatorios de entes superiores.

PSI 09.2.5 Pruebas de aceptación del sistema

El jefe de seguridad informática debe garantizar que, durante las pruebas de aceptación, restricciones lógicas de acceso deben asegurar que los desarrolladores no tengan acceso de actualización y que el código fuente probado no pueda ser modificado sin consentimiento escrito. Si se notara problemas, se debe documentar el problema, el desarrollador debe realizar las modificaciones apropiadas en el ambiente de desarrollo y lo entregará para volver a probarlo.

PSI 09.3 Datos de prueba

PSI 09.3.1 Protección de los datos de prueba

El director de seguridad informática protegerá los datos de prueba que se entregarán a los desarrolladores, asegurando que no revelan información confidencial de los ambientes de producción, debe certificar que la información a ser entregada a los desarrolladores para sus pruebas será enmascarada y no revelará información confidencial de los ambientes de producción y por último debe eliminar la información de los ambientes de pruebas, una vez éstas han concluido.

PSI 10 Políticas de relaciones con los proveedores

Objetivo: respaldar que la información a la cual tienen acceso los proveedores por la relación comercial, esté segura y controlada de forma efectiva.

PSI 10.1 Seguridad de la información en las relaciones con los proveedores

PSI 10.1.1 Política de seguridad de la información para las relaciones con los proveedores

Los proveedores y todos aquellos que tengan responsabilidades sobre los recursos tecnológicos de la organización (tales como recursos de procesamiento de la información, correos electrónicos, servidores, servicios de red, internet, sistemas de alarmas, sistemas biométricos de acceso a las instalaciones etc.) deben adoptar los lineamientos contenidos en el presente documento y en todos aquellos documentos relacionados con la prestación de servicios de terceros, esto con el fin de mantener la integridad y confidencialidad y asegurar la disponibilidad de la información.

El personal de la organización encargado de realizar las negociaciones, firmas de contratos y/o convenios con terceras partes son los que deben velar por la divulgación de las políticas de seguridad informática para su cumplimiento.

PSI 10.1.2 Abordar la seguridad dentro de los acuerdos con los proveedores

Es necesario incluir en los contratos de prestación de servicios de los proveedores un acuerdo que garantice la custodia de los medios de almacenamiento y documentos de la organización, en el cual se asegure que dicha información no será compartida y será resguardada de la mejor forma para que no exista posibilidad de fuga ya sea de forma dolosa o sin intensión y

que caso contrario se podrá dar por finalizada la relación comercial y que cualquier repercusión será responsabilidad del proveedor que no haya acatado las normas y políticas establecidas en este documento, para esto es necesario ver el ***anexo 8,*** en donde se brinda un ejemplo de la cláusula que debe incluir cada contrato que se celebre con proveedores críticos con los accesos a la plataforma tecnológica.

PSI 10.2 Gestión del servicio de entrega del proveedor

PSI 10.2.1 Monitoreo y revisión de los servicios del proveedor

El director de seguridad informática debe monitorear los acuerdos de confidencialidad periódicamente, el cumplimiento de ellos, así como de los servicios que brindan, para lo cual puede optar por una revisión semestral con los encargados de contratar los servicios, así como con los usuarios a través de una evaluación de proveedor en los que incluyan los aspectos a evaluar tales como:

- Calidad del servicio.
- Cantidad de servicios brindados.
- Incidencias con el servicio.
- Precio del servicio vs el mercado.
- Aspectos de mejora.
- Nivel de respuesta ante inconvenientes con el servicio.

Durante la prestación de los servicios el director de seguridad informática debe monitorear que las condiciones de comunicación son seguras, así como también el cifrado y transmisión

de información desde y hacia terceros en concordancia con los acuerdos establecidos previamente en el contrato o convenio.

PSI 10.2.2 Gestión de cambios en los servicios del proveedor

La gerencia general en coordinación con el director de seguridad informática debe administrar los cambios que surjan en el suministro de la red de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos previamente y monitoreando la adición de nuevos servicios y nuevos posibles riesgos.

PSI 11 Políticas de gestión de incidentes de seguridad de la información

Objetivo: gestionar de manera adecuada todos los incidentes en la seguridad informática para garantizar que la empresa cuenta con medidas adecuadas para minimizar los riesgos de seguridad en los sistemas de información**.**

PSI 11.1 Gestión de incidentes de seguridad de la información y mejoras

PSI 11.1.1 Procedimientos y responsabilidades

El director de seguridad informática revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de los sistemas informáticos, por medio de la realización periódica de pruebas de vulnerabilidades, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas. Estas pruebas las realizara como responsable de revisar, valorar y gestionar las vulnerabilidades técnicas encontradas en los sistemas de información. También será el encargado de diseñar los procedimientos de gestión de los incidentes que ocurran en la seguridad informática de la empresa.

PSI 11.1.2 Informar sobre los eventos de seguridad de la información

Es de carácter obligatorio para todo el personal (Fijo, Contratado), la notificación inmediata de algún problema o violación de la seguridad, del cual fuere testigo; esta notificación debe realizarse por escrito vía correo electrónico al jefe de informática, quien está en la obligación de realizar las gestiones pertinentes al caso y de ser cierta la sospecha tomar las medidas adecuadas para solucionar el incidente. Estos reportes deben incluir lo siguiente:

- Nombre de la persona que reporta el evento.
- Hora y ocurrencia del evento.

- Descripción del evento sucedido.
- Responsable de solucionar el problema.
- Descripción de la respuesta inicial ante el evento.
- Descripción de la solución del evento (si aplica).
- Hora y fecha en la que se solucionó el problema (si aplica).

PSI 11.1.3 Informar sobre las debilidades de seguridad de la información

Es responsabilidad del personal de la empresa reportar cualquier debilidad de seguridad en el sistema de la empresa, este reporte debe de realizarlo al jefe de informática ya sea por escrito o por correo electrónico y dicho reporte debe incluir como mínimo lo siguiente:

- Área donde se identificó la debilidad de seguridad.
- Nombre de la persona que reporta la debilidad de seguridad.
- Encargado del procedimiento donde se identificó la debilidad de seguridad.
- Descripción de la debilidad de seguridad identificada.
- Fecha de reporte de la debilidad de seguridad.
- Posible impacto al poseer la debilidad de la seguridad.
- Posible solución a la debilidad de seguridad identificada.

PSI 11.1.4 Evaluación y toma de decisión sobre los eventos de seguridad de la información

El director de seguridad informática debe evaluar cada incidente de seguridad para determinar el impacto que el mismo causa en la empresa, para luego proceder a:

- Aplicar un proceso disciplinario en el caso que un empleado haya cometido el incidente de manera premeditada para afectar la seguridad informática de la empresa.
- Elaborar junto con el departamento legal denuncias por la vulneración a la seguridad informática de la empresa, en el caso que un tercero haya violado la seguridad informática de la empresa de manera premeditada, para afectar el buen funcionamiento de las operaciones empresariales.
- Corregir de manera inmediata las vulnerabilidades en los sistemas informáticos de la empresa para evitar futuros incidentes de seguridad.

PSI 11.1.5 Respuesta a incidentes de seguridad de la información

Un incidente de seguridad es la ocurrencia de una situación que afecte las políticas de la información o genere falla en los controles implementados por la organización. Un incidente de seguridad es el acto intencional o no intencional que tiene una alta probabilidad de afectar las operaciones de la empresa. Por tanto, para mitigar este tipo de situaciones es necesario:

- La implementación de un plan de contingencia que incluya un análisis e identificación de la causa del incidente, comunicarse con los afectados o involucrados y reportar a la autoridad responsable de la empresa, solucionar de manera inmediata en la medida que se pueda el incidente ocurrido para regresar a la normalidad de la empresa.
- El director de seguridad informática debe clasificar los incidentes de seguridad según el grado en que afectan el normal funcionamiento de la empresa. Asegurar que se haga una adecuada evaluación del impacto en la empresa frente a los eventos relevantes, realizar planes de atención de incidentes y mejora de procesos para

aquellos eventos que resultaren críticos para la supervivencia del mismo. Estos planes deben considerar medidas técnicas y administrativas para solucionar los incidentes de manera adecuada.

PSI 11.1.6 Recolección de evidencia

Es responsabilidad del director de seguridad informática en cuanto sepa que existió una violación de la seguridad informática por parte de un empleado o tercero:

- Soportar las investigaciones sobre violaciones a la seguridad de los sistemas y presentar los informes respectivos a la Dirección Superior.
- Investigar, documentar e informar a los propietarios de la información los incidentes de seguridad tanto lógica como física.
- Realizar seguimiento a las acciones disciplinarias y legales asociadas con los incidentes de seguridad investigadas.

PSI 12 Políticas de aspectos de seguridad de la información en la gestión de la continuidad del negocio

Objetivo: proporcionar las herramientas y recursos necesarios, para que los sistemas de gestión contemplen la continuidad de la seguridad de la información, y esto permita la continuidad del negocio de la organización.

PSI 12.1 Continuidad de la seguridad de la información

PSI 12.1.1 Planeación de la continuidad de la seguridad de la información

Debido a la vulnerabilidad en el país, la organización debe de estar preparada ante situaciones de crisis o desastres, que puedan afectar la información, y continuidad del negocio por lo que a través del director de seguridad informática deberá:

- Identificar aquellas circunstancias que serán catalogadas como emergencias o desastres para la organización, los procesos y áreas críticas y determinar cómo se debe de actuar.
- Responder de manera efectiva ante catástrofes y según la magnitud y el grado de afectación procurara reestablecer las operaciones con el menor costo y perdidas posible, procurando mantener la seguridad de la información durante y posterior a dichos eventos.
- Proveer un plan de contingencia que incluya mantener canales de comunicación adecuados y efectivos con los gerentes de área, empleados claves, funcionarios, proveedores y terceras partes interesadas.

- Liderar los temas que estén relacionados con la continuidad del negocio y con la recuperación ante los posibles desastres.

PSI 12.1.2 Implementación de la continuidad de la seguridad de la información

El director de seguridad informática debe de:

- Asegurar la realización de pruebas de forma periódicas del plan de recuperación ante desastres y/o continuidad del negocio, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.
- Validar que los procedimientos de contingencia para la recuperación y el retorno a la normalidad incluyan consideraciones de seguridad de la información.
- Realizar los análisis de impacto al negocio y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.

PSI 12.2 Redundancias

PSI 12.2.1 Disponibilidad de las instalaciones de procesamiento de la información

La gerencia general propondrá la existencia de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para la organización por medio del director de seguridad informática el cual:

- Establecer los requerimientos mínimos de redundancia para los sistemas de información e información crítica para la organización.

- Evaluar y probar las soluciones de redundancia tecnológica y optar por soluciones que mejor cumplan con los requerimientos de la organización.
- Administrar las soluciones de redundancia y realizar pruebas de forma periódica para asegurar el cumplimiento de la disponibilidad de la información.

PSI 13 Políticas de cumplimiento

Objetivo: velar por la identificación, documentación y cumplimiento de manera adecuada de las obligaciones legales, estatutarias o contractuales que estén relacionadas con la seguridad de la información de aquellos requerimientos de seguridad.

PSI 13.1 Cumplimiento con requerimientos legales y contractuales

PSI 13.1.1 Identificación de la legislación aplicable y requerimientos contractuales

El director de seguridad informática en conjunto con el departamento legal o en su defecto un asesor debe de identificar, documentar y mantener actualizados los requisitos legales, reglamentarios y contractuales que sean aplicables a la organización y estén relacionados con la seguridad de la información tales como:

- Certificar que todo software que se utiliza en la organización este protegido por derechos de autor y posea licencia de uso o en su defecto asegurarse de que de no poseerla sea un software o aplicación de libre distribución y uso.
- Realizar un inventario con el software y sistemas de información que se encuentran permitidos en los ordenadores de los empleados o equipos móviles de la organización para el cumplimiento de sus actividades laborales, así como monitorear periódicamente que el software instalado corresponda únicamente al permitido según inventario.

PSI 13.1.2 Derechos de propiedad intelectual

La organización a través del director de seguridad informática debe velar por el cumplimiento de las leyes de derechos de autor y acuerdos de licenciamiento de software aplicables en el país, para lo cual es importante divulgar y enfatizar a todo nivel dentro de la organización que es

ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y que su reproducción no autorizada es una violación de ley.

PSI 13.1.3 Protección de los registros

La gerencia general es el responsable de proteger los registros que dentro de la organización se ingresan, procesan, distribuyen y transmiten contra la perdida, destrucción, falsificación, accesos o divulgación no autorizada todo esto de conformidad con las leyes, regulaciones, contratos basados en los requerimientos del negocio.

A manera de protección el director de seguridad informática proveerá un procedimiento de resguardo de información física que sea de carácter confidencial, para que cada empleado de la organización resguarde la información en un lugar seguro y así evitar la fuga de información, la cual a su vez para ser recuperada o manipulada deberá de ser entregada o utilizada solo por el personal autorizado.

PSI 13.1.4 Privacidad y protección de información identificada como personal

La organización por medio de la gerencia de tecnología y su director de seguridad informática velara por la protección de los datos personales de sus partes interesadas siendo estos: beneficiarios, clientes, proveedores y demás terceros de los cuales reciba y administre información.

Las áreas que procesan datos personales deben obtener autorización para el tratamiento de esos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la

organización, adicional asegurarse que solo personas que tengan una necesidad laboral legitima puedan tener acceso a dichos datos.

Establecer condiciones de seguridad y contractuales para todas las entidades vinculadas o aliadas que hayan sido delegadas para el tratamiento de los datos personales, velar por que toda información que se envié a través de mensajes o correos electrónicos estén acordes a las directrices técnicas y procedimientos establecidos.

Es imprescindible por parte de los empleados guardar la discreción o reserva absoluta respecto a toda aquella información de carácter personal de los empleados a todo nivel desde personal operativo hasta personal de gerencia y accionistas de la organización evitando su divulgación a menos que esto sea solicitado de ley.

PSI 13.2 Revisión de seguridad de la información

PSI 13.2.1 Revisión independiente de la seguridad de la información

La gerencia general velara por la actualización, difusión, revisión y aplicación de:

- Objetivos estratégicos.
- Objetivos de control.
- Controles.
- Políticas.
- Procesos.
- Procedimientos.

Relacionados con la seguridad de la información y estos deberán ser tratados de forma independiente y evaluados en periodos planificados a excepción de cuando por alguna circunstancia se produzcan cambios significativos que ameriten evaluar los riesgos que estos cambios puedan generar.

PSI 13.2.2 Cumplimiento de las políticas y normas de seguridad

El gerente de seguridad informática en coordinación con los gerentes de las diferentes áreas de la organización ejecutara la actividad de revisar periódicamente el cumplimiento de los procedimientos y normas para el manejo y procesamiento de la información de acuerdo a las políticas de seguridad establecidas en el presente documento, así como las normas y otros requerimientos adicionales que establezcan leyes o reglamentos aplicables en el país relacionados con la seguridad.

PSI 13.2.3 Revisión de cumplimiento técnico

El director de seguridad informática solicitara periódicamente con previa autorización de la gerencia general auditorías a los sistemas de información para velar por su integridad y asegurar que estos cumplen con las normas y políticas de seguridad de la información de la organización.

