UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

“MODELO DE GESTIÓN PARA LA SEGURIDAD EN LA INFORMACIÓN DE MONITOREO EN LÍNEA PARA EMPRESAS DE TRANSPORTE MARÍTIMO Y AÉREO BASADO EN LOS OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS (COBIT 5)”

TRABAJO DE GRADUACIÓN PRESENTADO POR:

BONILLA GALDÁMEZ, WALBER EDGARDO

REYES PÉREZ, KARLA GABRIELA

ZAVALA LAZO, KARLA JACQUELINE

PARA OPTAR AL GRADO DE:

LICENCIADO EN CONTADURÍA PÚBLICA

SEPTIEMBRE, 2017

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

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 Mendoza de Hernández
Coordinador General de Procesos de Graduación Facultad De Ciencias Económicas	:	Licenciado Mauricio Ernesto Magaña Menéndez
Coordinador de seminario	:	Licenciado Daniel Nehemías Reyes López
Docente Director	:	Licenciado Mario Hernán Cornejo Pérez
Jurado Examinador	:	Licenciado Mario Hernán Cornejo Pérez
		Licenciado Daniel Nehemías Reyes López
		Licenciado Carlos Ernesto Ramirez

Septiembre, 2017

San Salvador, El Salvador, Centro América.

AGRADECIMIENTOS

A Dios todo poderoso y la virgen Maria por la vida, la familia, sabiduría, bendiciones, y oportunidades recibidas. A mi familia por su incondicional apoyo, mis padres por sus oraciones y su motivación para ser mejor cada día, a todos mis hermanos, en especial a Fredy por su incondicional apoyo, a mis sobrinas. Amigos y compañeros y a una persona especial que me ha brindado su apoyo y motivación.

A mis compañeras de trabajo de graduación por su amistad, apoyo y dedicación. A nuestro asesor por su enseñanza, dedicación y su profesionalismo. Por ultimo a la Universidad de El Salvador por haberme formado a través de sus docentes con principios éticos y profesionales.

Bonilla Galdámez, Walber Edgardo

A Dios gracias por ser el motivo de mi inspiración para alcanzar mis sueños y metas propuestas, este día doy por culminada una de las más importantes en mi vida profesional, gracias a la sabiduría y fuerza adquirida por medio de Él.
A mi padre y madre que han sido un apoyo fundamental a lo largo de este camino, por todo lo que han sacrificado para verme triunfar, sus oraciones y ánimos en momentos difíciles, este logro también es de ellos; a cada miembro de mi familia y amigos que me han animado y apoyado en todo momento.
A mi equipo de trabajo de graduación por hacer vida este sueño que iniciamos juntos y ahora lo vemos culminado, y a cada uno de los docentes que compartieron sus conocimientos para formar una profesional en mí.

Reyes Pérez, Karla Gabriela

A Dios todo poderoso y a la Virgen Maria, por darme discernimiento, sabiduría, fortaleza y todo lo necesario para alcanzar la meta propuesta.

A mis abuelos por su apoyo y comprensión a lo largo de mi carrera y por ser parte de este triunfo, a mis padres por su esfuerzo y por siempre estar a mi lado, mis hermanas por ser mi motivo de inspiración, a mi asesor especialista por su enseñanza, orientación y confianza, a los docentes que formaron parte de mi formación, a mi equipo de trabajo de graduación por su apoyo, unión y dedicación para poder concluir satisfactoriamente esta meta, mis amigas/os por apoyarme y darme palabras de aliento, motivándome a seguir adelante y a todos aquellos que de una u otra forma son parte de este éxito.

Zavala Lazo, Karla Jacqueline

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ANEXOS

RESUMEN EJECUTIVO

El comercio electrónico en los últimos años ha incrementado considerablemente y las empresas de transporte marítimo y aéreo que están a la vanguardia de este tipo de transacciones han incrementado su volumen de operación, ya que los compradores necesitan que sus mercancías sean transportadas desde su origen, dichos compradores han demandado que se les informe sobre la ubicación de sus mercancías, por lo que las empresas han desarrollado aplicaciones las cuales generan un valor agregado al servicio de transporte que estas empresas brindan, y es necesario que se gestionen todos riesgos relacionados a este tipo de información, el encardo de TI y gerencia general juega un papel importante en la identificación de vulnerabilidades, por tal sentido se desarrolló un trabajo de investigación, el cual consiste en proponer un modelo de evaluación para la gestión de riesgos en seguridad de información enfocada en las empresas de transporte marítimo y aéreo que brindan servicio de monitoreo en línea aplicando COBIT 5.

` La investigación está enfocada en el desarrollo de un modelo de gestión de riesgos en seguridad de la información para empresas de transporte marítimo y aéreo que brindan el servicio de monitoreo en línea ubicadas en el área metropolitana de San Salvador. Con la aplicación del modelo, permitirá a las empresas identificar posibles amenazas, alteraciones o extravió de información que pudiera ocurrir y que es de mucha importancia para las empresas mantenerla resguardada, ya que es indispensable evaluar la suficiencia de las medidas de control que adopta las empresas, con la evaluación e identificación que le permitirá disminuir la posibilidad de que los riesgos se materialicen, con el propósito de salvaguardar los recursos informáticos y que la información que se produce sea confiable y útil para la correcta y oportuna toma de decisiones.

El desarrollo de un modelo de evaluación basado en el marco de referencia en seguridad COBIT 5 Para la Seguridad de la Información que permita la medición del impacto y probabilidad de que un evento ocurra será útil , ya que al contar con este modelo basado en un marco de referencia de mucha calidad y prestigio a nivel internacional en materia de seguridad, el cual es emitido por la Asociación de Auditoría y Control de Sistemas de Información(ISACA) por sus siglas en inglés que es un organismo emisor de normas técnicas en materia de gestión de tecnologías de información, así como certificaciones internacionales como lo es la Certificación de Auditor de Sistemas de Información (CISA) por sus siglas en inglés para auditores de sistemas de información que en la actualidad es de mucho prestigio contar con dicha certificación a nivel mundial.

El trabajo de campo fue desarrollado con el apoyo de las empresas dedicadas al sector, la in La investigación fue hipotética deductiva, utilizando para la misma instrumentos y técnicas para la recolección de datos, de los cuales se realizó un análisis de resultados lo cual finalizo en un diagnóstico general. En el instrumento de evaluación se analizó cada pregunta y sus respectivas respuestas para conocer la importancia de presentar un modelo de gestión de seguridad en la información, la información obtenida nos sirvió de base para plasmar el caso práctico, que es la propuesta desarrollada. La encuesta utilizada nos sirvió para dar respuesta a la hipótesis planteada.

De acuerdo a los resultados se concluye que las empresas de transporte marítimo y aéreo que brindan el servicio de monitoreo en línea no poseen un modelo de gestión de seguridad de la información que les permita identificar los riesgos relacionados a la confidencialidad, integridad y disponibilidad de la información brindada a través de la aplicación.

INTRODUCCIÓN

La tecnología y las formas de comunicarse cambian permanentemente, por lo que las empresas de transporte marítimo y aéreo, han hecho uso de herramientas tecnológicas que les permiten brindar información a sus clientes de forma más oportuna y fiable. Para que los datos que se brindan en las aplicaciones web utilizadas por estas empresas sean útiles a sus usuarios, deben proporcionar una seguridad razonable de su veracidad.

En tal sentido, las empresas deben implementar controles de seguridad, que les permitan minimizar los riesgos de proceso y muestra de información errónea o viciosa, y que en la medida que los usuarios encuentran consistencia en los servicios de monitoreo en línea (*tracking online*) con los estatus y ubicación exacta de sus envíos, tendrán confianza hacia la empresa, lo cual le generará valor agregado y fidelidad.

Por lo antes descrito, en el capítulo I se describe el planteamiento del problema, los antecedentes y el desarrollo de la logística a nivel internacional y nacional, y el desarrollo de aplicaciones tecnológicas utilizadas en la organización que han contribuido al auge de operaciones comerciales, que facilitan la fluidez en la comunicación.

Además en el capítulo II, se desarrolló un marco teórico que incluye el diseño de instrumentos, guías y procedimientos aplicados a la seguridad de la información. Posteriormente; el diseño metodológico como respaldo en el proceso investigativo en el cual se definirá tipo de estudio, unidad de análisis, universo, muestra, instrumentos y técnicas a utilizar en la investigación, procesamiento de la información, análisis e interpretación de los datos procesados y diagnóstico de la misma.

En el capítulo III se formulará la hipótesis, identificando la variable dependiente e independiente y su operacionalización, la técnica para la recopilación de información fue la encuesta por medio de la cual se realizó la tabulación de los datos y análisis de resultados.

El objetivo de la investigación será desarrollar un modelo de gestión para la seguridad en la información, que permitirá a las empresas de transporte marítimo y aéreo gestionar y garantizar la integridad de la información, tomando como base marcos técnicos basados en buenas prácticas para la gestión de recursos de Tecnologías de información (TI), con énfasis en la seguridad, que son emitidos por organismos internacionales y que son implementados por empresas en todos los rubros de manera general, por lo que se adaptaran al rubro de este tipo de empresas tal como se expresa en el capítulo IV.

CAPITULO I. PLANTEAMIENTO DEL PROBLEMA

1.1 Situación problemática de la seguridad de la información

Durante los años ochenta y principios de los noventa la seguridad lógica se centraba en proteger los equipos de los usuarios, proporcionando seguridad a ordenadores y sus sistemas operativos para evitar que estos dejaran de funcionar correctamente, centrándose también en la protección de virus informáticos.

Con la aparición del internet y la creación en 1991 de la red mundial (*World Wide Web, w.w.w*) y su uso globalizado a nivel empresarial, la seguridad lógica comenzó a enfocarse hacia la conectividad de redes o creación de redes (*networking*), protegiendo los equipos y servidores accesibles públicamente a través del internet, controlando a niveles periféricos por medio de dispositivos corta fuegos (*Firewalls*), dando la posibilidad tecnológica de poder conectarse, llevando implícitamente la aparición de vulnerabilidades que podían ser explotadas exponiendo la información crucial para el negocio, siendo accesible gracias a la conectividad.

La seguridad de la información ha venido tomando mucha importancia en los últimos años, ya que para las empresas contar con procedimientos de seguridad les ha permitido restringir el acceso y minimizar la vulnerabilidad de la información, lo cual evita que terceros puedan manipular datos sin autorización. Muchas empresas han estado expuestas a filtraciones, tanto que han sufrido ataques informáticos, los que les han ocasionado pérdidas económicas y de confianza de sus clientes, proveedores. La vulnerabilidad ha existido en empresas pequeñas como en grandes corporaciones, tal es el caso que han recibido ataques compañías como PlayStation en abril de 2011, Adobe en 2013 y Yahoo en el 2016 (El Economista, 2011). Los efectos en el mercado de

dichos ataques y robo de información han sido perjudiciales, cuantificando las pérdidas en millones de dólares. Con el fin de fortalecer la seguridad en puntos muy concretos se han desarrollado modelos de gestión para distintos sectores, tales como, bancario, servicios, comercio, lo que les ha permitido minimizar el riesgo de filtración y así aseguran el bien más valioso para las empresas: la información. (Gelbstein, 2011)

Las formas de gestionar seguridad lógica ha evolucionado, debido a que las empresas conocen la importancia que tiene su información, por lo cual se han visto obligadas a invertir en medidas y controles de seguridad que les permitan minimizar el riesgo de la manipulación inadecuada, errores y alteraciones.

En la actualidad a nivel informático se considera que el activo más valioso en una empresa es la información que esta posee, y debido a que existen atacantes o grupos organizados que aprovechan la vulnerabilidad de los sistemas tecnológicos y las redes de telecomunicación, para acceder a los datos más críticos y sensibles a través de personal especializado en ataques informáticos. Se han desarrollado procedimientos que permiten gestionar las vulnerabilidades, ya que se considera que no se puede lograr tener la información 100% segura, pero se logra disminuir o eliminar las deficiencias, además, se han desarrollado herramientas que permiten medir el retorno de la inversión en seguridad, como lo es la herramienta ROSI por su siglas en inglés (Return on security investment).

1.2 Enunciado del problema

La falta de seguridad en la información es el resultado de no implementar mecanismos de control que la mantengan a salvo aplicando barreras y procedimientos

que resguarden el acceso a la misma y solo les permitan acceder a las personas autorizadas.

Las empresas dedicadas al transporte marítimo y aéreo en el área metropolitana de San Salvador que brindan el servicio de monitoreo en línea, tienen riesgos en la gestión de su información ya que no cuentan con un modelo que les permita garantizar que la información está segura y que no será expuesta a terceros o personas afines a la entidad tales como empleados, ex empleados, proveedores, clientes insatisfechos, empresas dedicadas a la misma actividad (competencia).