F. _____

ELABORADO POR:

DIRECTOR DE SEGURIDAD INFORMÁTICA EMPRESARIAL

F._____

REVISADO POR:

DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN EMPRESARIAL

F._____

APROBADO POR:

GERENTE GENERAL

LUGAR Y FECHA: _____

CONCLUSIONES

1. La seguridad informática en las empresas del sector logístico y transporte de carga muestra vulnerabilidad y/o riesgos, esto producto a que la normativa con la que cuentan, no está basada en criterios técnicos o estándares internacionales especializados en el tema; algunas de las prácticas de seguridad implementadas, son producto de exigencias de las empresas internacionales que representan o a solicitud de la casa matriz, adicional los hackers están al asecho para provocar perdida de información, así como fallos en los sistemas de información que interfieran en las operaciones de las empresas del sector.
2. Los principales riesgos detectados en los sistemas de información son la falta de control para: las conexiones remotas de los empleados, acceso a las instalaciones, riesgos ambientales, medidas de seguridad física, infecciones de virus, almacenamiento, dispositivos móviles y correo spoofing,
3. La aplicación de políticas de seguridad informática para minimizar o eliminar los riesgos en las empresas del sector, son fundamentales para la continuidad del negocio, competitividad en el mercado de logística, ampliación de mercado, incremento de su rentabilidad, ampliación de recursos, mejora en el control de su información y de las partes interesadas.
4. La seguridad informática para los contadores públicos, gerentes financieros y auditores es crucial por lo que es importante estén a la vanguardia de los avances tecnológicos, ya que esto les permite mantener la información de la organización (clientes, proveedores, empleados) segura ante cualquier intento de sustracción o robo cumpliendo así con los objetivos de la gerencia general y con el propósito de su trabajo.

RECOMENDACIONES

Después de realizada la investigación, se recomienda lo siguiente:

1. A las empresas del sector de logística y transporte de carga, fortalecer la seguridad informática para lo cual optar por asistencia técnica para la elaboración, aprobación e implantación, de políticas fundamentadas en estándares internacionales; como lo es la Norma Técnica Salvadoreña ISO/IEC 27001:2013 "Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requerimientos".
2. A los encargados de TI de las empresas del sector, establecer programas de mejora continua para la seguridad informática y con eso mantener en constante actualización al personal de la empresa, tomando en consideración los principales riesgos detectados, además los diferentes métodos aplicados para garantizar la seguridad informática, identificar nuevas vulnerabilidades según la expansión de las tecnologías y necesidades de sistemas o aplicaciones requeridas en las organizaciones.
3. A las empresas del sector de logística y transporte de carga mantenerse a la vanguardia de tecnología, que le permita optimizar sus procesos operativos y administrativos, así como la satisfacción del cliente como base principal de su desarrollo y crecimiento, para cumplir con los objetivos estratégicos y metas planteadas por la organización, tomando en cuenta que cada mejora o implementación de nuevas plataformas implican nuevos riesgos que deben evaluarse y controlarse.
4. A los profesionales de la contaduría pública ampliar sus conocimientos en Tecnologías de la Información, ya que actualmente es una exigencia técnica de la Federación Internacional de Contadores (IFAC), con el fin de ampliar su portafolio de servicios profesionales y mejora de su competencia y credibilidad ante las empresas que lo contratan.

BIBLIOGRAFÍA

Asamblea Legislativa de El Salvador . (16 de agosto de 1993). Ley de propiedad intelectual. SAN SALVADOR, EL SALVADOR : DIARIO OFICIAL N° 150 TOMO 320.

Asamblea Legislativa de El Salvador. (26 de febrero de 2016). Ley especial contra los delitos informáticos y conexos. SAN SALVADOR , EL SALVADOR : Diario oficial N° 40, TOMO 410.

Banco Central de Reserva. (2016). INFORME DE SITUACION ECONOMICA 2016-02. *INFORME DE SITUACION ECONOMICA* , 23. Obtenido de http://www.bcr.gob.sv/bcrsite/uploaded/content/category/741629262.pdf

CASTRO, E. E.-E. (Junio de 2011). LA GESTIÓN DE LAS CADENAS LOGÍSTICAS EN EL SALVADOR BAJO LA PERSPECTIVA DE LA LEY DE SERVICIOS INTERNACIONALES. Santa Ana, El Salvador.

CEPA. (2010). *www.cepa.gob.sv*. Recuperado el 20 de febrero de 2017, de http://www.cepa.gob.sv/historia

COMCA EL SALVADOR. (2012). *COMCA Internacional*. Recuperado el 23 de junio de 2017, de COMCA Internacional: http://www.comca.com.sv

Crowley Maritime Corporation. (2017). *CROWLEY*. Recuperado el 03 de mayo de 2017, de CROWLEY: http://www.crowley.com

DHL. (2007). *DHL EL SALVADOR*. Recuperado el 12 de marzo de 2017, de DHL EL SALVADOR: http://www.dhl.com.sv

EL DIARIO DE HOY [EDH]. (05 de octubre de 2015). *elsalvador.com*. Recuperado el 25 de marzo de 2017, de elsalvador.com: http://www.elsalvador.com/noticias/negocios/165845/robo-de-informacion-dana-gestion-de-empresas-en-el-salvador/

ELDIARIO ES. (2012). *EL DIARIO.ES*. Recuperado el 15 de febrero de 2017, de EL DIARIO.ES: http://www.eldiario.es/que_es/

Entonado, F. B. (2001). *SOCIEDAD DE LA INFORMACION Y EDUCACION.* Mérida: JAVIER FELIPE S.L. (Producciones & Diseño).

Guzmán, F. F. (1 de julio de 2011). *El Reservado.es*. Recuperado el 30 de marzo de 2017, de El Reservado.es: http://www.elreservado.es/news/view/220-noticias-espias/1363-operacion-anti-security

ISACA. (2012). *COBIT 5 PROCESOS CATALIZADORES.* ESTADOS UNIDOS: ISACA. Recuperado el 12 de mayo de 2017

LA PAGINA. (11 de Noviembre de 2011). *Diario La Pagina*. Recuperado el 15 de marzo de 2017, de Diario La Pagina: http://www.lapagina.com.sv/nacionales/58230/2011/11/06/Gobierno-confirma-ataque-de-hackers-a-sitios-web-oficiales

MAERSK. (2017). *MAERSK LINE*. Recuperado el 06 de julio de 2017, de MAERSK LINE: http://app.communication.maerskline.com/e/es?s=754438491&e=376473&elq=d56db1f0bc634

158853da5ec397b844c&elq=~~eloqua..type--emailfield..syntax--recipientid~~&elqCampaignId=~~eloqua..type--campaign..campaignid--0..fieldname--id~~&elqaid=~~eloqua..type--emai

MAERSK. (2017). *MAERSK LINE*. Recuperado el 27 de junio de 2017, de MAERSK LINE: http://app.communication.maerskline.com/e/es?s=754438491&e=372775&elq=f21bed4744284b51b525532e32bd1c34&elq=~~eloqua..type--emailfield..syntax--recipientid~~&elqCampaignId=~~eloqua..type--campaign..campaignid--0..fieldname--id~~&elqaid=~~eloqua..type--emai

MUDISA, S.A. DE C.V. (2005). *MUDISA*. Recuperado el 15 de febrero de 2017, de MUSIDA: http://www.mudisa.com.sv

NTS ISO/IEC 27001. (2013). NTS ISO/IEC 27001:2013.

NTS ISO/IEC 27001. (2013). NTS ISO/IEC 27001:2013. OSN. Recuperado el 15 de junio de 2017, de ISO 27000.ES: http://www.iso27000.es/sgsi.html

Organismo Salvadoreño de Normalización [OSN]. (24 de marzo de 2015). *Organismo Salvadoreño de Normalización*. Obtenido de Organismo Salvadoreño de Normalización: http://www.osn.gob.sv/index.php?option=com_k2&view=item&id=113:osn-realiza-evento-de-difusi%C3%B3n-de-normas-en-tecnolog%C3%ADa-de-la-informaci%C3%B3n&Itemid=79

PROESA (Productor), & Comunicaciones, P. (Dirección). (2013). *El Salvador Logístico: Corazón de Las Américas* [Película]. El Salvador. Recuperado el 15 de abril de 2017, de https://www.youtube.com/watch?v=lhtLeFfELBI&t=404s

RANSA. (2017). *RANSA EL SALVADOR*. Recuperado el 15 de junio de 2017, de RANSA EL SALVADOR: https://www.ransa.biz/es-PE/elsalvador/

WikiLeaks. (11 de abril de 2010). *wikileaks.org*. Recuperado el 02 de junio de 2017, de wikileaks.org: https://wikileaks.org/wiki/Talk:Wikileaks/es

ANEXOS

ANEXO 1

Listado de empresas del sector de logística y transporte de carga del municipio de Antiguo Cuscatlán

No.	Empresa	Rubro	Dirección	Teléfono	Contacto	Email	página web
1	Aimar S.A. de C.V.	Agencia de Carga	Zona Franca Santa Tecla	2209-7951	Daniel Crespín	dcrespin@aimargroup.com	www.aimargroup.com
2	Transportemos S.A. de C.V.	Agencia de Carga	Blvd Acero No. 12-A Centro Logístico, Antiguo Cuscatlán, La Libertad	2250-9300	Mónica Guevara	mguevara@comca.com.sv	www.comca.com.sv
3	Transportes Sebastián S.A. de C.V.	Agencia de Carga	Urb. Industrial Plan de La Laguna, Edificio Transebastian, Lote # 1., Antiguo Cuscatlán	2523-6400	Rodrigo Huezo	rhuezo@gruporemor.com.sv	www.transebastian.com
4	Codotrans S.A. de C.V.	Agencia de Carga	Calle llama del bosque poniente urbanización Madre Selva III etapa Edificio Avante 7-11, Antiguo Cuscatlán	2241-8080	Oscar Valladares	oscar.valladares@codotrans.com	www.codotrans.com
5	Hermes S.A. de C.V.	Agencia de Carga	Blvd Acero No. 12-A Centro Logístico, Antiguo Cuscatlán, La Libertad	2250-9300	Yenci Arias	yarias@hermes.com.sv	www.hermes.com.sv
6	Corporación Oceánica S.A. de C.V.	Agencia de Carga	Col Lomas de San Fco Av Albert Einstein Edif Construmarket 1er Nivel Loc 1-5 Antiguo Cuscatlán	2121-2900	Katia Pérez	kperez@oceanica.wz	www.oceanworldlines.com
7	CAN Logistics	Agencia de Carga	Blvd Acero No. 12-A Centro Logístico, Antiguo Cuscatlán, La Libertad	2250-9300	Carlos Menéndez	cmenendez@canregional.com	www.canregional.com
8	Mudanzas Internacionales S.A. de C.V.	Agencia de Carga	Z Industrial Sta Elena Cl Chaparrastique No 34 , Antiguo Cuscatlán	2210-3200	Oscar Martínez	mudisa@mudisa.com.sv	www.mudisa.com.sv
9	Triton Logistics S.A. de C.V.	Naviera	Blvd Acero No. 12-A Centro Logístico, Antiguo Cuscatlán, La Libertad	2250-9390	Norma Hernández	marketing@trilog.com.sv	www.trilog.com.sv
10	Argus Logistics S.A. de C.V.	Agencia de Carga	Blvd Acero No. 12-A Centro Logístico, Antiguo Cuscatlán, La Libertad	2250-9300	Steve Mangandi	smangandi@arlog.com.sv	www.arlog.com.sv
11	Carga Global S.A. de C.V.	Agencia de Carga	Residencial Cumbres de La Esmeralda, Calle Xochilt Polígono C2 No 2, Antiguo Cuscatlán, La Libertad.	2556-1300	Miriam Siciliano	msicilianosal@cargaglobal.com	www.cargaglobal.com
12	Blanco Logistics Incoporated S.A. de C.V.	Agencia de Carga	Col. Jardines de San Francisco, Av. Los Laureles, No. 7, Antiguo Cuscatlán,	2273-0426	Carlos Guillen	operaciones@blielsalvador.com	

13	Sia Consolidadores S.A. de C.V.	Agencia de Carga	Centro comercial ATRIUM, primer nivel, local #7 Santa Elena, Antiguo Cuscatlán	2110-6060	Daniel Calderón	infosia@siaconso.com	www.siaconsolidadores.com
14	Zim Integrated Shipping Service	Naviera	Blvd Acero No. 12-A Centro Logístico, Antiguo Cuscatlán, La Libertad	2250-9394	Norma Hernández	hernandez.norma@sv.zim.com	www.zim.com
15	Sistemas Aéreos S.A. de C.V.	Agencia de Carga	Calle llama del bosque poniente urbanización Madre Selva III etapa Edificio Avante 7-8, Antiguo Cuscatlán	2500-4077	Erick Renderos	erenderos@americalogisticsgroup.com	www.sistemasaereos.com
16	Ransa S.A. de C.V.	Almacenadora	Blvd Bayer Cl L-1 No 44-C Cdad Merliot	2244-1500	Hugo Rafael	hmendozam@ransa.net	www.ransa.net
17	Flomar de El Salvador S.A. de C.V.	Agencia de Carga	Residencial Cumbres de La Esmeralda, Calle Teotl Polígono E8 No 19, Antiguo Cuscatlán, La Libertad.	2252-5468	Alcides Martínez	info@flomartransport.com	www.flomartransport.com
18	Hamburg Sud El Salvador	Naviera	Urbanización Madre Selva #3, Calle Llama del Bosque Poniente, Pasaje S, Lote 15 y 17 Edificio Avante, Oficina 9-06 Santa Elena	2133-9200	Danny Moran	Danny.Moran@hamburgsud.com	www.hamburgsud-line.com
19	Rex Cargo de El Salvador S.A. de C.V.	Agencia de Carga	Edificio Eben Ezer, Boulevard Sur Santa Elena	2563-4514	Osvaldo García	salimport@rexcargo.com	www.rexcargo.com
20	Transportes CLT S.A. de C.V.	Transporte de carga	Blvd Santa Elena, Calle Llama del Bosque pasaje S, Edificio Valencia 4to nivel, Antiguo Cuscatlán	2563-4524	Carlos Bodewig	carlos.bodewig@clt.com.sv	www.clt.com.sv

Anexo 2

Encuesta dirigida a los jefes de informática de las empresas del sector de logística y transporte de carga del municipio de Antiguo Cuscatlán

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE CONTADURÍA PÚBLICA
(Encuesta de uso didáctico)

Proyecto de investigación: Políticas de seguridad informática para empresas del sector de logística y transporte de carga del municipio de Antiguo Cuscatlán, basadas en la Norma Técnica Salvadoreña ISO/IEC 27001:2013.
Dirigida a: los jefes o encargados del área de sistemas informáticos de las empresas del sector de logística y transporte de carga del municipio de Antiguo Cuscatlán.
Objetivo de la encuesta: Conocer si las empresas del sector de logística y transporte de carga del municipio de Antiguo Cuscatlán, cuenta con políticas de seguridad informática que gestionen adecuadamente los riesgos en los sistemas de información.
Indicaciones: encierre en un círculo las respuestas que más se apeguen a su realidad, en las preguntas de opción múltiple puede elegir más de una opción.

I. A.6 Dispositivos móviles y trabajo remoto

1. ¿La empresa permite la conexión de dispositivos móviles (smartphone, laptop, tablet) a las redes internas (intranet, internet, WLAN, VPN)? ***(Ref. A.6.1 dispositivos móviles y trabajo remoto; DSS05.02)***

   A. SÍ

   B. NO

Objetivo: conocer si las redes de conexión de la empresa pueden tener riesgos debido a los aparatos móviles que se conectan y no cumplen con protocolos de seguridad.