El hurto, exposición inadecuada de la información o pérdida de esta, son algunas de las consecuencias a la que se enfrenta la empresa hoy en día, ya que por ser un recurso valioso puede ocasionarle una mala imagen o la pérdida de sus clientes, es por ello que es necesario la implementación de un modelo de gestión para la seguridad de la información que le permita tener un mayor control sobre su uso, tal es el caso del hackeo que sufrió la empresa Maersk Line en junio de 2017, en el cual todos sus sistemas fueron infiltrados por el virus *ramsonware* llamado *Petya* (Sarabia, 2017)

Los sistemas de información que utilizan las empresas de transporte marítimo y aéreo para brindar el servicio de monitoreo en línea deben tener controles, entre los cuales se pueden identificar como necesarios los siguientes:

- Limitar el acceso a determinadas aplicaciones, programas o archivos mediante claves o a través de la criptografía. Al implementar este control se garantizará que solo personas autorizadas tengan acceso a información clasificada como confidencial.

- Otorgar los privilegios mínimos a los usuarios de las aplicaciones informáticas. Es decir solo proporcionar privilegios al personal que los necesita para desempeñar su actividad.

- Controlar que la información que se ingrese, procese y muestre, a través de sus aplicaciones informáticas sea íntegra y confiable.

- Que la información no pueda ser modificada por usuarios que tengan acceso a ella, solamente personal autorizado.

- Diseñar un procedimiento que le permita recolectar información actualizada, real y verídica de la ubicación de los envíos.

- Implementar lineamientos y estándares que deberán seguir para la implementación en la seguridad de la información. Deben ser aplicados en las empresas y dar cumplimientos a ellos.

- Los encargados de TI deben tener la competencia necesaria, lo que permita detectar cualquier anomalía, de manera que sus procedimientos sean suficientes y adecuados.

¿Cómo afecta a la empresas de transporte marítimo y aéreo ubicadas en el área metropolitana de San Salvador que brindan el servicio de monitoreo en línea no contar con un modelo de gestión de riesgos para la seguridad de la información?

1.3 Justificación de la investigación

El desarrollo de la investigación está orientado en las empresas de transporte marítimo y aéreo ubicadas en el área metropolitana de San Salvador que brindan servicio de monitoreo en línea, para que implementen controles para gestionar los

riesgos de la información que se brinda en línea a los usuarios. Se han tomado como referencia los Objetivos de Control para la Información y Tecnologías relacionadas (COBIT, por sus siglas en inglés, versión 5).

En COBIT 5 Para la seguridad de la información, se definen metas específicas que se han tomado como referencia y se adaptaron de acuerdo a los objetivos que las empresas de transporte marítimo y aéreo que brindan servicio de monitoreo en línea han estipulado, ya que como organización tienen propósitos que cumplir dentro del servicio que brindan. Por lo cual deben estar integrados con todos los procesos de la organización.

La seguridad de la información es una de las prioridades que las organizaciones deben plantearse, y esto se logra al revisar cada proceso que se ha implementado para la recolección y procesamiento de datos, por lo tanto, COBIT 5 procesos catalizadores, con su enfoque de integrar procesos, da los lineamientos a considerar para elaborar un modelo de gestión de seguridad de la información íntegro, es decir, que el modelo incluya todos los procesos donde se genera información en la empresa, tomando en consideración el principio dos de COBIT 5 cubrir la empresa de extremo a extremo, y principio tres, aplicar un modelo de gestión de seguridad de información único integrado.

En la actualidad es importante contar con la disponibilidad de la información, lo cual según COBIT es poder acceder a ella en el momento que se necesite, siempre y cuando se cuente con la debida autorización para hacerlo y que esta información sea útil para la toma de decisiones. (ISACA, 2012)

Cada día se utilizan más las herramientas tecnológicas para transferir información a los usuarios, las empresas de transporte han hecho propias aplicaciones

tecnológicas que les permiten informar a sus clientes sobre el estatus de sus envíos, las operaciones de comercio internacional (importaciones, exportaciones) aumentan cada año, así como las compras por internet en aplicaciones como, Amazon o eBay, las cuales hacen los envíos a través de empresas de mensajería (*Courier*), así como, a través de Correos de El Salvador, que actualmente está implementando su servicio de correo expreso (*EMS por sus siglas en ingles*). (Correos de El Salvador, 2017) (Gelbstein, 2011) y brindará a los usuarios un número para que estos puedan monitorear sus envíos.

1.3.1 Novedoso

Se considera novedoso el desarrollo de la investigación, ya que en la actualidad no existe un modelo de gestión en la seguridad de la información enfocado a este tipo de empresas, y debido al auge del comercio electrónico (*e-commerce*), estas empresas están interesadas en brindar a sus usuarios información fiable y oportuna a fin de generar un valor agregado al servicio, lo cual solo lo lograrán, gestionando adecuadamente su información a través de una gestión adecuada.

1.3.2 Factibilidad

La factibilidad de la investigación se consideró en dos aspectos:

La investigación se considera factible, ya que existen normas técnicas y buenas prácticas a las que se tuvo acceso, las cuales tratan sobre la gestión de la seguridad de la información, así como tesis, libros sobre gestión de riesgos, entre otros, los que contienen procedimientos que han sido adaptados para que sean aplicados por las empresas de transporte que brindan servicio de monitoreo en línea.

1.3.2.1 De campo

La investigación se realizó en las empresas de transporte marítimo y aéreo, que brindan servicio de monitoreo en línea ubicadas en el área metropolitana de San Salvador, a las que se tuvo acceso para evaluar sus procedimientos aplicados para la seguridad de la información a través de encuestas.

1.3.2.2 Apoyo institucional.

Para desarrollar la investigación, se contó con docentes asignados por la Escuela de Contaduría Pública de la Universidad de El Salvador, con conocimientos técnicos relacionados al área de estudio, quienes garantizaron que se cumpliera con los objetivos y metas esperados por la coordinación de los trabajos de graduación.

1.3.3 Utilidad social

Con el desarrollo de la investigación se pretende aportar a las empresas de transporte que brindan servicio de monitoreo en línea un modelo de gestión para la seguridad de la información, con el propósito que su servicio de monitoreo en línea agregue valor a sus empresas, generando confiabilidad y preferencia en sus clientes, lo cual se vea reflejado en los resultados financieros y operativos de las entidades.

Así mismo, se pretende que esta investigación sea útil para los profesionales en contaduría pública, encargados del área de TI, ya que podrán evaluar la gestión de seguridad de la información implementada por la entidad y la disponibilidad de la misma hacia el cliente. Tomando como base de medición el modelo que será propuesto al final de la investigación.

1.4 Objetivos de la investigación

1.4.1 Objetivo general

Proponer un modelo de gestión para la seguridad de la información para las empresas de transporte marítimo y aéreo que brindan servicio de monitoreo en línea.

1.4.2 Objetivos específicos

- ✓ Elaborar un manual de seguridad que le permita a la entidad establecer las políticas del modelo de gestión.

- ✓ Desarrollar procedimientos de seguridad que le permita a la entidad minimizar el nivel de exposición de su información.

- ✓ Elaborar una lista de verificación que permita identificar los procedimientos de seguridad aplicados.

1.5 Hipotesis

La implementación de un modelo de gestión de riesgos basado en "COBIT 5 Para la seguridad de la información" permitirá a las empresas de transporte marítimo y aéreo que brindan servicio de monitoreo en línea, garantizar, la confidencialidad, integridad y disponibilidad de la información.

CAPITULO II. MARCO TEÓRICO

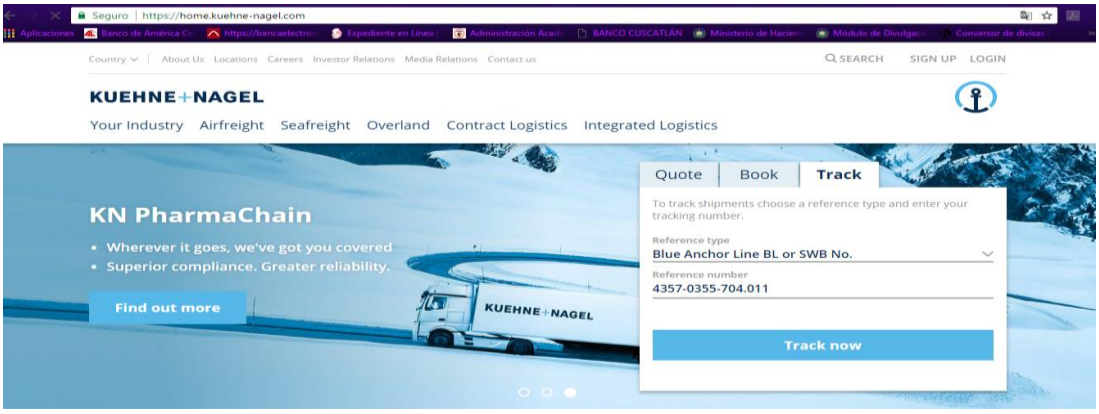
2.1 Estado actual de la seguridad de la información

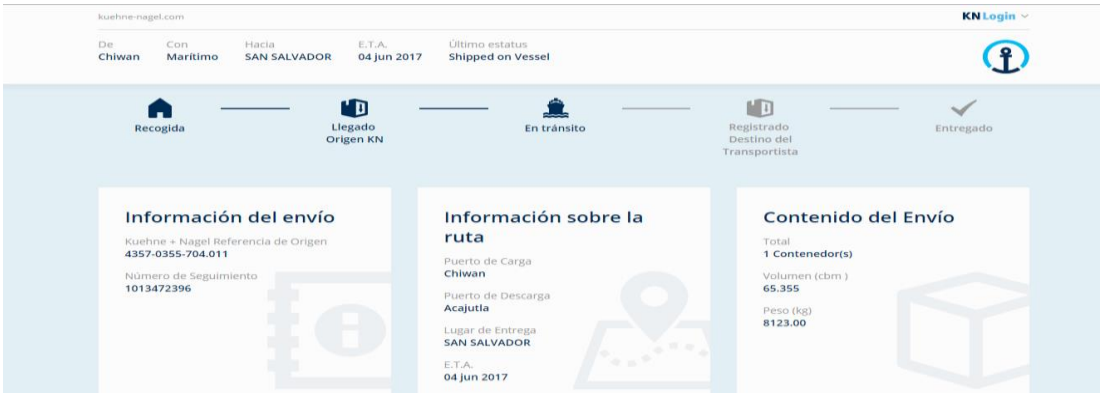
Las empresas de transporte de carga han cambiado su forma de comunicarse, ya que el mercado les ha exigido brindar información más oportuna, debido a que los clientes demandan calidad en sus servicios; y obtener información de forma inmediata sobre la ubicación de las mercancías es uno de los elementos principales del servicio.

Haciendo uso de las herramientas tecnológicas las empresas de transporte han desarrollado aplicaciones que les permiten brindar información del estatus de la mercadería, empresas de transporte multinacionales como Maersk, Hamburg Sud, DHL, Kuehne Nagel, PCS, han desarrollado aplicaciones web y últimamente aplicaciones móviles.

En la siguiente ilustración podrá observar un ejemplo de la aplicación en línea que posee la empresa Kuehne Nagel:

Figura 1: Aplicación de monitoreo en línea K+N





Fuente: https://www.kn-portal.com/faqs/shipment_tracking_help/

Antes de las aparición de las primeras computadoras, la seguridad en la información de las empresas era rigurosa ya que se hacían uso de bodegas, archivadores y toneladas de papeles para resguardar datos de clientes, contabilidad y todo documento que para la empresa fuera de importancia; la amenaza a la seguridad de la información solamente podía darse al momento de ocurrir desastres naturales ya que esta información era bastante compleja y no cualquiera podía extraer información discretamente de la empresa.

Con la aparición de la computación y las redes de internet todo comenzó a digitalizarse, de manera que las empresas ya no necesitaban de bodegas y tantos papeles para resguardar su información, cuando esta podían resumirla en un disco duro el cual ocupaba un espacio muy pequeño, pero al momento de darse esta evolución en medio de tantas ventajas que traía consigo también traía un nuevo problema para el mundo de la informática, la información era mucho más práctica de transportar por lo tanto estaba más expuesta a ser hurtada o alterada, y es por ello que se comenzaron a desarrollar sistemas de seguridad para resguardar la información.

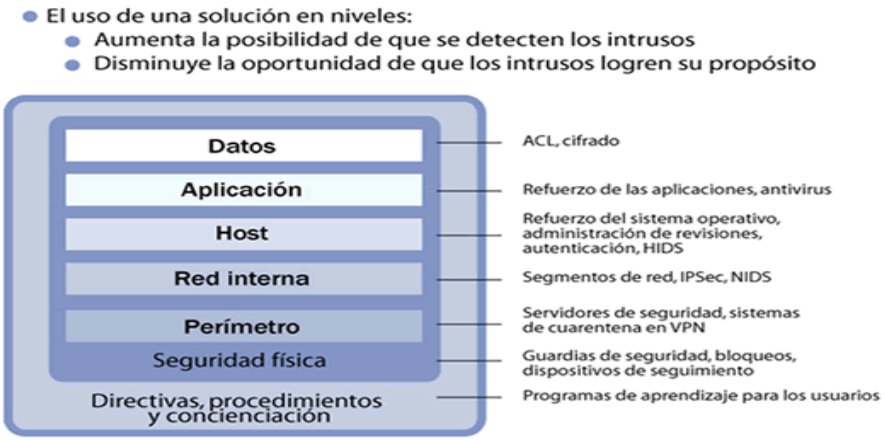
Con la evoluciones de las redes en internet se comenzaron a dar los famosos hackers en la red en el cual la información ya no solamente corría el peligro de ser hurtada físicamente sino por medio de las redes, por lo que surgieron programas de seguridad y aplicaciones las cuales procuraban brindar seguridad a los sistemas que las entidades poseían. (https://visualstudio316.wordpress.com/2016/10/06/implementacion-de-la-seguridad-en-redes-lan/)