2. Si la empresa permite la conexión de dispositivos móviles a sus redes internas, ¿Cuáles son las medidas de seguridad que aplican en estos casos? ***(Ref. A.6.1 dispositivos móviles y trabajo remoto; DSS05.02)***

A. Permite sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa.
B. Configura estos dispositivos para forzar la solicitud de contraseña.
C. Implementa mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.
D. Cifra la información en tránsito de acuerdo con su clasificación.
E. Realiza pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.
F. No se aplica ninguna.

Objetivo: verificar si la empresa implementa protocolos de seguridad para las conexiones de dispositivos móviles.

3. ¿Cuáles de los siguientes controles aplica la empresa a los empleados que trabajan de forma remota y fuera de las instalaciones de la empresa? ***(Ref. A.6.2 dispositivos móviles y trabajo remoto)***
    A. Validación de datos.
    B. Software antivirus en las unidades externas.
    C. Accesos restringidos desde IP externa.
    D. Asignación de ID únicos para establecer responsabilidades.
    E. Monitoreo de la información que se genera.
    F. Bloqueo de impresión de documentos y/o almacenamiento en unidades externas.
    G. No aplicamos ninguna.
    H. No se permite el trabajo de forma remota

Objetivo: Evidenciar la aplicación de al menos una medida de seguridad para las conexiones de usuarios en forma remota.

II. A.7 Términos y condiciones de empleo

4. Cuando se contrata a un nuevo empleado; ¿se incluye una cláusula de confidencialidad en su contrato para garantizar la seguridad de la información? ***(ref. A.7.1.2 términos y condiciones de empleo)***
    A. SÍ
    B. NO

Objetivo: verificar que la empresa cuenta con herramientas legales ante cualquier fuga de información confidencial por parte de un empleado.

III. A.8 Gestión de activos

5. De las siguientes medidas de seguridad; ¿Cuáles aplica la empresa para el uso adecuado de los activos informáticos? ***(ref. A.8 Gestión de activos)***
    A. Los empleados devuelven los activos informáticos al finalizar su contrato de trabajo.
    B. Se asignan activos informáticos de acuerdo a las funciones de cada empleado.
    C. No se permite a los empleados el uso de dispositivos de almacenamiento móviles.
    D. Asigna claves de acceso único para fotocopia, impresión y escaneo.
    E. No aplica ninguna.

Objetivo: cerciorarse si los activos informáticos se usan de manera adecuada en la empresa.

IV. A.9 Control de acceso

6. ¿Cuáles son las medidas de seguridad que implementan para el acceso a las instalaciones de la empresa? ***(ref. A. 9 control de acceso)***

A. Vigilante.

B. Tarjetas de acceso.

C. Autentificación biométricos (huellas dactilares, retina, iris, patrones faciales).

D. No aplica ninguna.

Objetivo: identificar si la empresa cuenta con medidas de seguridad y cuáles son las más utilizadas.

7. ¿La empresa cuenta con una política que restrinja el acceso a la información y a funcionalidades de los sistemas de información por parte de usurarios indebidos***? (Ref. A.9.4 control de acceso a sistemas y aplicaciones)***

   A. SÍ

   B. NO

Objetivo: comprobar que en la empresa se hayan definido los atributos que cada usuario puede tener según su perfil de puesto o actividades que desarrollara.

V. A.11 seguridad física y ambiental

8. Los equipos informáticos de la empresa ¿están protegidos contra los siguientes riesgos ambientales? ***(Ref. A.11.1.4 protección contra amenazas externas y ambientales)***

   A. Humedad.

   B. Polvo.

   C. Sobrecarga o ausencia de energía eléctrica.

   D. Luz solar.

   E. No posee ninguna.

Objetivo: determinar si existen controles que ayuden a disminuir posibles daños en los equipos informáticos.

9. ¿La empresa cuenta con las siguientes medidas de seguridad física? ***(ref. a.11 seguridad física y ambiental)***

    A. Cámaras de video vigilancia.

    B. Alarma contra incendios.

    C. Alarma contra robos.

    D. Planta eléctrica.

    E. Rutas de evacuación en caso de siniestros.

    F. Extintores de fuego y equipo respiratorio.

    G. Cables debidamente protegidos.

    H. Aires acondicionados o ventilación adecuada.

    I. UPS en cada computadora.

    J. Controles de acceso a las instalaciones.

    K. Acceso controlado de visitas.

    L. Mantenimiento correctivo y preventivo de los equipos informáticos.

    M. No cuenta con ninguna.

Objetivo: Verificar que la empresa cuenta con herramientas que le permitan mantener la seguridad para sus empleados y sistemas informáticos.

VI. A.12 Seguridad de las operaciones

10. ¿Realiza copias de seguridad de toda la información sensible de la empresa? ***(ref. A. 12.3.1 Copias de seguridad)***

    A. SÍ

    B. NO

Objetivo: comprobar que la empresa realiza backups de su información manteniéndola segura y accesible en cualquier momento.

11. Si realiza copias de seguridad de seguridad de la información ¿Cuál es la frecuencia con la cual lo realiza? ***(ref. A. 12.3.1 Copias de seguridad)***

    A. Diario.

    B. Semanal.

    C. Mensual.

    D. Trimestral.

    E. Semestral.

    F. Anual.

Objetivo: cerciorarse que la información está siendo resguardada en forma oportuna.

12. ¿La empresa cuenta con un software antivirus para la detección y prevención de los ataques de software maliciosos? ***(ref. A.12.2.1 controles contra software maliciosos; SS05.01 Proteger contra software malicioso.***)

    A. SI

    B. NO

    Mencione el nombre del software: _____

Objetivo: determinar si las organizaciones cuentan con herramientas que le ayude a evitar pérdida o fuga de información.

VII. A.13 Seguridad de las comunicaciones

13. ¿cuáles de las siguientes medidas aplican en la empresa para garantizar la seguridad de la información generada por los sistemas? ***(ref. A.13.2 transferencia de información***)

A. Autentificación de usuarios (Contraseñas).

B. Control de acceso a los datos.

C. Encriptación de datos sensibles o confidenciales.

D. Socialización a los usuarios de normas o políticas de seguridad Informática.

E. Actualización de Software.

F. Validación de datos.

G. Software antivirus.

H. No aplicamos ninguna medida.

Objetivo: Determinar si dentro de la empresa aplican medidas de seguridad para evitar fuga de información.

14. ¿Cuáles de las siguientes características utiliza la empresa para autentificar las contraseñas de usuario? ***(DSS05.02 gestionar la seguridad de las redes y conexiones)***

    A. Asignación de ID únicos para establecer responsabilidades.

    B. Técnicas de cifrado.

    C. Bloqueo de accesos por intentos fallidos.

    D. Cambio de contraseña cada determinado periodo.

    E. No se utiliza ninguna.

Objetivo: comprobar que las contraseñas no sean fácil de identificar por otros usuarios y que puedan utilizarlas con fines de acceso a información que no corresponda a sus perfiles.

VIII. A.16 Gestión de incidentes de seguridad de la información

15. ¿Ha sufrido la empresa ataques informáticos los últimos 3 años? ***(A.16.1.3 Informar sobre debilidades de seguridad de la información)***

    A. SI

B. NO

Objetivo: Verificar si la empresa ha tenido incidencias de pérdida o fuga de información.

16. De los ataques informáticos sufridos por la empresa ¿Cuáles fueron las causantes del ataque? ***(A.16.1.4 evaluación y toma de decisión sobre los eventos de seguridad de la información)***

    A. Ataques de hackers.
    B. Uso inadecuado de internet.
    C. Modificación de mensajes.
    D. Acceso no autorizado (áreas físicas).
    E. Correo spoofing (remitentes falsos).
    F. Virus informáticos.
    G. Ataque interno de empleados.
    H. Puertos USB abiertos.
    I. Utilización de claves y usuarios de otros empleados.

Objetivo: Identificar las principales razones de un ataque informático en las organizaciones

17. De los ataques informáticos sufridos por la empresa ¿Cuáles fueron las consecuencias del ataque? ***(A.16.1.6 aprendizaje de los incidentes de seguridad de la información)***

    A. Robo de contraseñas.
    B. Infiltración a los sistemas informáticos.
    C. Perdidas económicas.
    D. Acceso a costos y planes estratégicos de la compañía.
    E. Atraso en las operaciones del negocio.
    F. Pérdida de credibilidad ante terceros.

G. Modificación de datos en los sistemas informáticos.

H. Otras.

Objetivo: Verificar el impacto de los ataques sufridos en las empresas.

IX. Políticas se seguridad informática basadas en NTS ISO/IEC 27001:2013

18. ¿Considera que la aplicación de políticas de seguridad informática le ayudaría a la empresa a proteger la información y generar credibilidad y confianza ante terceros?

    A. SÍ

    B. NO

Objetivo: comprobar la necesidad de políticas que ayuden a las empresas del sector de logística y transporte de carga a salvaguardar la información.

19. ¿Cree que la empresa estaría interesada en aplicar políticas de seguridad informática basadas en la Norma Técnica Salvadoreña ISO/IEC 27001:2013?

    A. SÍ

    B. NO

Objetivo: verificar la oportunidad de proponer políticas para la protección de la información y el uso que las empresas le podrían dar.

ANEXO 3

Análisis e interpretación de los resultados

Pregunta 1

¿La empresa permite la conexión de dispositivos móviles (smartphone, laptop, tablet) a las redes internas (intranet, internet, WLAN, VPN)? ***(Ref. A.6.1 dispositivos móviles y trabajo remoto; DSS05.02)***

Objetivo: conocer si las redes de conexión de la empresa pueden tener riesgos debido a los aparatos móviles que se conectan y no cumplen con protocolos de seguridad.

Tabla No. 1

Permisibilidad de conexión de dispositivos móviles

Opciones	Frecuencia	Porcentaje
SI	14	70.00%
NO	6	30.00%
Total encuestados 20	20	100.00%

Grafico No.1

Permisibilidad de conexión de dispositivos móviles

Análisis: Los avances tecnológicos como parte de las herramientas esenciales de las comunicaciones, la globalización y la expansión del comercio internacional y las negociaciones

con empresas internacionales hace de las conexiones remotas una necesidad para la mayoría de empresas del sector de logística debido a que estas representan empresas multinacionales y con esto la visita de personas tanto clientes, como compañeros de trabajo de oficinas de otros países o sucursales requieren las conexiones de dispositivos móviles como laptops y teléfonos a la redes internas, en esta ocasión el 70% (14) de las empresas encuestadas confirmaron que permiten la conectividad de personas externas a sus redes.

Pregunta 2

Si la empresa permite la conexión de dispositivos móviles a sus redes internas, ¿Cuáles son las medidas de seguridad que aplican en estos casos? ***(Ref. A.6.1 dispositivos móviles y trabajo remoto; DSS05.02)***

Objetivo: verificar si la empresa implementa protocolos de seguridad para las conexiones de dispositivos móviles.

Tabla No. 2

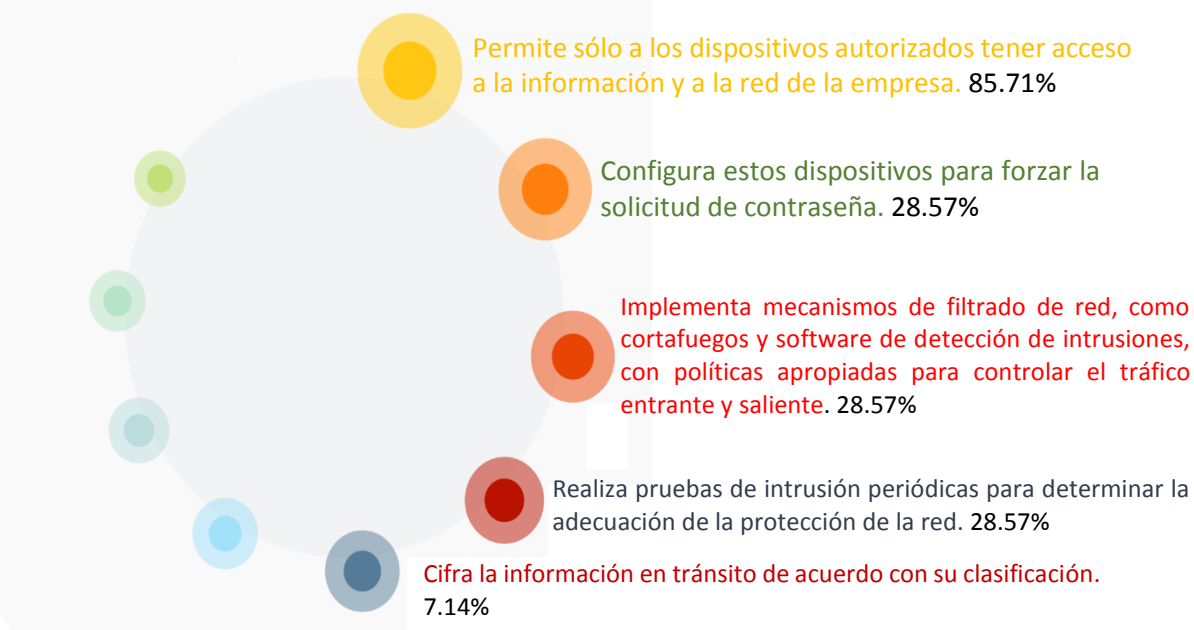
Medidas de seguridad para la conexión de dispositivos móviles a redes internas (selección múltiple)

Opciones	Frecuencia	Porcentaje
Permite sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa.	12	85.71%
Configura estos dispositivos para forzar la solicitud de contraseña.	4	28.57%
Implementa mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.	4	28.57%
Realiza pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.	4	28.57%
Cifra la información en tránsito de acuerdo con su clasificación.	1	7.14%
No se aplica ninguna.	0	0.00%

Total encuestados 14

Grafico No.2

Medidas de seguridad para la conexión de dispositivos móviles a redes internas



Análisis: Ante la necesidad de la conexión de dispositivos móviles se ha evaluado cuales son las principales medidas de seguridad que utilizan las empresas del sector de la logística de carga debido a que siempre será necesario permitir el acceso a usuarios externos a sus redes, la principal medida es que permiten el acceso solo a los dispositivos autorizados a tener acceso a la red de la empresa ya que el 86% aplican esta medida, en segundo lugar configurar estos dispositivos para forzar la solicitud de contraseña, políticas apropiadas para controlar el tráfico entrante y saliente así como realizar pruebas de intrusión periódicas las 3 medidas con un 29%, dejando en último lugar el cifrar la información en tránsito de acuerdo con su clasificación ya que solo el 7% de las 14 empresas que respondieron a esta pregunta (que son las q permiten el acceso a sus redes con dispositivos móviles) aplican esa medida, ante esto se puede observar que no se está aplicando la mejor medida de protección ya que cualquier usuario autorizado puede substraer, compartir, copiar o eliminar información de las redes o inclusive insertar algún virus a la red local; a pesar de que

todas las empresas aplican una medida de seguridad las que obtiene el mayor índice son las menos efectivas.

Pregunta 3

¿Cuáles de los siguientes controles aplica la empresa a los empleados que trabajan de forma remota y fuera de las instalaciones de la empresa? ***(Ref. A.6.2 dispositivos móviles y trabajo remoto)***

Objetivo: Evidenciar la aplicación de al menos una medida de seguridad para las conexiones de usuarios en forma remota.