Como resultado las empresas se enfocaron en adquirir los mejores sistemas de seguridad para el resguardo de su información, pero se debe tener en claro que la seguridad de la información es un conjunto de herramientas y procedimientos tecnológicos, sociales y culturales que buscan proteger y defender la información de cualquier agente interno o externo que pueda afectar sus tres principios básicos los cuales son confidencialidad, integridad y disponibilidad. La seguridad no es un término estrictamente tecnológico; de nada servirá tener una red saturada de complejos firewalls, sistemas de detección de intrusos, políticas y passwords si el administrador de la red deja su contraseña escrita en un papel y pegada en una esquina del monitor o anotada en una libreta. No existe sistema operativo que tenga la posibilidad de ver a través de la

pantalla quien está digitando la contraseña en el teclado, por lo que un descuido por parte de una persona puede ser fatal para la seguridad a nivel global de una organización.

Es por ello que comienzan a surgir nuevas formas de obtener una mayor seguridad en el resguardo de la información y es así como los líderes en tecnología inician una serie de estudios, en mejorar la enseñanza respecto a la seguridad ya sea físicamente como informáticamente, Microsoft se da la tarea de esquematizar de una manera más práctica la estructura de organización de la seguridad por lo que a continuación se presenta dicho esquema.

Figura 2: Estructura organizacional de la seguridad



Fuente: Curso Seguridad Microsoft Technet Learning Center.

En esencia, esquematizar en niveles este concepto enseña principalmente que la seguridad es un aspecto transversal, que va desde la información misma hasta las dependencias físicas donde se encuentra la información, pasando por un conjunto de procesos que se relacionan entre sí. Aun así lo más destacable del modelo de defensa en profundidad es que todos estos procesos involucran al ser humano y una solución de

seguridad que no tenga considerado el impartir conocimientos respecto al tema a cada uno de los usuarios está expuesta al fracaso.

Los niveles de seguridad no solamente deben ser internos sino externos, tal y como lo describe la ilustración 2, se debe tener un equilibrio entre ambos para que la seguridad en la empresa sea confiable.

Hasta hace un tiempo, se creía que el villano de la información era el hacker, una persona de aspecto tenebroso, oculta tras un computador de última tecnología en algún lugar del mundo. Sin embargo, esto ha pasado a ser un mito de la informática; muchas veces el enemigo puede estar dentro de la misma empresa, y no necesariamente es un experto en programación ni un maestro en informática. Es más, para poder atacar los sistemas hoy en día basta con saber hacer una buena búsqueda en los distintos motores que nos provee Internet. Si uno escribe "Hacking Manual" en google aparecen más de 4 millones de resultados, muchos de ellos con completísimos manuales en español e inglés de cómo entrometerse en los sistemas de información. A esto sumamos que existen muchos errores humanos con respecto a la seguridad de la información y uno de ellos es precisamente creer que todos los posibles factores de peligro de la información se encuentran en el exterior.

Este error ha sido reafirmado por numerosas estadísticas que demuestran que un gran porcentaje de los problemas de seguridad se producen en el interior mismo de las empresas. Empleados insatisfechos, usuarios curiosos y por sobre todo poco consientes del impacto que pueden tomar sus acciones en una red son uno de los principales dolores de cabeza que los encargados de seguridad tienen a diario.

Todos estos antecedentes no hacen más que reafirmar teorías tan simples y poderosas como el modelo de defensa en profundidad. No sirve absolutamente de nada tener el perímetro protegido con decenas de Firewalls, Proxies, IDS y otras herramientas de seguridad si cometemos el descuido de no cambiar nunca la contraseña del administrador de la red, incluso aunque hayan cambiado a dicho administrador.

La seguridad informática consiste en asegurar que los recursos del sistema de información de una organización sean utilizados de la manera que se decidió y que la información que se considera importante no sea fácil de acceder por cualquier persona que no se encuentre acreditada. Existen dos tipos de seguridad: la seguridad lógica que incluye aplicaciones para la seguridad, herramientas informáticas, etc. y la seguridad física que incluye la infraestructura, mantenimiento eléctrico, anti-incendio, humedad, y todo daño ocasionado por desastres naturales.

Las amenazas a la seguridad informática pueden ser programas malignos como virus, espías, troyanos, gusanos, phishing, spamming, entre otros. Los cuales pueden provocar la pérdida de información; pero para ellos existen técnicas, aplicaciones y dispositivos que permiten evitar estas amenazas como por ejemplo aplicaciones de protección, encriptación de información y uso de contraseñas, capacitación a los usuarios sobre las nuevas tecnologías y amenazas que pueden traer. https://www.microsoft.com/conosur/technet/articulos/seguridadinfo/

En la actualidad la información es el objeto de mayor valor para las empresas, el avance de la informática y de las redes de comunicación nos muestras una nueva forma de observarla donde la forma de medir los objetos son en bits y bytes estos poseen diferentes formas y ocupan un lugar en otra dimensión, pero esto no quiere decir que por eso su valor disminuye al contrario muchos de ellos tienen un valor superior. Por

ello la seguridad de la información es muy importante ya que afecta directamente al gobierno, institutos, empresas e individuos.

Las empresas en la actualidad han adoptado marcos de referencia para obtener un mejor control en la seguridad de su información; que es su activo más valioso, entre los cuales se pueden mencionar: COBIT 5, ISO 27002, ITIL; ya que estos incluyen buenas practicas que son eficientes para la gestión de la seguridad. Entre las prácticas sugeridas están las siguientes: la elaboración de manuales de seguridad que se encargan de dirigir todo el sistema, este expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales del modelo de gestión de la seguridad de la información. Así como procedimientos que aseguran que se realicen de forma eficaz la planificación, operación y control en los procesos de la seguridad. Además instrucciones para realizar listas de verificación, formularios que describen como se realizan las tareas y actividades específicas relacionadas con la seguridad. Adicional sugieren elaborar registros que proporcionen una evidencia objetiva del cumplimiento de los requisitos del modelo de gestión que la entidad haya decidido implementar.

Estos procedimientos son eficaces para muchos tipos de empresas y la forma en que se aplican depende del rubro a que se dedique la empresa y la información con la que esta cuenta, por ejemplo, una institución financiera aplica procedimientos más estrictos que una comercializadora de productos varios ya que la información se considera más confidencial y la ausencia de esta puede ocasionar pérdidas económicas, de credibilidad y confianza en sus clientes.