Tabla No.3

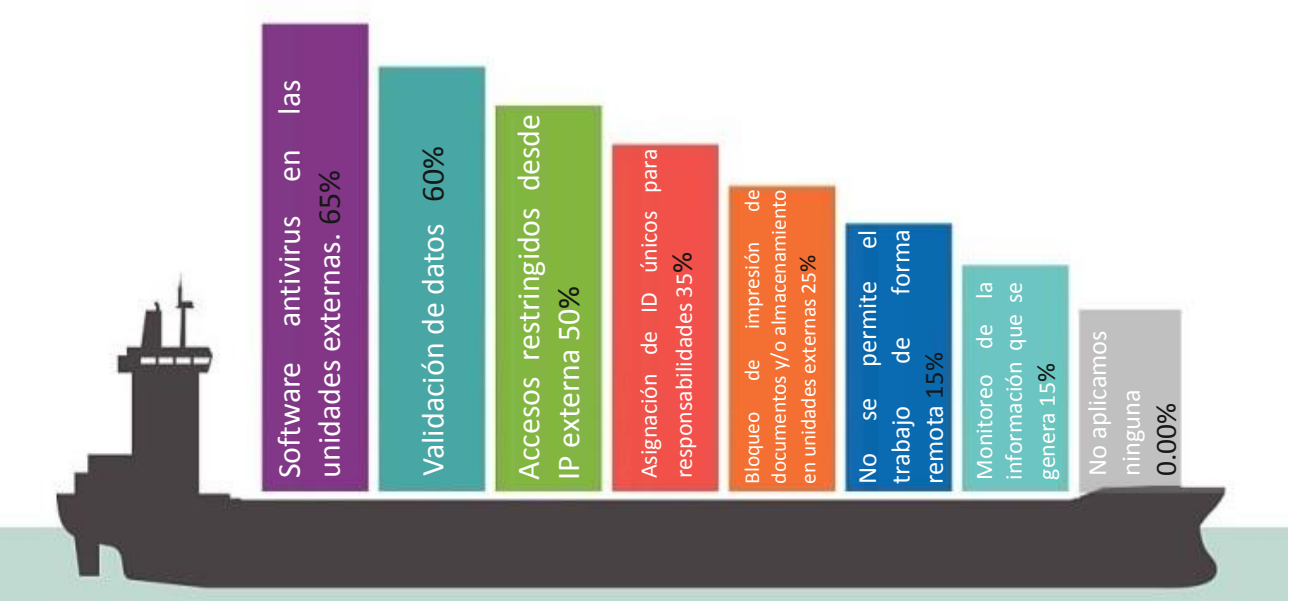
Controles para trabajos de forma remota fuera de las instalaciones de la empresa (selección múltiple)

Opciones	Frecuencia	Porcentaje
Software antivirus en las unidades externas	13	65.00%
Validación de datos	12	60.00%
Accesos restringidos desde IP externa	10	50.00%
Asignación de ID únicos para establecer responsabilidades	7	35.00%
Bloqueo de impresión de documentos y/o almacenamiento en unidades externas	5	25.00%
Monitoreo de la información que se genera	3	15.00%
No se permite el trabajo de forma remota	3	15.00%
No aplicamos ninguna	0	0.00%

Total encuestados 20

Grafico No.3

Controles para trabajos de forma remota fuera de las instalaciones de la empresa



Análisis: Los servicios que las empresas de logística de carga y transporte ofrecen a sus clientes son 24/7 dado que siempre hay carga en movimiento, tanto marítima, aérea y terrestre, ya que siempre hay barcos en tránsito y en operación en todas las partes del mundo así como aviones operando en diferentes aeropuertos y camiones o tráiler en movimiento de una frontera o país a otro; adicional a esto los cambios de horario entre regiones como Asia y América posibilitan que mientras unas personas han salido de su horario normal de trabajo otros inicien su jornada, ante esto la necesidad de trabajos de forma remota desde una computadora portátil o un celular es algo que es fundamental para mantener una alta competitividad y un servicio de calidad es por ello que existe la necesidad de tomar las medidas pertinentes. Las 20 empresas encuestadas han determinado como principal herramienta el uso de un software antivirus (65%), la validación de datos es decir uso de claves de acceso en 2do lugar (60%), el acceso restringido solo a IP autorizadas en tercer lugar (50%) y a pesar de que todas utilizan una medida de seguridad notamos que las principales medidas de seguridad son utilizadas muy poco tales como asignación de ID

únicos (35%) bloqueo de impresión de documentos externamente (25%) y monitoreo de la información que se genera externamente (15%), adicional a esto el 15% es decir 3 de las empresas encuestadas no permite el acceso de forma remota por lo que su competitividad es baja en una industria dinámica y que necesita comunicación fluida.

Pregunta 4

Cuando se contrata a un nuevo empleado; ¿se incluye una cláusula de confidencialidad en su contrato para garantizar la seguridad de la información? ***(ref. A.7.1.2 términos y condiciones de empleo)***

Objetivo: verificar que la empresa cuenta con herramientas legales ante cualquier fuga de información confidencial por parte de un empleado.

Tabla No.4

Cláusula de confidencialidad en contrato de trabajo.

Opciones	Frecuencia	Porcentaje
SI	16	80.00%
NO	4	20.00%
Total encuestados 20	20	100.00%

Grafico No.4

Cláusula de confidencialidad en contrato de trabajo.

Análisis: La confidencialidad de la información de todos los negocios así como de los embarques que manejan los empleados de estas empresas es fundamental para la continuidad del negocio ya que existe mucha información de uso exclusivo de proyectos y de carga delicada que debe de distribuirse con precaución por ejemplo la movilización de armamento o municiones que son bajo autorizaciones de la defensa nacional de cada país y que es un producto altamente delicado por la tasa de robo o hurto, productos como electrodomésticos y vehículos que también son sujetos a robos y los empleados conocen las rutas donde estas unidades transitan. Adicional existen proyectos de manejo de carga por volúmenes grandes en los cuales muchas empresas del sector licitan y ofertan a las mismas empresas interesadas en que les brinden servicio y en las que los costos de oferta son claves para obtener el negocio (la información es un activo valioso para las empresas), el divulgar costos u ofertas a la competencia sería muy grave e impactaría de forma negativa es por ello que según las respuestas obtenidas el 80% de las empresas del sector utilizan herramientas legales para disminuir la fuga de información, el 20% restante no utiliza esta herramienta por lo que estas empresas están con altos índices de probabilidades de fuga de información y dado el índice de rotación de personal entre estas empresas es mucho más probable que se compartan carteras de clientes y de proveedores.

Pregunta 5

De las siguientes medidas de seguridad; ¿Cuáles aplica la empresa para el uso adecuado de los activos informáticos? ***(ref. A.8 Gestión de activos)***

Objetivo: cerciorarse si los activos informáticos se usan de manera adecuada en la empresa.

Tabla No.5

Medidas de seguridad para el uso de los activos informáticos (selección múltiple).

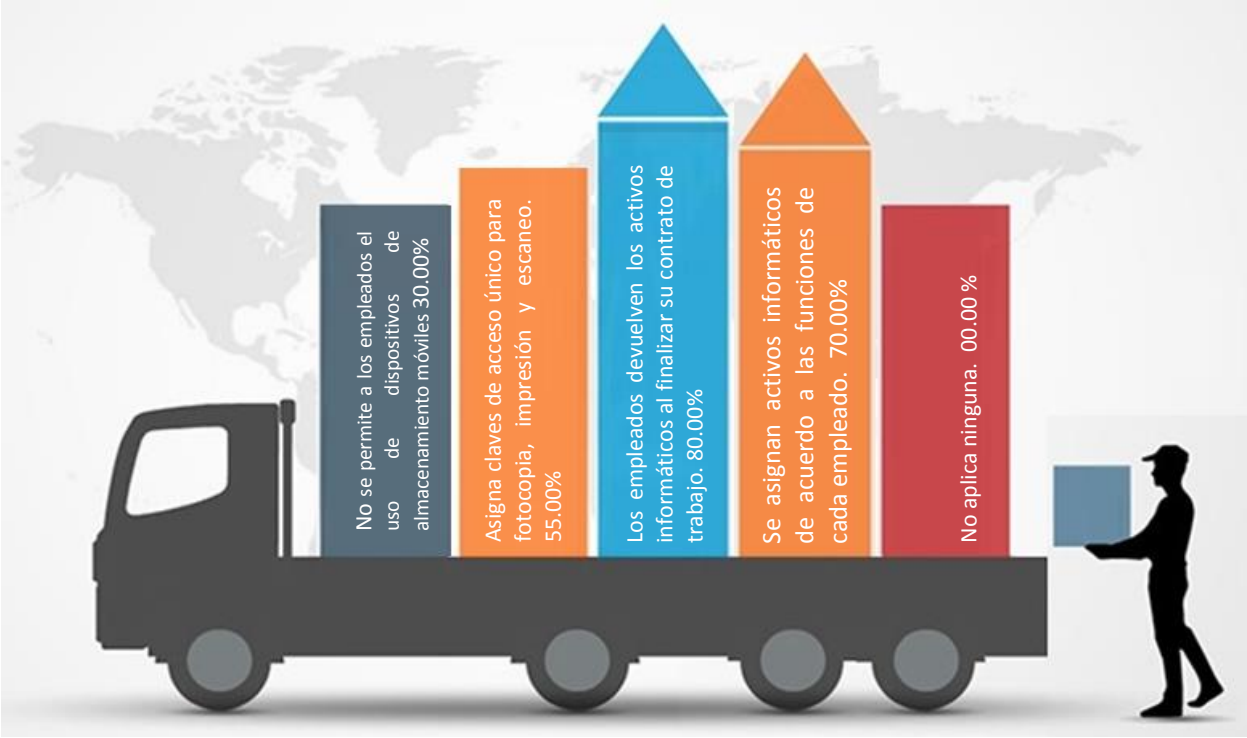
Opciones	Frecuencia	Porcentaje
Los empleados devuelven los activos informáticos al finalizar su contrato de trabajo.	16	80.00%

Se asignan activos informáticos de acuerdo a las funciones de cada empleado.	14	70.00%
Asigna claves de acceso único para fotocopia, impresión y escaneo	11	55.00%
No se permite a los empleados el uso de dispositivos de almacenamiento móviles.	6	30.00%
No aplica ninguna.	0	0.00%

Total encuestados 20

Grafico No.5

Medidas de seguridad para el uso de los activos informáticos.



Análisis: El control y resguardo de los activos informáticos es vital para el funcionamiento de los servicios y continuidad de los embarques, dentro de los activos más comunes que son utilizados por los empleados de estas empresas tenemos: Computadoras portátiles, carnets de identificación y con accesos a las áreas según sus perfiles, teléfonos móviles, scanners y lectores de barras, usuarios y claves para accesos a sistemas según su perfil; descrito todo esto es posible hacerse una idea de lo crucial de la información que cada uno de los empleados manipula, genera y distribuye

entre los diferentes departamentos o áreas por lo tanto su resguardo o correcta manipulación es crucial. De las 20 empresas encuestadas el 80% se asegura que los empleados devuelvan los activos informáticos lo cual genera un riesgo alto dado que no se verifica que todos los empleados reintegren los activos o recursos asignados, el 70% asigna los activos según los perfiles de sus empleados lo cual pone en riesgo el otorgar permisos o recursos que no son necesarios, el 55% asigna claves de acceso único a cada usuario para impresión, escaneo y fotocopias es decir existen muchos usuarios que pueden imprimir y fotocopiar documentos sin discreción y lo que ellos quieran, el 30% no permite el uso de dispositivos móviles de almacenamiento (memorias flash, SD) por lo que los demás permiten que los empleados almacenen información y la copien o distribuyan en otras áreas o computadoras personales, inclusive enviarlas por correo electrónico.

Pregunta 6

¿Cuáles son las medidas de seguridad que implementan para el acceso a las instalaciones de la empresa? ***(ref. A. 9 control de acceso)***

Objetivo: identificar si la empresa cuenta con medidas de seguridad y cuáles son las más utilizadas.

Tabla No.6

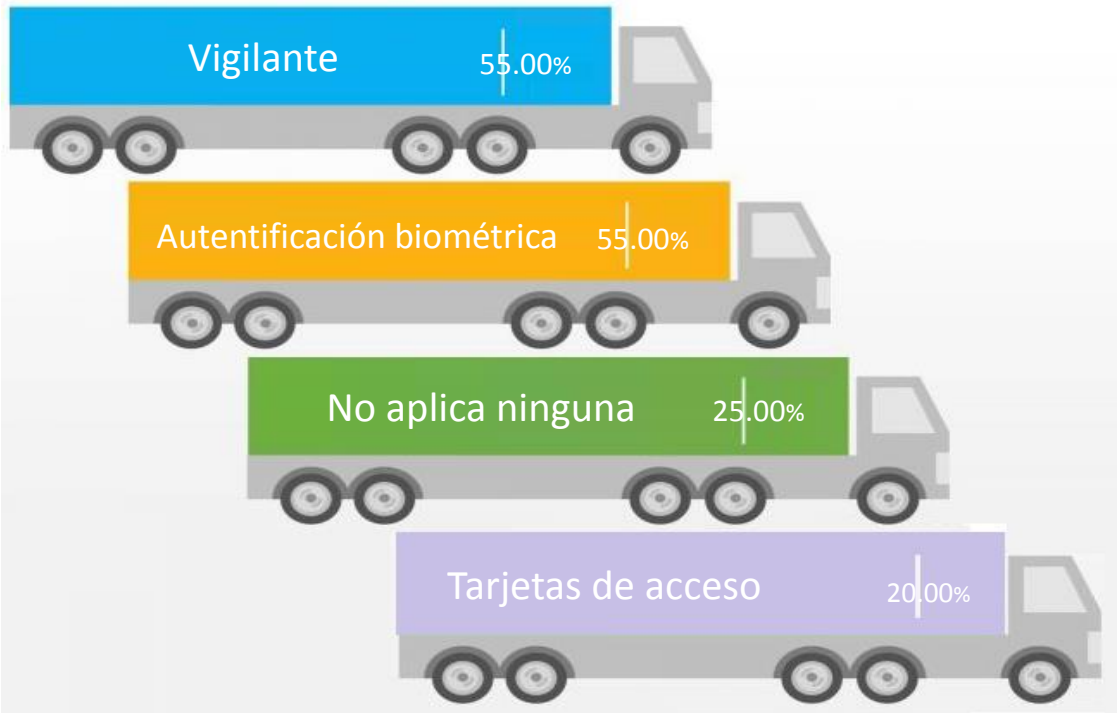
Medidas de seguridad para el acceso a la instalaciones de la empresa (selección múltiple).

Opciones	Frecuencia	Porcentaje
Vigilante	11	55.00%
Autentificación biométricos (huellas dactilares, retina, iris, patrones faciales)	11	55.00%
No aplica ninguna	5	25.00%
Tarjetas de acceso	4	20.00%

Total encuestados 20

Grafico No.6

Medidas de seguridad para el acceso a la instalaciones de la empresa.



Análisis: El nivel de inseguridad en general en El Salvador es bastante alto por lo que el contar con medidas apropiadas de acceso a las instalaciones de la empresa es muy importante, de esta forma se puede controlar el acceso de personas externas que puedan causar daños a la información y a los activos informáticos, así como el acceso a los departamentos de tecnología (empleados sin autorización) donde se encuentran los servidores o almacenan información electrónica importante de las empresas. Las medidas de seguridad más adoptadas por las empresas de logística de carga y transporte son dos principalmente, el uso de vigilante que monitorea y restringe el ingreso y la autentificación biométrica que permite el acceso solo a las personas autorizadas por la administracion o gerencia con un 55% cada una, el 20% utiliza tarjetas de acceso a todas las instalaciones y lo que parece un poco alarmante es que un 25% no aplique ninguna medida de seguridad para la protecciones de sus instalaciones.

Pregunta 7

¿La empresa cuenta con una política que restrinja el acceso a la información y a funcionalidades de los sistemas de información por parte de usurarios indebidos***? (Ref. A.9.4 control de acceso a sistemas y aplicaciones)***

Objetivo: comprobar que en la empresa se hayan definido los atributos que cada usuario puede tener según su perfil de puesto o actividades que desarrollara.

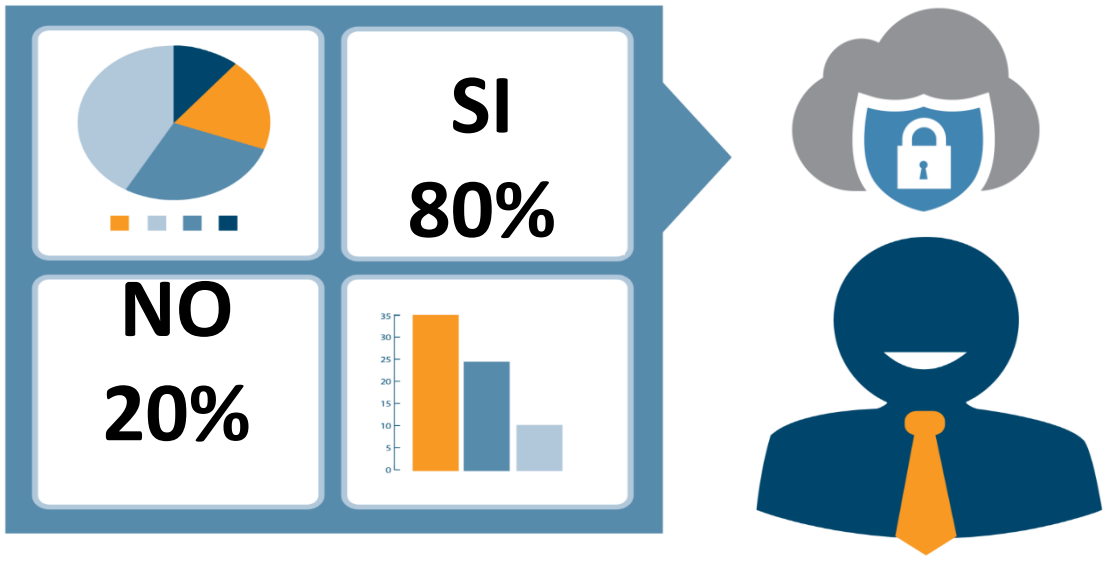
Tabla No. 7

Restricción al acceso de la información y funcionalidades de los sistemas de información.

Opciones	Frecuencia	Porcentaje
SI	16	80.00%
NO	4	20.00%
Total encuestados 20	20	100.00%

Grafico No.7

Restricción al acceso de la información y funcionalidades de los sistemas de información.



Análisis: Se ha comprobado que el 80% de las empresas del sector restringen el acceso a usuarios indebidos a través de la definición de ciertos atributos que corresponde a cada uno de sus perfiles,

lo cual es oportuno ya que esto les permite otorgar accesos a los usuarios solo a los módulos de los sistemas que deben de accesar, a pesar de esto es importante tomar en cuenta que existe un 20% que no aplica restricciones a sus usuarios y aquellos que si lo hacen es vital el seguimiento en su actualización de perfil cuando un usuario es ascendido de puesto o existe rotación a otros departamentos, el 20% que no aplica restricciones están en una desventaja competitiva y esto les puede ocasionar riesgos a su información y sistema ocasionando perdida de información, fuga de información, eliminación de información ya sea involuntariamente (usuarios que no tienen el conocimiento total del sistema pero si el acceso a todos los módulos) o con mal intención (usuarios que conocen del sistema y saben que pueden manipular o cambiar información).

Pregunta 8

Los equipos informáticos de la empresa ¿están protegidos contra los siguientes riesgos ambientales? ***(Ref. A.11.1.4 protección contra amenazas externas y ambientales)***

Objetivo: determinar si existen controles que ayuden a disminuir posibles daños en los equipos informáticos.

Tabla No.8

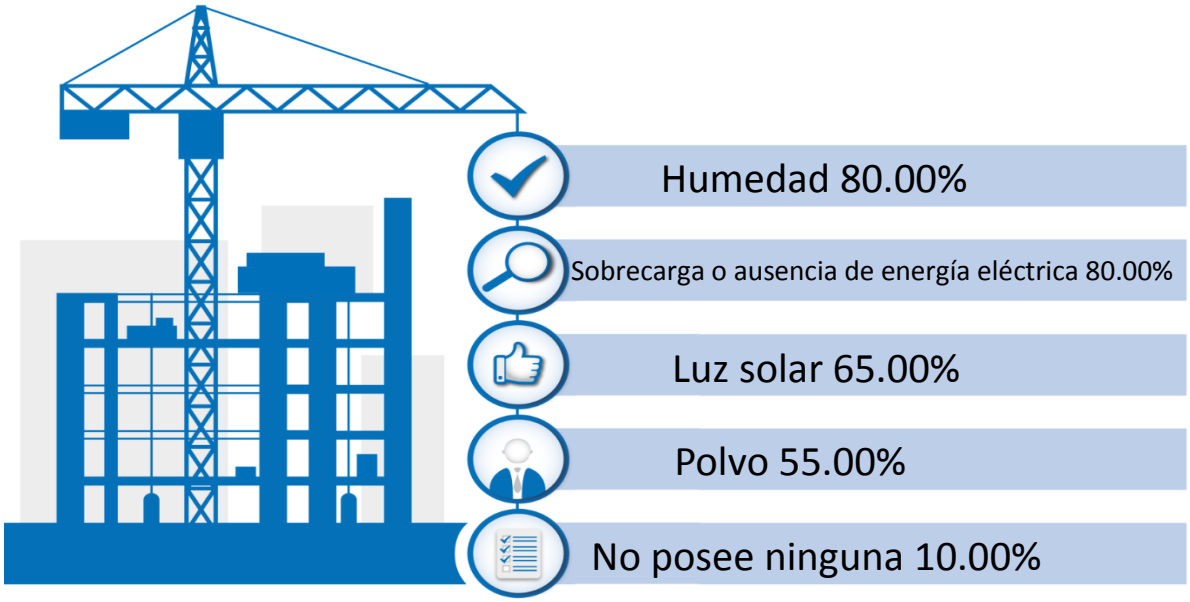
Protección para los equipos informáticos de los riesgos ambientales (selección múltiple)

Opciones	Frecuencia	Porcentaje
Humedad	16	80.00%
Sobrecarga o ausencia de energía eléctrica	16	80.00%
Luz solar	13	65.00%
Polvo	11	55.00%
No posee ninguna	2	10.00%

Total encuestados 20

Grafico No.8

Protección para los equipos informáticos de los riesgos ambientales



Análisis: La protección de los equipos informáticos para un correcto funcionamiento y alargar la vida útil es importante para las empresas con el objetivo de optimizar recursos y resguardar la información que se genera y almacena en estos equipos, los resultados reflejan que los principales controles implementados para los riesgos ambientales son humedad y sobrecarga o ausencia de energía eléctrica con un 80% respectivamente, la protección para la exposición a luz solar cuenta con un 55%, en El Salvador donde se utilizan casas como oficinas la protección de contra el polvo es importante pero acá puede observarse que solo el 55% aplican protección y un 10% que no aplica ninguna medida o control para proteger sus equipos informáticos.

Pregunta 9

¿La empresa cuenta con las siguientes medidas de seguridad física? ***(ref. a.11 seguridad física y ambiental)***

Objetivo: Verificar que la empresa cuenta con herramientas que le permitan mantener la seguridad para sus empleados y sistemas informáticos.

Tabla No.9

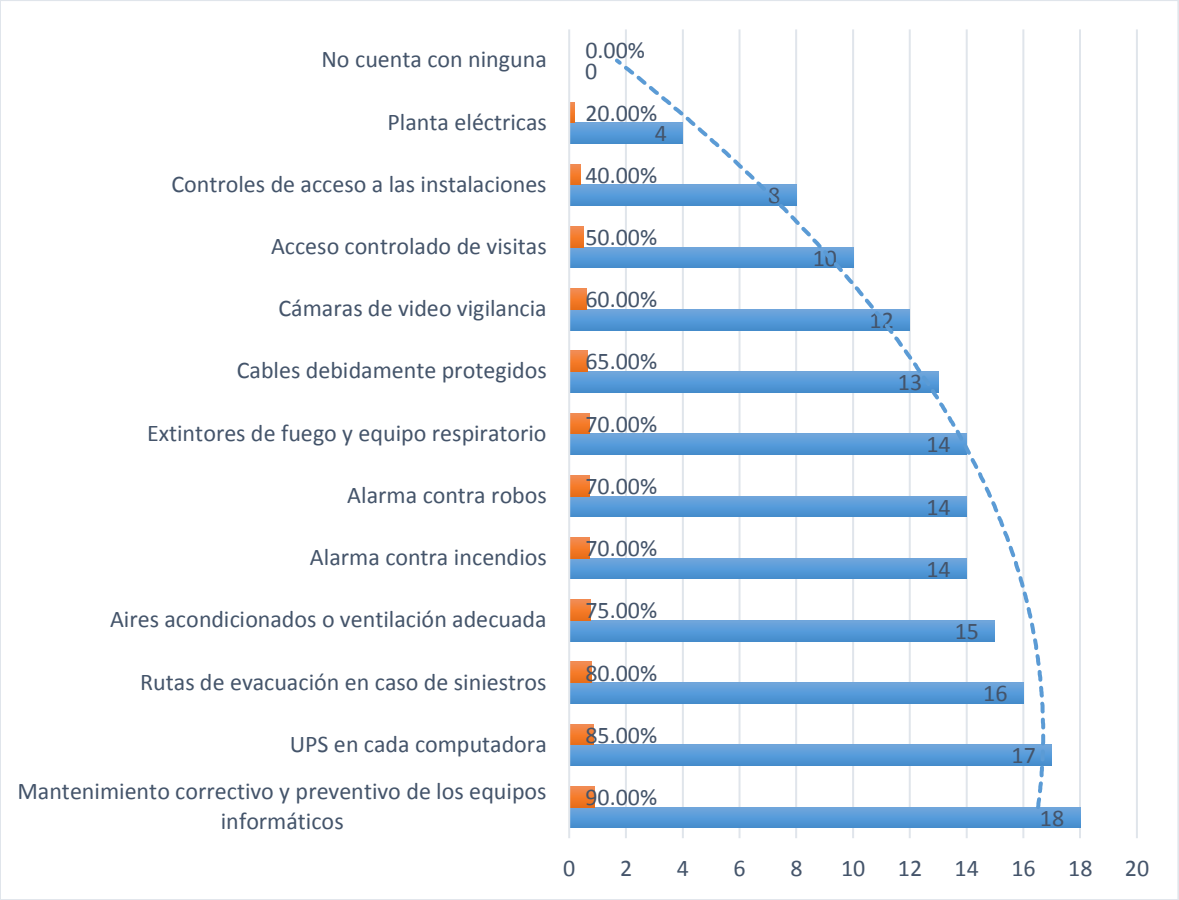
Medidas de seguridad física (selección múltiple)

Opciones	Frecuencia	Porcentaje
Mantenimiento correctivo y preventivo de los equipos informáticos	18	90.00%
UPS en cada computadora	17	85.00%
Rutas de evacuación en caso de siniestros	16	80.00%
Aires acondicionados o ventilación adecuada	15	75.00%
Alarma contra incendios	14	70.00%
Alarma contra robos	14	70.00%
Extintores de fuego y equipo respiratorio	14	70.00%
Cables debidamente protegidos	13	65.00%
Cámaras de video vigilancia	12	60.00%
Acceso controlado de visitas	10	50.00%
Controles de acceso a las instalaciones	8	40.00%
Planta eléctricas	4	20.00%
No cuenta con ninguna	0	0.00%

Total encuestados 20

Grafico No.9

Medidas de seguridad física



Análisis: De las 20 empresas encuestadas se recopilo información de las principales medidas de seguridad que implementan, siendo las principales el mantenimiento correctivo y preventivo de los equipos informáticos con un 90% esto con el fin de proteger la información (cartera de clientes, correos electrónicos, bases de datos de proveedores, contratos, proyectos, documentos de embarques, etc.) y no exponerse a su pérdida o interrupción de trabajo por no contar con la información en el momento oportuno; cada computadora posee un UPS para el 85% de las empresas encuestadas para proteger el equipo y resguardarlas de bajones o cortes de energía, con la implementación de la Ley General de Prevención de Riesgos en los Lugares de Trabajo en El Salvador la implementación de rutas de evacuación en caso de siniestros (80%), ventilación

adecuada (75%) alarma contra incendios (70%), extintores de fuego (70%) se vuelve necesaria y de carácter obligatorio por lo que en un futuro a mediano plazo todas las empresas deberán de cumplir con estas medidas de seguridad, por otro lado son pocas las empresas que cuentan con plantas eléctricas (20%) lo cual puede afectar cuando existan interrupciones de energía eléctrica y esto afectar en su operatividad.

Pregunta 10

¿Realiza copias de seguridad de toda la información sensible de la empresa? ***(ref. A. 12.3.1 Copias de seguridad)***

Objetivo: comprobar que la empresa realiza backups de su información manteniéndola segura y accesible en cualquier momento.

Tabla No.10
Copias de seguridad de la información

Opciones	Frecuencia	Porcentaje
SI	19	95.00%
NO	1	5.00%
Total encuestados 20	20	100.00%

Grafico No.10

Copias de seguridad de la información

Análisis: Mantener la información disponible en todo momento permite que las empresas del sector de logística y transporte desarrollen sus servicios en forma oportuna, el intercambio de documentación electrónica así como la alimentación de los sistemas que estas empresas utilizan debe resguardarse y contar con soportes ante un problema de ataque por medio de virus a computadoras los cuales son muy comunes en nuestra actualidad y avances tecnológicos y pueden perjudicar a la empresa, es por ello que el 95% de las empresas encuestadas confirmaron que realizan backup o copias de seguridad de la información como uno de los principales activos de la empresa, solo un 5% no hace copias de seguridad y exponen su operación e información tanto interna como de terceros (clientes, agentes representantes, proveedores) ante posibles pérdidas.

Pregunta 11

Si realiza copias de seguridad de la información ¿Cuál es la frecuencia con la cual lo realiza? ***(ref. A. 12.3.1 Copias de seguridad)***

Objetivo: cerciorarse que la información está siendo resguardada en forma oportuna.