Por lo tanto el nivel de exposición a los riesgos será proporcional a la pérdida o impacto al que la entidad está expuesta.

2.2 Principales definiciones

Riesgo: estimación del grado de exposición a que una amenaza se materialice sobre la información causando daños o perjuicios a la empresa. El riesgo indica lo que le podría pasar a la información si no se protege adecuadamente. Es importante considerar qué características son de interés en cada tipo de información.

Análisis de riesgos: proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una la información.

Gestión de riesgos: selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

Seguridad de la información: asegura que dentro de la empresa, la información está protegida contra su divulgación a usuarios no autorizados (confidencialidad), modificación inadecuada (integridad) y su falta de acceso cuando se la necesita (disponibilidad).

COBIT: objetivos de control para la información y tecnologías relacionadas.

Infraestructura de TI: conjunto de dispositivos físicos y aplicaciones de software requeridos para operar en una la entidad. Esta infraestructura también incluye un conjunto de servicios a nivel empresarial presupuestado por la gerencia, que abarca las capacidades tanto humanas como técnicas.

2.3 Legislación aplicable

Dentro de la base legal referente a la gestión de la seguridad de la información para las empresas de transporte marítimo y aéreo, está en los artículos 87 y 42, respectivamente del Código Aduanero Uniforme Centroamericano y su respectivo Reglamento, el cual faculta a la autoridad aduanera para que pueda fiscalizar y solicitar cualquier información referente a las importaciones y exportaciones, 4 años posteriores a la aceptación de la declaración de mercancías.

2.4 Normativa técnica aplicable

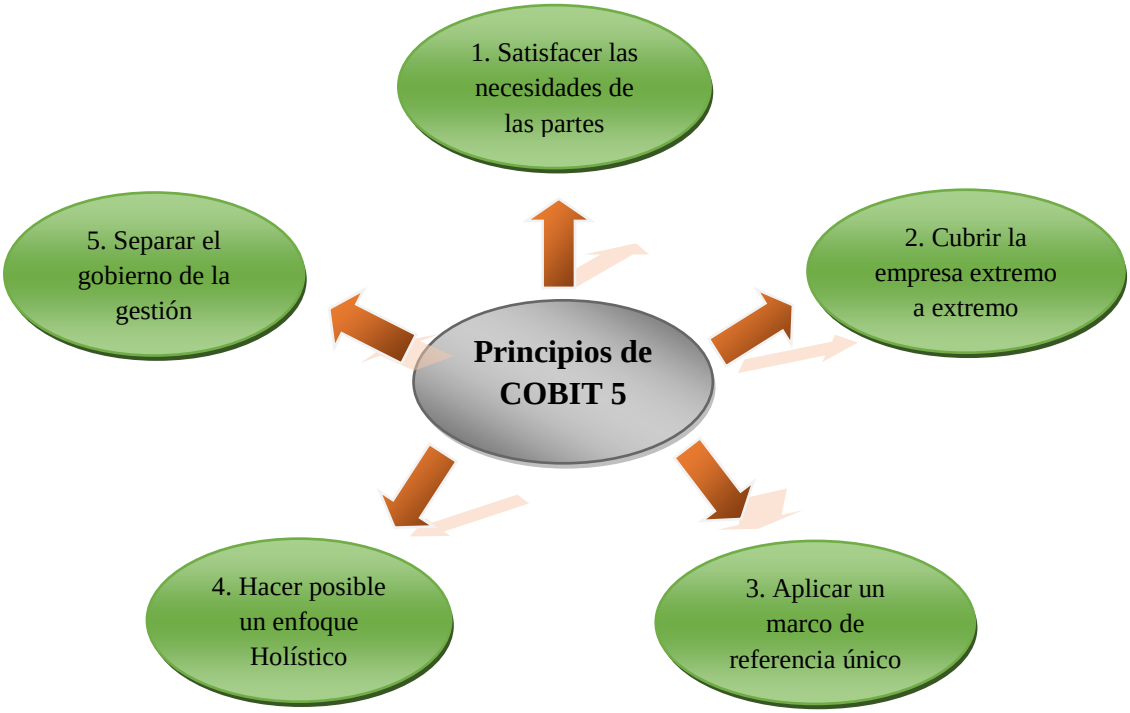
Para la gestión de seguridad de la información existen modelos de gestión que contienen mejores prácticas emitidos por organismos internacionales, que permiten tomarlos como marcos de referencia ‘’*framework*’’ para diseñar procedimientos de gestión, entre ellos los Objetivos de Control para la Información y Tecnologías Relacionadas 5, (COBIT 5 por su siglas en ingles) para la seguridad de la información, emitido por la Asociación de Auditoría y Control en Sistemas de Información, (Information Systems Audit and Control Association ISACA por su siglas en inglés), el cual es en el que se fundamenta el modelo propuesto en este trabajo.

2.4.1 COBIT 5 para Seguridad de la Información

Incluye buenas prácticas en gestión de sistemas de información y ofrece una visión holística en temas de gestión de seguridad y gobierno de TI, que se complementa con guías y publicaciones adicionales, específicas para gestión de riesgos, cumplimiento, seguridad, aseguramiento y gobierno de TI. La implementación de COBIT 5 se puede concatenar con otros marcos de referencia usados en las empresas, esto permitirá agregar valor en los procesos de TI.

COBIT 5 para la seguridad de la información se basa en 5 principios los cuales permiten una gestión integrada dentro de las entidades, ya que los recursos de TI no deben estar aislados del gobierno corporativo, como se muestra en la siguiente ilustración:

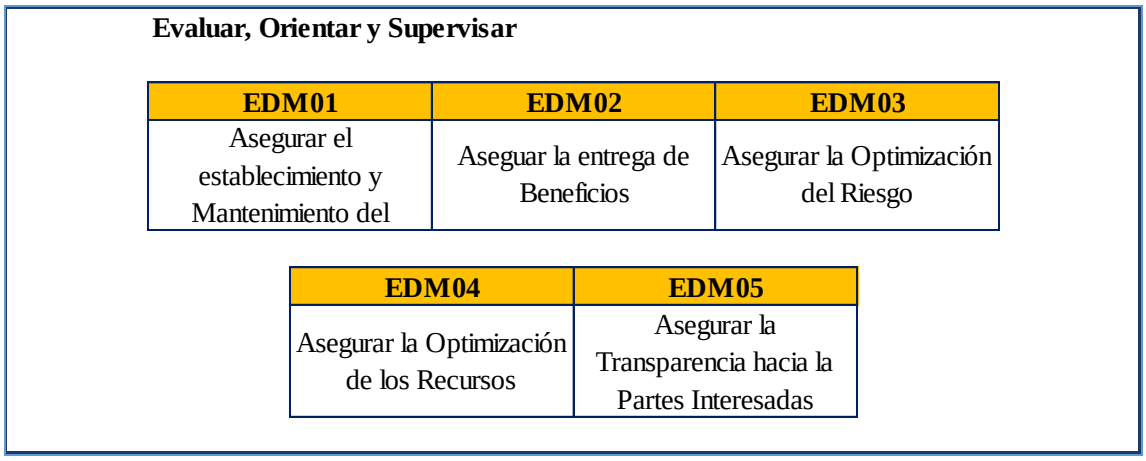
Figura 3: Principios de COBIT 5



Fuente: COBIT 5 para la seguridad de la información

El enfoque de COBIT 5, es separar la gestión de recursos de TI con el gobierno corporativo, y a cada uno le asigna diferentes roles a los cuales se le asocian diferentes procesos que se hacen visibles mediante el modelo de procesos, que incluye procesos de gestión y procesos gobierno, cada grupo con sus propias responsabilidades. Lo anterior lo divide en cinco dominios, de los cuales uno pertenece al gobierno corporativo con los roles de evaluar (E) orientar (D) y supervisar (M) EDM. Tal como se muestra en la siguiente figura.

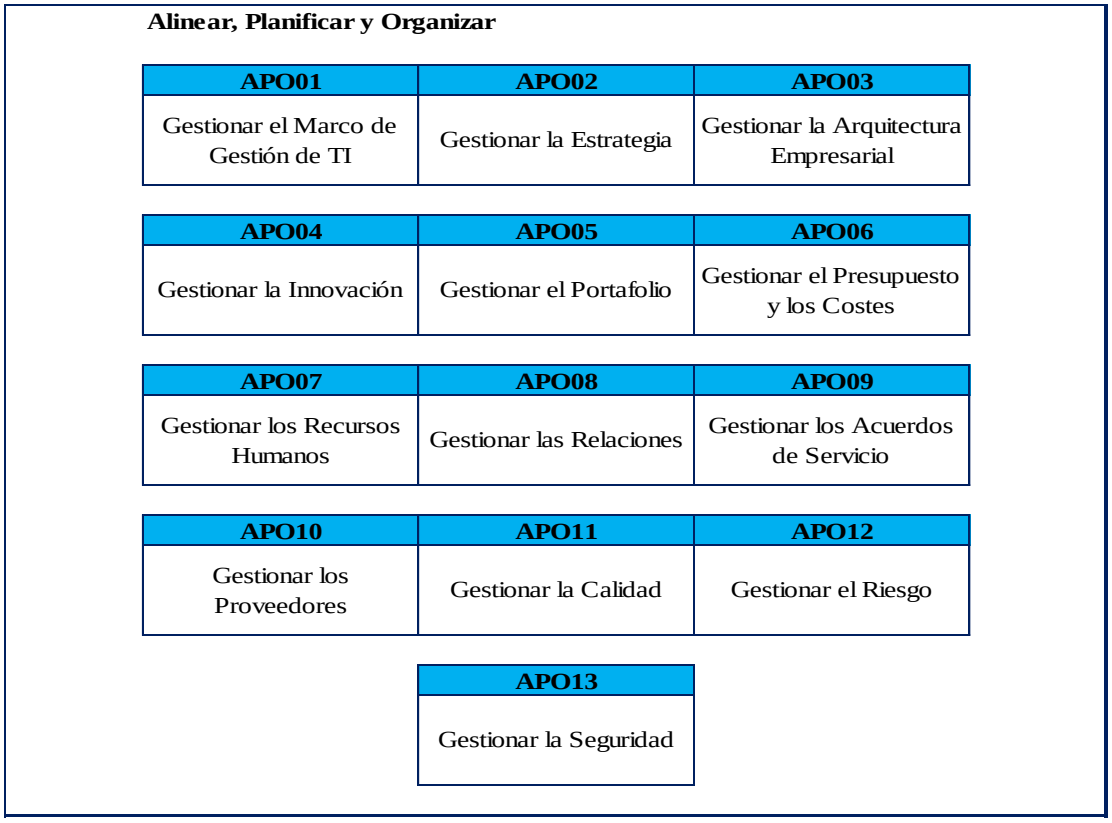
Figura 4: Procesos de Gobierno de TI Empresarial



Fuente: Cobit 5 Para la Seguridad de Información

Los roles de la gestión de TI empresarial están divididos en 4 dominios, los cuales se muestras en las siguientes figuras.

Figura 5: Procesos para la gestión de TI empresarial



Supervisar, Evaluar y Valorar

MEA01	MEA02	MEA03
Supervisar, Evaluar y Valorar Rendimiento y Conformidad	Supervisar, Evaluar y Valorar el Sistema de Control Interno	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos

Construir, Adquirir e Implementar

BAI01	BAI02	BAI03
Gestionar los Programas y Proyectos	Gestionar la Definición de Requisitos	Gestionar la Identificación y la Construcción de Soluciones

BAI04	BAI05	BAI06
Gestionar la Disponibilidad y la Capacidad	Gestionar la Introducción de Cambios Organizativos	Gestionar los Cambios

BAI07	BAI08	BAI09
Gestionar la Aceptacón del Cambio y de la Transición	Gestionar el Conocimiento	Gestionar los Activos

BAI010
Gestionar la Configuración

Entregar, dar Servicio y Soporte

DSS01	DSS02	DSS03
Gestionar las Operaciones	Gestionar las Peticiones y los Incidentes del Servicio	Gestionar los Problemas

DSS04	DSS05	DSS06
Gestionar la Continuidad	Gestionar los Servicios de Seguridad	Gestioanr los Controles de los Procesos del Negocio

Fuente: COBIT 5 para la seguridad de la información

COBIT 5 para la seguridad de la información define gobierno y gestión de la siguiente manera.

Gobierno: ‘’*Asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas*’’.

Gestión: ‘’*planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales*’’.