Tabla No.11

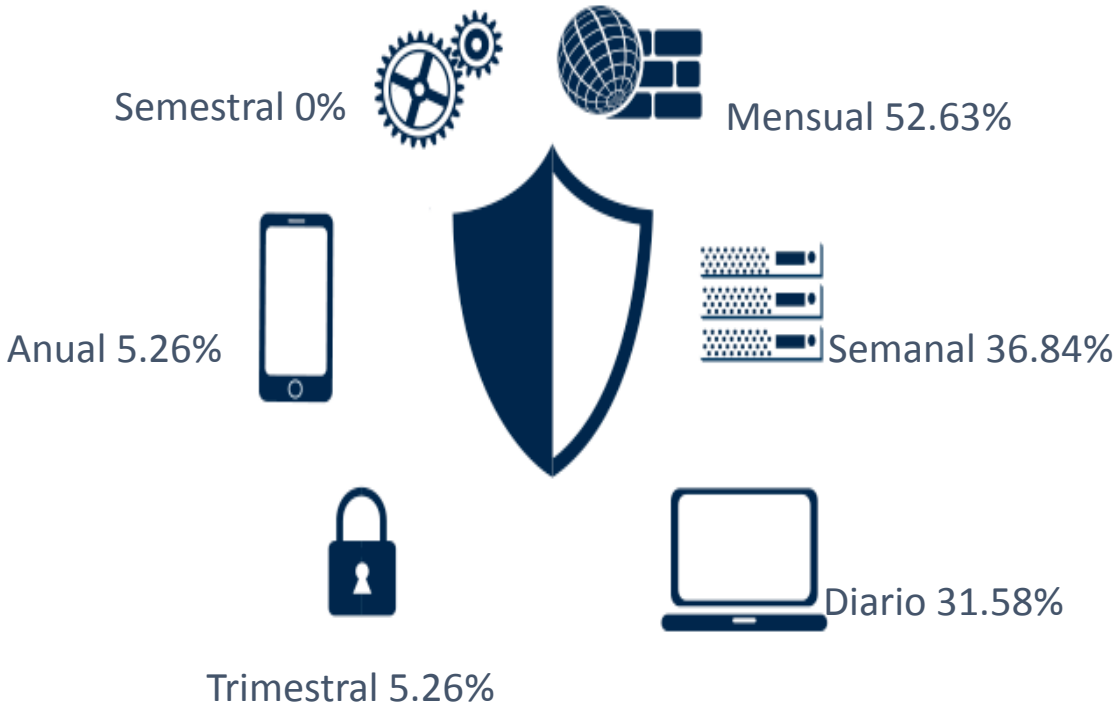
Periodicidad de las copias de seguridad de la información (selección múltiple)

Opciones	Frecuencia	Porcentaje
Mensual	10	52.63%
Semanal	7	36.84%
Diario	6	31.58%
Trimestral	1	5.26%
Anual	1	5.26%
Semestral	0	0.00%

Total encuestados 19

Grafico No.11

Periodicidad de las copias de seguridad de la información



Análisis: De las 19 empresas que confirmaron que efectúan copias de seguridad la periodicidad con la que lo realizan es variado y esta es determinada por la cantidad de información que han generado y necesitan almacenar, la mayoría de empresas realizan sus copias de seguridad mensualmente (52.6%) que es el tiempo oportuno que consideran para tener sus respaldos, otra parte lo hace semanalmente (36.8%) ya que cuentan con una cantidad considerable de información; en forma diaria (31.5%) existe una cantidad considerable que lo hace y esto es para resguardar su información y disminuir la brecha de perdida de información; otra porción de empresas lo hace trimestral (5.2%) pero es en menor cantidad y existe una porción de las empresas (5.2%) que lo hace anualmente las cuales se observa toman demasiado tiempo para hacer una copia de seguridad y esto les puede generar inconvenientes ante una pérdida de información.

Pregunta 12

¿La empresa cuenta con un software antivirus para la detección y prevención de los ataques de software maliciosos?. ***(ref. A.12.2.1 controles contra software maliciosos; SS05.01 Proteger contra software malicioso.***)

Objetivo: determinar si las organizaciones cuentan con herramientas que le ayude a evitar pérdida o fuga de información.

Tabla No. 12

Software antivirus para la detección y prevención.

Opciones	Frecuencia	Porcentaje
SI	19	95.00%
NO	1	5.00%
Total encuestados 20	20	100.00%

Grafico No.12

Software antivirus para la detección y prevención.

Análisis: De las 20 empresas encuestadas el 95% utiliza un software antivirus y con esto contrarrestan los posibles ataques a sus sistemas operativos o información electrónica, la utilización de este tipo de software lo ven positivo porque les ayuda a prevenir ataques, pero para ello se ha constatado la preferencia del software utilizado a manera de determinar la calidad de software utilizado

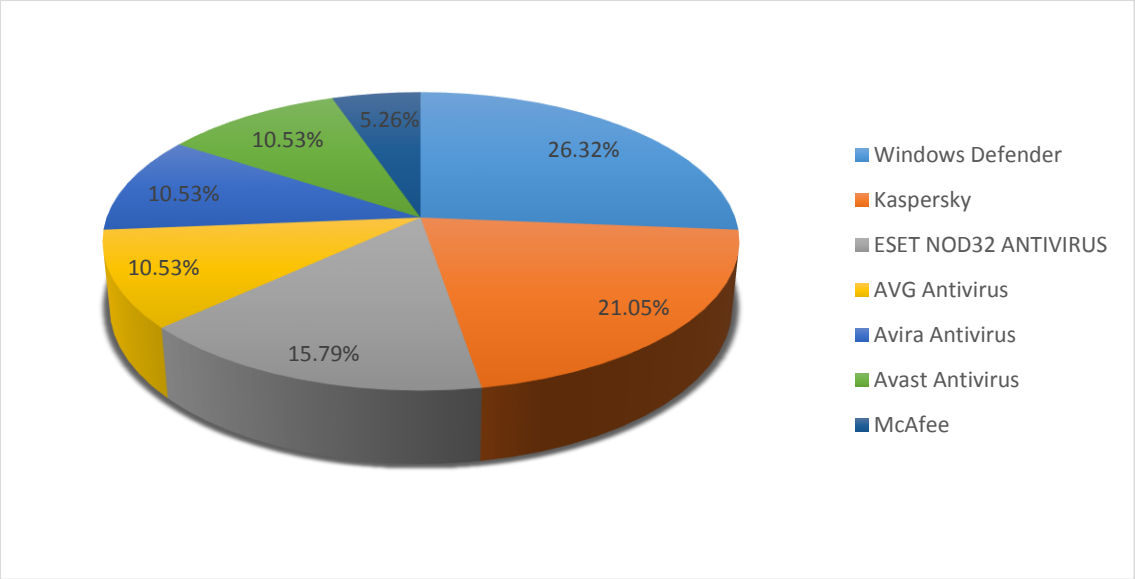
Tabla 13

Título:Software antivirus más utilizado

Opciones	Frecuencia	Porcentaje
Windows Defender	5	26.32%
Kaspersky	4	21.05%
ESET NOD32 ANTIVIRUS	3	15.79%
AVG Antivirus	2	10.53%
Avira Antivirus	2	10.53%
Avast Antivirus	2	10.53%
McAfee	1	5.26%
Total encuestados 19	19	100.00%

Grafico No.13

Software antivirus más utilizado



Análisis: La preferencia del software utilizado por las empresas del sector de logística y transporte en primer lugar se encuentra Windows defender (26.3%) y esto es entendible debido a que es un software que se incluye en la licencia de paquetes de los sistemas operativos Windows ; en segundo lugar Kaspersky (21%) que se promueve como una de las mejores alternativas de seguridad de información en el medio, ESET NOD 32 (15.8%) una buena herramienta para Windows que está ganando mercado, AVG, Avast y Avira comparten de las últimas elecciones de las empresas del sector de logística y transporte (10.5%) y en último lugar de preferencia McAfee (5.3%) que ha permanecido en el mercado por mucho tiempo pero por ser un software pagado no tiene tanta aceptación, se ha comprobado que las elecciones de software están determinados en si son gratis y no en las características de seguridad que puedan cumplir.

Pregunta 13

¿Cuáles de las siguientes medidas aplican en la empresa para garantizar la seguridad de la información generada por los sistemas? ***(ref. A.13.2 transferencia de información***)

Objetivo: Determinar si dentro de la empresa aplican medidas de seguridad para evitar fuga de información.

Tabla 14

Medidas de seguridad para la información generada por los sistemas (selección múltiple)

Opciones	Frecuencia	Porcentaje
Autentificación de usuarios (Contraseñas)	19	95.00%
Software antivirus	19	95.00%
Actualización de Software	15	75.00%
Control de acceso a los datos	11	55.00%
Socialización a los usuarios de normas o políticas de seguridad Informática	5	25.00%
Validación de datos	5	25.00%
Encriptación de datos sensibles o confidenciales	2	10.00%
No aplicamos ninguna medida.	0	0.00%

Total encuestados 20

Grafico No.14

Medidas de seguridad para la información generada por los sistemas

Análisis: La información que se genera en sistemas internos por las empresas del sector de logística y transporte es utilizada como de lectura para externos en particular por clientes locales e internacionales, en donde se verifica el status actual de un embarque y ubicación, además se ingresa información de embarcadores (shipper) y receptores de carga (consignee), descripciones de productos, pesos y dimensiones así como otra información necesaria para el tránsito de la carga, estos sistemas generan aparte de estatus, documentos de tránsitos como BL, manifiesto, guía aérea, carta de porte, notificaciones de arribo etc., acá se incluyen términos de negociaciones y números de contratos o tarifas, lo anterior refleja que toda esta información es muy delicada y confidencial por lo que su resguardo es muy importante, la forma más común de protegerla es por medio de autentificación de usuarios (95%) y solo con usuario y clave se puede accesar a los sistemas, software antivirus (95%) es muy utilizado y en tercer lugar la actualización de software (75%) que permitan detectar anomalías en los lenguajes de programación o problemas de enlaces de información, el control de acceso a los datos (55%) permitiendo solo a usuarios autorizados; es importante tomar en cuenta que al no contar con normas o políticas de seguridad (25%) estas no se pueden socializar a los usuarios para sus prácticas, la validación de datos (25%) y la encriptación de datos sensibles (10%) son las medidas menos utilizadas y quizás las de mejor efectividad a la hora de proteger la información.

Pregunta 14

¿Cuáles de las siguientes características utiliza la empresa para autentificar las contraseñas de usuario? ***(DSS05.02 gestionar la seguridad de las redes y conexiones)***

Objetivo: comprobar que las contraseñas no sean fácil de identificar por otros usuarios y que puedan utilizarlas con fines de acceso a información que no corresponda a sus perfiles.

Tabla No.15

Autentificación de contraseñas (selección múltiple)

Opciones	Frecuencia	Porcentaje
Asignación de ID únicos para establecer responsabilidades	14	70.00%
Cambio de contraseña cada determinado periodo	12	60.00%
Bloqueo de accesos por intentos fallidos	8	40.00%
Técnicas de cifrado	4	20.00%
No se utiliza ninguna	2	10.00%

Total encuestados 20

Grafico No.15

Autentificación de contraseñas

Análisis: Saber que cada usuario es único y utiliza el usuario correcto (no hay intercambios de usuarios y claves entre colegas del trabajo) es un factor fundamental para asegurar el correcto funcionamiento de los permisos y perfiles asignados en los sistemas, para ello la asignación de contraseñas es un punto esencial y se ha podido identificar que las principales medidas que toman las empresas del sector de logística de carga son: en primer lugar la asignación de ID únicos (70%) donde se establecen las responsabilidades según el perfil del usuario, en segundo lugar los cambios de contraseñas cada determinado periodo (60%) para evitar que otros usuarios lo utilicen y tengan accesos a módulos que no están autorizados y así evitar manipulación de la información, el bloqueo de usuario por intentos de acceso fallidos (40%) es el tercer lugar en la lista y es una muy buena práctica para controlar el acceso por usuarios desconocidos o aquellos que intentan utilizar otros usuarios que no son de ellos, en último lugar se encuentra las técnicas de cifrado (20%) y existe un 10% de las empresas que no aplica ninguna medida para autentificar las contraseñas de los usuarios.

Pregunta 15

¿Ha sufrido la empresa ataques informáticos los últimos 3 años? ***(A.16.1.3 Informar sobre debilidades de seguridad de la información)***

Objetivo: Verificar si la empresa ha tenido incidencias de pérdida o fuga de información.

Tabla No.16

Ataques informáticos

Opciones	Frecuencia	Porcentaje
SI	5	25.00%
NO	15	75.00%
Total encuestados 20	20	100.00%

Grafico No.16

Ataques informáticos

Análisis: Al indagar respecto a los ataques informáticos sufridos en los últimos años el 25% de las empresas encuestadas confirmaron haberlo sufrido, en un primer momento un 25% puede parecer poco pero si de cada 100 empresas en el sector 25 son vulnerables a ataques este número ya es un poco más alarmante, sobre todo cuando algunas empresas sufren ataques pero no los catalogan como si lo fuesen (uso indebido de internet, modificación de información, modificación de correos electrónicos, correos spoofing) debido a que estos incidentes en algún momento no son detectados ni reportados a las unidades de análisis de tecnología por el mismo temor a una sanción o problema de parte de la administración.

Pregunta 16

De los ataques informáticos sufridos por la empresa ¿Cuáles fueron las causantes del ataque? ***(A.16.1.4 evaluación y toma de decisión sobre los eventos de seguridad de la información)***

Objetivo: Identificar las principales razones de un ataque informático en las organizaciones

Tabla No.17

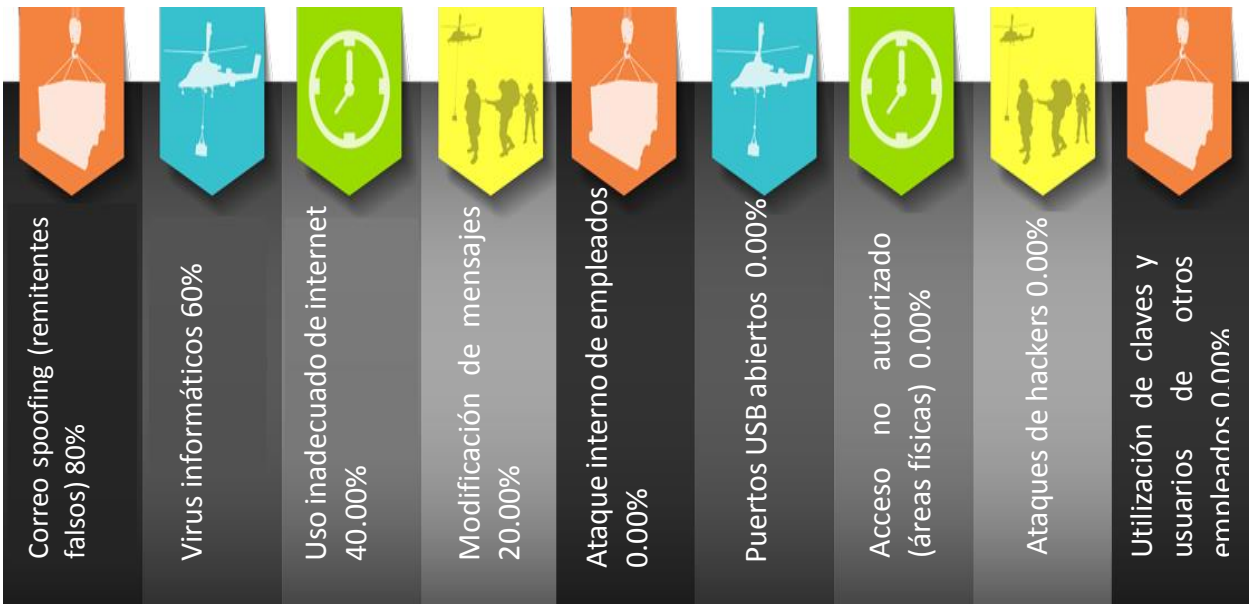
Causantes de los ataques informáticos (selección múltiple)

Opciones	Frecuencia	Porcentaje
Correo spoofing (remitentes falsos)	4	80.00%
Virus informáticos	3	60.00%
Uso inadecuado de internet	2	40.00%
Modificación de mensajes	1	20.00%
Ataques de hackers	0	0.00%
Acceso no autorizado (áreas físicas)	0	0.00%
Ataque interno de empleados	0	0.00%
Puertos USB abiertos	0	0.00%
Utilización de claves y usuarios de otros empleados	0	0.00%

Total encuestados 5

Grafico No.17

Ataques informáticos



Análisis: Del 25% de las empresas que sufrieron ataques en los últimos años la principal razón ha sido los correos spoofing (80%) los cuales aparentan ser remitentes confiables pero no lo son y solicitan usuarios y claves para poder accesar a las cuentas posteriormente, esta medida es una de las más utilizadas actualmente por los hackers, en segundo lugar los virus informáticos (60%) ya que muchas de las actualizaciones de estos software no se han realizado según lo recomendado, en tercer lugar el uso inadecuado de internet (40%) en donde los usuarios pueden accesar a cualquier página web o sitio y no son bloqueados por lo que no solo está en riesgo la información sino también la productividad de los empleados, en cuarto y último lugar se ubica la modificación de correos (20%) el cual se ve como una práctica de empleados o usuarios a fin de modificar información que les respalde en los servicios que brindan.

Pregunta 17

De los ataques informáticos sufridos por la empresa ¿Cuáles fueron las consecuencias del ataque? ***(A.16.1.6 aprendizaje de los incidentes de seguridad de la información)***

Objetivo: Verificar el impacto de los ataques sufridos en las empresas.

Tabla No.18

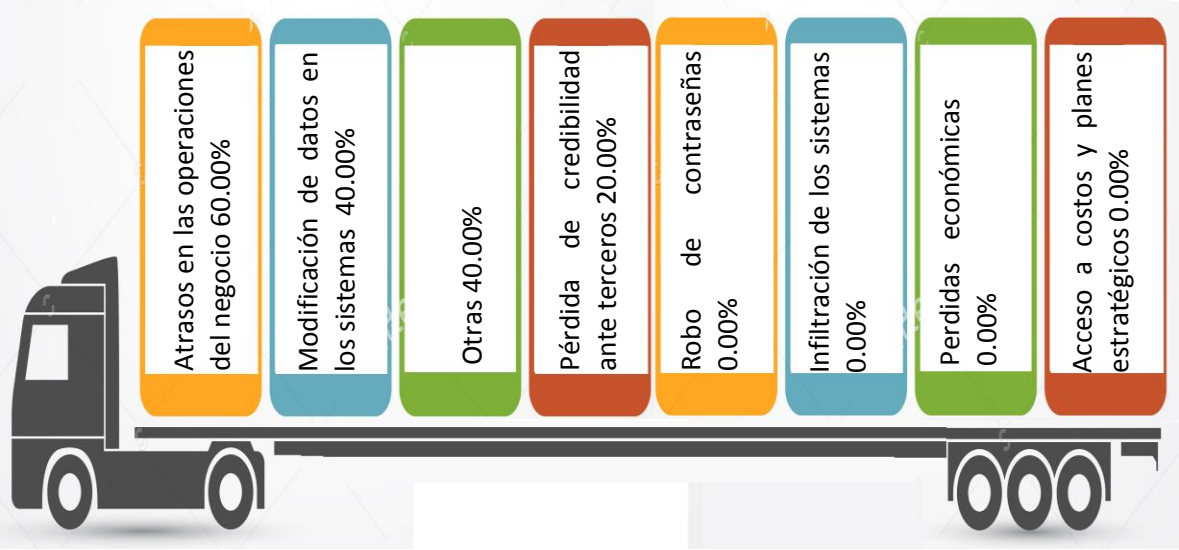
Consecuencias de los ataques informáticos (selección múltiple)

Opciones	Frecuencia	Porcentaje
Atraso en las operaciones del negocio	3	60.00%
Modificación de datos en los sistemas informáticos	2	40.00%
Otras	2	40.00%
Pérdida de credibilidad ante terceros	1	20.00%
Robo de contraseñas	0	0.00%
Infiltración a los sistemas informáticos	0	0.00%
Perdidas económicas	0	0.00%
Acceso a costos y planes estratégicos de la compañía	0	0.00%

Total encuestados 5

Grafico No.18

Consecuencias de los ataques informáticos



Análisis: Las consecuencias de los ataques sufridos por las empresas del sector de logística de carga y transporte han sido principalmente el atraso en las operaciones (60%) lo cual afecta la eficacia y eficiencia así como la productividad, el incremento de incidencias y reclamos de parte de los clientes y de los agentes representados en el país puede incrementar debido a este punto; en segundo lugar las modificaciones de datos en los sistemas (40%) este punto es preocupante ya que el modificar un dato o registro repercute en información falsa, otras causas han sido identificadas (40%) las cuales son base de datos de clientes que los empleados comparten con otras empresas del sector esto repercute en la disminución de volumen de carga o perdida de clientes; en último lugar se encuentra la pérdida de credibilidad ante terceros (20%) debido a que al brindar información falsa o no tener los sistemas actualizados los terceros (clientes, agentes) no confían en la información proporcionada.

Pregunta 18

¿Considera que la aplicación de políticas de seguridad informática le ayudaría a la empresa a proteger la información y generar credibilidad y confianza ante terceros?

Objetivo: comprobar la necesidad de políticas que ayuden a las empresas del sector de logística y transporte de carga a salvaguardar la información.

Tabla No.19

Protección de la información

Opciones	Frecuencia	Porcentaje
SI	20	100.00%
NO	0	0.00%
Total encuestados 20	20	100.00%

Grafica No.19

Aplicación de políticas de seguridad

Análisis: El 100% de las empresas consideran que las políticas de seguridad informática les pueden ayudar a mejorar su seguridad y esto convertirlo en una herramienta para protección e incremento de sus negocios.

Pregunta 19

¿Cree que la empresa estaría interesada en aplicar políticas de seguridad informática basadas en la Norma Técnica Salvadoreña ISO/IEC 27001:2013?

Objetivo: verificar la oportunidad de proponer políticas para la protección de la información y el uso que las empresas le podrían dar.

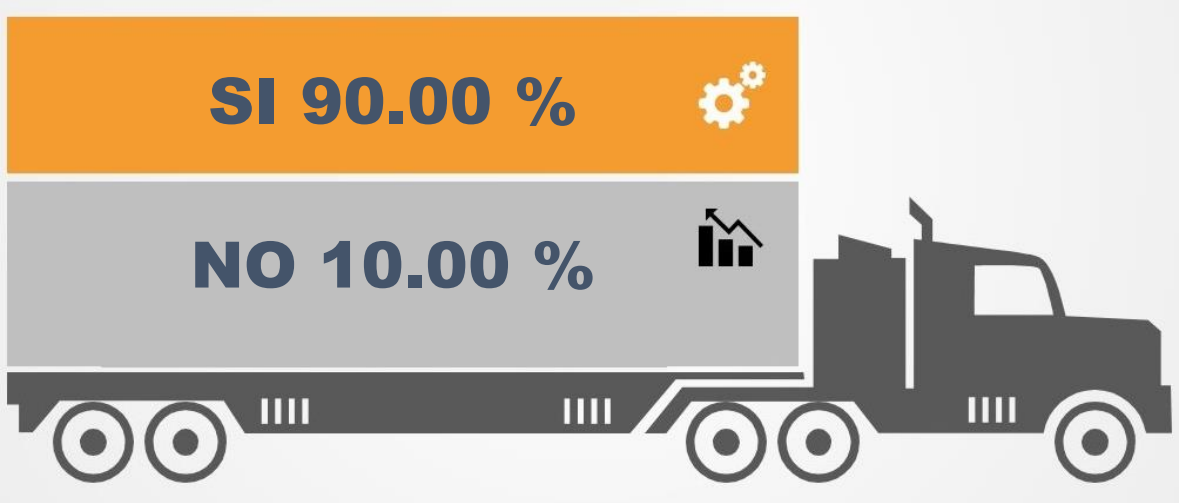
Tabla No.20

Aplicación de políticas de seguridad

Opciones	Frecuencia	Porcentaje
SI	18	90.00%
NO	2	10.00%
Total encuestados 20	20	100.00%

Grafico No.20

Aplicación de políticas de seguridad



Análisis: El 90% de las empresas consideran que estarían interesados en aplicar políticas de seguridad informática ya que esto les permitirá mejorar sus niveles de seguridad y dar mayor competitividad en el sector de logística de carga y transporte sobre todo por que estarán basadas en una normativa técnica con estándares internacionales como las empresas que representan en el país.

ANEXO 4

Contrato de trabajo con cláusula de confidencialidad

El presente Contrato Individual de Trabajo lo otorgan, por una parte ***(nombre de la empresa)***, como patrono, representada por ***(represente o apoderado legal);*** y por otra parte ***(nombre del empleado),*** como el trabajador.

GENERALES DEL REPRESENTANTE PATRONAL:

Nombre:
Fecha de nacimiento:
Sexo:
Estado Civil:
Profesión u oficio:
Del Domicilio de:
Nacionalidad:
Documento único de identidad:
Fecha de expedición:
Fecha de vencimiento:

Actuando como Apoderado General Administrativo de ***(nombre de la empresa)***, que puede abreviarse como ***(nombre de la empresa)***, del domicilio de: ***(domicilio de la empresa)*** quien en adelante se denominará "el Patrono".

GENERALES DE ELLA) EMPLEADO (A)

Nombre:
Fecha de nacimiento:
Sexo:
Estado Civil:
Profesión u oficio:
Domicilio y residencia:
Nacionalidad:
No. de DUI:
Lugar y fecha de expedición:

Actuando por sí mismo(a) y quien en adelante se denominará "el (la) Empleado(a)".

Ambas partes, en el carácter que aparece indicado, convienen en celebrar el presente CONTRATO INDIVIDUAL DE TRABAJO sujeto a las siguientes cláusulas:

CLAUSULA 1: El (la) empleado(a) trabajará para y a las órdenes de El Patrono, con el cargo de ***(cargo del empleado***), cumpliendo las obligaciones que le impongan las leyes laborales, sus reglamentos y el Reglamento Interno de Trabajo; tendrá como responsabilidad principal: ***(funciones del empleado***), y otros; así como cumplir con las tareas y actividades detalladas en su Descriptor de Puesto, entre otras funciones solicitadas por el jefe inmediato y que sean inherentes al cargo, o que sean necesarias para el mejor desempeño del mismo, o que surjan como consecuencia de circunstancias no previstas, relacionadas con la naturaleza del cargo.

CLAUSULA 2 El lugar en que el (la) Empleado(a) prestará sus servicios será donde el Patrono estime conveniente por la naturaleza del Trabajo. Las oficinas principales serán en: ***(Dirección de la empresa),*** en el entendido que podrá ser trasladado a cualquier dependencia del Patrono presentes o futuras o a los lugares en que sea necesaria la prestación de sus servicios.

Clausula 3 (Pago del sueldo)

Clausula 4 (Horario y lugar de trabajo)

Clausula 5 (Prestaciones laborales)

Cláusula 6 (Dependientes económicos del empleado)

Clausula 7 (Prohibiciones)

CLAUSULA 8 CLAUSULA DE CONFIDENCIALIDAD:

*El (la) Empleado(a) se compromete a mantener bajo estricta confidencialidad, toda aquella información necesaria que corresponde al Patrono tales como base de datos de clientes, proveedores, costos de servicios, rutas, embarques en tránsito, proyectos en desarrollo, etc***.** *Queda expresamente convenido entre el Patrono y el (la) Empleado(a) que cualquier*

infracción(es) a la confidencialidad, al reglamento interno, a la costumbre de la empresa, demás leyes o tratados aplicables y/o a las disposiciones contenidas en el presente contrato serán notificadas por escrito a él (la) Empleado(a) como amonestaciones laborales internas de la empresa, debiéndose enviar una copia de dicha amonestación al Ministerio de Trabajo y Previsión Social.

F_____ **F**_____

(Empleador) **(Empleado)**

ANEXO 5

Comprobante de entrega de políticas de seguridad informática a empleados

Yo: ***(nombre del empleado)*** he recibido una copia de la Políticas de seguridad informática, las he leído me he familiarizado con ésta y la he entendido. También he participado y completado la capacitación sobre las mismas. Por medio del presente acepto cumplir con los requisitos específicos de la Política en todos aspectos durante mi empleo, u Otro servicio o relación comercial con la empresa o compañías afiliadas, y posteriormente, en la medida que lo requiera la Política. Entiendo que cualquier actividad que viole la ley aplicable se encuentra prohibida, y entiendo las posibles consecuencias de dicha violación. Actualmente me encuentro en total cumplimiento con la Política, y no conozco ninguna violación a la política por otra entidad o persona sujeta a esta Política, salvo por las que han sido previamente informadas a la empresa. Reconozco que la falta de cumplir con todos los aspectos de la Política puede ser motivo para terminación con causa de mi empleo, u otro servicio o relación comercial con la empresa.

Nombre:

Firma:

Puesto:

ANEXO 6

Acuerdo de intercambio de información

El presente acuerdo de intercambio entra en vigencia en ***[fecha]*** y se celebra

ENTRE: ***[Nombre de la organización]***

Y: ***[Nombre del tercero al que se le transfiere la información]***

El objetivo es garantizar la protección de la información que se transmitirá entre las partes involucradas y determinar responsabilidades en caso de manipulación, pérdida o uso inadecuado de la misma.

En mutuo acuerdo de ambas partes, por medio de la presente las partes acuerdan lo siguiente:

- Responsabilidades para el control, despacho y recepción de la información.
- Procedimientos para notificar al remitente la recepción de la información
- Responsabilidades y obligaciones en caso de ocurrir incidentes de seguridad, como pérdida de documentos.
- Utilización de un sistema de etiquetado que especifique lo confidencial o crítica que es la información

F	F
[FIRMA DE AUTORIZACIÓN]	***[FIRMA DE AUTORIZACIÓN]***

LUGAR Y FECHA

ANEXO 7

Contrato de confidencialidad

El objeto de garantizar la confidencialidad de: ***[Nombre de la información],*** se hace necesario la firma de un acuerdo que garantice los niveles de confianza entre las partes. El documento se firmará una vez aceptado y firmado por ambas partes.

El contenido del acuerdo es el que figura a continuación. Contenido

DE UNA PARTE: ***[nombre de la empresa]*** y en su nombre y representación (con poder suficiente para ello) D/Dña. ***[nombre completo],*** en calidad de ***[cargo, administrador, apoderado,]***

DE OTRA PARTE: ***[nombre del tercero].*** Y en su nombre y **representación (con poder suficiente para ello)** D/Dña. *[nombre completo],* en calidad de ***[cargo, administrador, apoderado,]***

Reunidos en ***[lugar de la firma del contrato]***, a ***[día]*** de ***[Mes]*** de ***[Año]***

EXPONEN

I – Que las partes, anteriormente citadas, están interesadas en el desarrollo del presente contrato, para lo cual, aceptaron celebrar el presente Acuerdo de Confidencialidad con el fin de establecer el procedimiento que regirá la custodia y no transmisión a terceros de la información distribuida entre las partes, así como los derechos, responsabilidades y obligaciones inherentes en calidad de remitente, propietario y «destinatario» de la referida información.

II – Que las partes, en virtud de lo anteriormente expuesto, convinieron que el presente Acuerdo de Confidencialidad se rija por la normativa aplicable al efecto y, en especial por las siguientes.

CLÁUSULAS

CLAUSULA 1: Las partes consideran confidencial la «Información propia» de la otra parte que le pudiera suministrar y acuerdan su guarda y custodia estricta, así como a su no divulgación o suministro, ni en todo ni en parte, a cualquier tercero sin el previo, expreso y escrito consentimiento de «Fuente». Tal consentimiento no será necesario cuando la obligación de suministrar o divulgar la «Información propia» de la «Fuente» por parte del «Destinatario» venga impuesta por Ley en vigor o Sentencia Judicial Firme. Este Acuerdo no autoriza a ninguna de las partes a solicitar o exigir de la otra parte el suministro de información, y cualquier obtención de información de/o sobre la «Fuente» por parte del «Destinatario» será recibida por éste con el previo consentimiento de la misma.

CLAUSULA 2: El «Destinatario» será responsable de la custodia de la «Información propia» y cuantas copias pudiera tener de la misma suministrada por la «Fuente», en orden a su tratamiento, como secreta, confidencial o restringida, en el momento presente y futuro, salvo indicación explicita de la «Fuente». Al objeto de garantizar esta custodia, se deberá devolver la «Información propia» y cuantas copias pudiera tener de la misma suministrada por la «Fuente», a la terminación de las relaciones comerciales, o antes, si fuera requerido por la «Fuente» y respondiendo a los daños y perjuicios correspondientes, en el caso de incumplimiento de lo aquí dispuesto. (En aquellos casos en los que no fuera necesaria la devolución de la «Información propia» deberá eliminarse este párrafo)

CLAUSULA 3: Ambas partes acuerdan mantener el presente Acuerdo de Confidencialidad, aún después de terminar sus relaciones comerciales.

CLAUSULA 4: El presente Acuerdo de Confidencialidad se regirá por la Legislación salvadoreña aplicable, y cualquier disputa, controversia o conflicto en cuanto a la interpretación o ejecución del presente Acuerdo será sometido a la jurisdicción de los Tribunales salvadoreños, con exclusión de cualquier otro que pudiera corresponder a las partes, al que en este momento renuncian.

Y en prueba de esta conformidad, las partes firman o presente acuerdo, por duplicado y a un solo efecto, en el lugar y fecha ut supra.

F

[FIRMA DE AUTORIZACIÓN]

F

[FIRMA DE AUTORIZACIÓN]

LUGAR Y FECHA

ANEXO 8

Cláusula para contrato de confidencialidad con proveedor

El acuerdo que debe contener todo contrato con terceros o proveedores que son críticos en la plataforma de tecnología, así como operatividad de la organización es el siguiente:

CLAUSULA 4: Es de común acuerdo entre las partes involucradas en la firma del contrato por servicios que la información a la cual tenga acceso nuestro proveedor: ***[nombre del tercero]*** tanto para servicios recurrentes como para proyectos será utilizada única y exclusivamente para los fines de prestar un servicio entre las partes relacionadas:

1. Durante la prestación del servicio que esté vinculado directamente con un servicio operativo, las tarifas, clientes, rutas y contactos principales serán de total confidencialidad y estos no podrán divulgarse con otras entidades, personal externo a menos que por ley se solicite.
2. Durante la prestación del servicio que esté vinculado a redes, accesos, claves, almacenamiento de información, transferencia de datos, toda la información relacionada será tratada como crítica y confidencial por lo que su resguardo es responsabilidad del proveedor y no podrá revelarse ni compartir con personas que no hayan sido autorizadas por la organización previamente.
3. Luego de finalizado el contrato es responsabilidad del proveedor eliminar toda la información incluyendo las copias de seguridad que este tuviera, así como está prohibido compartir información relacionada a la empresa por un periodo de 1 año posterior a la finalización del contrato.

ANEXO 9

Entrevista al Ing. Fernando Martinez, Gerente General del grupo empresarial Comca Internacional.

Entrevistado: Ing. Fernando Martinez, gerente general del grupo empresarial Comca Internacional.

Entrevistador: Nestor Canizalez, estudiante de la Universidad de El Salvador, facultad de ciencias económicas, optando a la licenciatura en contaduría pública.

Nestor: agradecemos al Ing. Fernando Martinez el espacio que nos brinda para poder conversar un poco acerca de las empresas de logística y transporte de carga, así como de los riesgos informáticos derivados de los avances tecnológicos y como estos ayudan a las empresas del sector.

Ing. Fernando: buenas tardes Nestor, a la orden y un gusto colaborarte, estamos listos para contestar tus inquietudes.

Nestor: gracias Ingeniero para comenzar nos gustaría saber *¿Que es COMCA Internacional?*

Ing. Fernando: Comca es una empresa familiar fundada en el año 1967, como una empresa de transporte de carga, mudanzas y de representaciones de Navieras, a lo largo de los años hemos representado diferentes empresas en el rubro de la carga, actualmente la empresa cuenta con aproximadamente 96 empleados directos y con aproximadamente 100 más indirectos (subcontratados), posee dos representaciones principales: 1. La naviera Israelita ZIM Integrated Shipping Services y 2. La empresa Alemana de carga DB Schenker, localmente contamos con el servicio de mudanzas internacionales y locales, la cual cuenta con el respaldo de asociaciones internacionales como: la Asociación Latinoamericanas de Empresas de Mudanzas (LATAM por sus siglas en ingles) y la Asociación Americana de Mudanzas (IAM por sus siglas en ingles).

A lo largo de estos 50 años se cuenta con una cobertura completa y global de todos los servicios de transporte incluyendo las mudanzas, desde un sobre hasta un contenedor o maquinaria completa.

Nestor: *¿Cuál es el aporte que las empresas como Comca Internacional dan a la economía en El Salvador?*

Ing. Fernando: las empresas del transporte son una parte fundamental de la economía de cualquier país, dado que tú puedes vivir en un país que produzca, pero si no tienes el medio de transporte para hacer llegar los productos de un lugar a otro no podes hacer nada, por lo que el aporte de las empresas de logística es esencial y primordial para las economías de cualquier país (ya sea desarrollado o en vías de desarrollo como el nuestro) al apoyar a realizar esta actividad de movilización de la carga.

Nestor: *¿Que tan importante es la tecnología para las operaciones de Comca?*

Ing. Fernando: es bien importante y se puede medir en diferentes etapas, digamos en el concepto básico de transporte que es hacer llegar un producto del punto A al punto B, lo podes hacer de una manera tan rudimentaria y sencilla como agarrar el producto y llevarlo en un vehículo convencional, ahora las necesidades modernas de las empresas y la competitividad que se les exige para tener éxito en el mercado mundial, que a su vez nos exigen a los operadores logísticos contar con procesos eficientes y efectivos y eso implica contar con tecnología y contar con información, entonces la tecnología se ha vuelto y creo seguirá siendo una parte muy importante para el desarrollo y éxito de las empresas en el rubro.

Nestor: en ese sentido entenderíamos nosotros que la comunicación es muy importante durante el proceso de la logística de carga, esta comunicación *¿cómo la administran ustedes localmente con sus clientes, proveedores y las empresas que ha mencionado que representan?*

Ing. Fernando: la comunicación es muy importante y va en dos sentidos, hacia nuestros clientes que se refiere a mantener a nuestros clientes informados con el status de su carga, a donde se encuentra, cuando va a llegar etc, y hacia adentro con esto me refiero al control interno para saber en qué etapa del proceso se encuentra el servicio, y esto incluye que por ser servicios internacionales, necesitamos contar con empresas extranjeras que son nuestros aliados, y empresas que necesitan se les retroalimente esta información o viceversa, entonces la información es básica para poder prestar el servicio.

Nestor: en la prestación del servicio ustedes *¿utilizan algún software o herramienta?*

Ing. Fernando: ocupamos desde lo básico que es el correo electrónico como una herramienta primordial, el teléfono, celulares con sus nuevas aplicaciones o herramientas que se están desarrollando por ejemplo Whatsapp que hasta hace unos años no era una aplicación que se utilizara para la comunicación, ahora se ha vuelto muy importante para la comunicación con clientes, además contamos con software desarrollados ya sean propios o comprados a proveedores que son específicos para el seguimiento de carga.

Nestor: en estos sistemas y herramientas por lo tanto se ingresa y sale información, *¿existe alguna forma de controlar la generación y el ingreso de esa información?*

Ing. Fernando: el control de la información siempre va estar sujeto al error humano, por lo tanto se requieren procesos de control y de verificación para reducir en lo mínimo estos tipos de errores, por contar con herramientas que utilizan información externa se requiere un control muy estricto

y el momento preciso en el que se tiene que estar digitando esa información, porque de nada sirve tener la información pero no en el momento oportuno, la custodia de la carga es tan importante como la custodia de la información, por ejemplo puede llegar la carga a su destino (puerto o aeropuerto) pero si yo no le aviso que ya llegó, el proceso para finalizar el servicio nunca se dará y al cliente se le generaran cargos adicionales por demoras o almacenaje.

Nestor: *¿entonces es importante la fluidez de esa información?*

Ing. Fernando: es importante la fluidez, pero también la calidad de la información, el tiempo en el que se digita la información y el sistema que se utiliza para tal fin es esencial.

Nestor: *¿han tenido algún inconveniente en el cual en algún momento no se haya podido informar o que no se haya cumplido con las características de la información que menciono y les generará algún problema?*

Ing. Fernando: sí, y esto generado por dos problemas: 1. La tecnología no es infalible y se han presentado ocasiones en la que los sistemas se caen y no se ha podido ingresar la información, o no se tiene la información adecuada en el momento oportuno para ingresarla, 2. Que la persona responsable de digitalizarla no está haciéndolo en el momento que corresponde, por lo que se necesita un control continuo para que la información esté disponible en el momento necesario.

Nestor: hablando de disponibilidad ustedes *¿proveen a los empleados herramientas para que ellos hagan el trabajo de forma oportuna?*

Ing. Fernando: definitivamente si, facilitamos las herramientas porque de otra manera seria imposible cumplir con las actividades designadas, obviamente los teléfonos inteligentes, las computadoras personales ya son herramientas indispensables, la otra cuestión que exige que los empleados tengan los accesos a la información y herramientas, es porque muchos servicios

(embarques, arribos) se prestan en países con diferentes horarios, por ejemplo Europa con 5 a 6 horas de diferencia, Asia con 12 horas de diferencia y es necesario mantener la comunicación y estar conectados.

Nestor: respecto a las herramientas que ustedes les brindan a los empleados, *¿en algún momento han sufrido alguna pérdida o robo?*

Ing. Fernando: si, lamentablemente es una realidad con la que tenemos que aprender a vivir y a trabajar, y exige que el departamento de informática de la empresa procure mantener respaldos de la información; Yo personalmente he sido víctima de robos de computadora y teléfono, afortunadamente se contaba con un respaldo de la información.

Nestor: y podríamos hablar que *¿se contaba con el 100% de información en esos respaldos?*

Ing. Fernando: no, la tecnología va cambiando y yo recuerdo cuando antes los respaldos se hacían cada tres meses, debido a que las capacidades de los recursos de almacenamiento no eran tan grandes como los de ahora, hoy en día entiendo que los respaldos se pueden hacer en línea y se hacen a la nube y esto permite que los respaldos sean casi al 100%, aunque para ello se deben de contratar servicios externos y creo que es interesante verificar si nuestro departamento de IT lo está aplicando así.

Nestor: en esos eventos de robo, *¿perdió alguna información importante?*

Ing. Fernando: sí, lamentablemente se perdió información de casi un mes, correos electrónicos, archivos etc.

Nestor: hemos hablado un poco de las tecnologías, herramientas y del sector, adicionalmente se ha comentado un poco referente al personal y un punto específico que quisiera me comentara, es

si dentro del sector es usual que los empleados ya sea trabajando para la organización o cuando se finaliza el contrato de trabajo, *¿comparten información de clientes, proveedores o posiblemente de proyectos que ustedes tengan en marcha?*

Ing. Fernando: es un riesgo constante que no solo las empresas de logística están expuestas, pero en el caso en particular nuestro, es especialmente delicado porque no solo estamos manejando información propia de la empresa, sino que también manejamos información de nuestros clientes, esto nos obliga a ser más estrictos y tener cuidado con la información de los clientes, por ejemplo en el caso de las mudanzas nosotros trabajamos con las pertenencias de diplomáticos o ejecutivos de alto nivel, que son trasladados de El Salvador a otro país y por requisitos de aduana nos vemos en la necesidad de recolectar información privada: como identidad, domicilio al que se trasladan etc.; obviamente la necesidad de contar con procesos que garanticen la privacidad de la información es muy importante, y es necesario contar con un control sobre el acceso de los colaboradores de la información y el custodio de la misma.

Es difícil, porque la misma tecnología facilita el traslado de la información de un medio a otro y en la medida que esos medios se multipliquen el riesgo aumenta, al estar sujetos a la rotación de personal y gente que se retira es una preocupación que constantemente tenemos y se está viendo cómo reducir ese riesgo.

Nestor: hablando de reducción de riesgo *¿considera usted importante generar políticas de seguridad informática, que puedan beneficiar a las empresas del sector disminuyendo estos riesgos?,* sobre todo si las políticas son basadas en una normativa de standard mundial como lo es la norma ISO 27001.

Ing. Fernando: la norma ISO es bien importante, nosotros tenemos el beneficio de contar con buenas prácticas de empresas multinacionales que ya han pasado por estos procesos, y que por operar en mercados más desarrollados (Europa, Estados Unidos y Asia) ellos ya tienen implementados algunos sistemas de control para reducir esos riesgos, esto es una ventaja dado que contamos con algunas buenas prácticas, y respecto a la norma ISO son reconocidas y son buenas prácticas probadas alrededor del mundo, nosotros contamos con una certificación en esta norma.

Nestor: *¿Ustedes ya tienen una certificación en las normas ISO?*

Ing. Fernando: sí, la empresa está certificada desde el 2005 con la Norma ISO 9001 con la versión 2008 y actualmente estamos en el proceso de pasar a la nueva versión 2015, esta es una norma de calidad que básicamente regula y da los parámetros de los requisitos del cliente y poder brindar los servicios ofrecidos de la mejor manera, permite llevar controles, medidas correctivas, hacer mejoras, es básicamente este el escope (alcance) de la norma.

Nestor: *¿Considera oportuno que las empresas del sector de logística como lo es Comca Internacional cuenten con políticas de seguridad informática basadas en la Norma ISO:27001?*

Ing. Fernando: yo creo que sí, es muy importante ya que todos estamos conscientes que vivimos en un país de alto riesgo, los índices de crimen nos colocan en el tope de la lista, obviamente el tener un control de la información y normas de seguridad es sumamente importante. Nosotros a pesar de contar con buenas prácticas adoptadas por requisitos de las empresas multinacionales (agentes, navieras) que representamos, estas nos dan herramientas y una base sobre las que podemos trabajar, pero lo correcto ese ponerlas en el contexto no solo de la empresa, de la industria des sector de la logística y transporte, sino también en el contexto del país en el que vivimos, algunos aspectos la legislación actual no los regula y por lo tanto las empresas debemos tomar

nuestras propias medidas, esto hace sumamente importante el contar con métodos, procedimientos y políticas que garantice la seguridad informática.

Nestor: Gracias por el tiempo que nos ha brindado para conversar un poco acerca de estos temas.

Ing. Fernando: un gusto y estamos a la orden para ampliar cualquier información.

Oficinas de Comca Internacional, Blvd. Acero No 12-A, Antiguo Cuscatlán

Lunes, 21 de agosto del 2017 2:30 PM