Dentro del rol de gobierno se tiene el proceso ADM01 el cual sugiere que se debe evaluar, orientar y supervisar las estrategias tomadas en relación a la seguridad de la información, tal como se muestra en la siguiente figura:

Figura 6: Proceso ADM01 para la seguridad

EDM01 Metas y métricas del proceso específicas de seguridad	
Metas del proceso específicas de seguridad	**Métricas relacionadas**
1. El sistema de gobierno de seguridad de la información está integrado en la empresa.	• Número de procesos de negocio y de TI en los que la seguridad de la información está integrada • Porcentaje de procesos y prácticas con clara trazabilidad a los principios • Número de brechas de seguridad de la información relativas a no conformidades con las directrices de comportamiento ético y profesional
1. Se obtiene garantía sobre el sistema de gobierno de la seguridad de la información.	• Frecuencia de revisiones independientes del gobierno de la seguridad de la información • Frecuencia de los informes sobre el gobierno de la seguridad de la información al comité ejecutivo y al consejo de administración • Número de auditorías y revisiones internas/externas • Número de no-conformidades

EDM01 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gobierno	**Desde**	**Descripción**	**Descripción**	**Hacia**
EDM01.01 Evaluar el sistema de gobierno. Identificar y comprometerse continuamente con las partes interesadas de la empresa, documentar la comprensión de los requerimientos y realizar una estimación del actual y futuro diseño del gobierno de TI de la empresa.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Factores internos y externos del entorno (obligaciones legales, regulatorias y contractuales) y tendencias	Principios que rigen la seguridad de la información	EDM01.02 APO01.01 APO01.03 APO01.04 APO02.01 APO02.05 APO12.03

Fuente: COBIT 5 para la seguridad de la información

Dentro de los procesos de gestión de TI empresarial se tienen, APO12 Gestionar el riesgo, APO13 Gestionar la seguridad, DSS04 Gestionar la continuidad y DSS05 Gestionar los servicios de seguridad, los cuales proporcionan una guía básica acerca de cómo definir, operar y supervisar un sistema para la gestión general de seguridad, los cuales están diseñados tomando como referencia que la seguridad se encuentra presente a lo largo de toda la empresa, con aspectos de seguridad de la información dentro de cada actividad y proceso realizado.

El objetivo del proceso APO12 sobre la gestión de riesgo de seguridad de la información, es minimizar hasta los niveles de riesgos asumidos por la dirección, en base a los recursos que esta le proporcione evaluando los costos y beneficios, según se muestra en la siguiente figura.

Figura 7: Proceso APO12-Gestión de riesgo

APO12 Gestionar el Riesgo	**Área: Gestión** **Dominio: Alinear, Planificar y Organizar**
Descripción del Proceso de COBIT 5 Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.	
Declaración del Propósito del Proceso de COBIT 5 Integrar la gestión de riesgos empresariales relacionados con TI en la gestión general de riesgos corporativos (ERM) y equilibrar los costes y beneficios de gestionar riesgos empresariales relacionados con TI.	
APO12 Metas y Métricas del Proceso específicas de Seguridad	
Metas del Proceso específicas de Seguridad	**Métricas Relacionadas**
1. Se dispone de un perfil de riesgo, completo y vigente, para la tecnología, las aplicaciones y la infraestructura, dentro de la empresa.	• Existencia, vigencia y completitud de los perfiles de riesgo.
2. La respuesta a incidentes de seguridad de la información forma parte del proceso global de gestión del riesgo para proporcionar la capacidad de actualizar el portafolio de gestión del riesgo.	• Número de incidentes con valoraciones de riesgo adecuadamente diseñadas

Fuente: COBIT 5 Para la seguridad de la información

Cada proceso de COBIT 5 está respaldado con prácticas claves que dentro de ellas nos brindan una guía ordenada de actividades a realizar a fin de identificar, analizar, gestionar y responder a los riesgos; el modelo de gestión de riesgo está basado en el proceso APO12 de COBIT5 para Seguridad de la Información y entre sus procesos están los siguientes:

- APO12.01 Recopilación de datos: Identificar y recopilar datos relevantes para hacer posible una identificación, análisis y notificación efectiva de riesgos relacionados con TI.
- APO12.02 Analizar el riesgo: Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tengan en cuenta la relevancia para el negocio de los factores de riesgo.
- APO12.03 Mantener un perfil de riesgo: Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados.
- APO12.04 Expresar el riesgo**.** Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de forma oportuna a todas las partes interesadas para una respuesta apropiada.
- APO12.05 Definir un portafolio de acciones para la gestión de riesgos: Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio.
- APO12.06 Responder al riesgo. Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.

Las prácticas de gestión de la seguridad de la información para el proceso APO13 Gestión de seguridad son las siguientes:

- APO13.01 Establecer y mantener un SGSI: Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineado con los requerimientos de negocio y la gestión de seguridad en la empresa.
- APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información: Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa. Asegurar que las recomendaciones para implementar las mejoras en seguridad se basan en casos de negocio aprobados, se implementan como parte integral del desarrollo de soluciones y servicios y se operan, después, como parte integral de las operaciones del negocio.
- APO12.03 Supervisar y revisar el SGSI: Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. Corregir las no conformidades para prevenir recurrencias. Promover una cultura de seguridad y de mejora continua.

Asimismo, Cobit 5 Para la Seguridad de la información detalla procesos para la gestión de Entrega (D), Servicio (S) y Soporte (S) de los recursos de TI, lo cual se muestra como el dominio DSS. Dentro de este domino tenemos los siguientes procesos:

- DSS01 Gestionar operaciones: Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.

- DSS02 Gestionar peticiones e incidentes de servicio: Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes, recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes.

- DSS03 Gestionar problemas: Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora.

- DSS04 Gestionar la continuidad: Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.

- 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.

Para cada uno de los procesos existen prácticas claves, las cuales permiten redactar procedimientos a implementar, a fin de asegurar y mantener la disponibilidad de la información a través de la gestión de la continuidad de los servicios de TI.

CAPITULO III. METODOLOGÍA DE INVESTIGACIÓN

3.1 Enfoque y tipo de investigación

El tipo de estudio utilizado fue el hipotético deductivo, ya que a través de éste se pudo observar el problema en estudio, operar hipótesis y sus variables, deducir las causas y medir sus efectos, lo que se tomó como base para proporcionar un modelo de gestión de seguridad de la información que sirva como orientación para la Dirección de las empresas de transporte marítimo y aéreo ubicadas en el área metropolitana de San Salvador.

3.2 Delimitación de la investigación

3.2.1 Temporal

La investigación se realizó a partir de la entrada en vigencia de COBIT 5 para la seguridad de la información en el año 2012, al 31 de agosto de 2017

3.2.2 Espacial

Se desarrolló la investigación en las empresas de transporte marítimo y aéreo, que brindan servicio de monitoreo en línea ubicadas en el área metropolitana de San Salvador, que estén debidamente autorizadas por la Dirección General de Aduanas (DGA).

3.3 Sujetos y objeto de estudio

3.3.1 Unidades de análisis

Las unidades de análisis consideradas en la investigación fueron los profesionales encargados del departamento de TI, así como los gerentes de las empresas que se dedican al transporte marítimo y aéreo que brindan servicio de monitoreo en línea ubicadas en el área metropolitana de San Salvador.

3.3.2 Población y marco muestral

El universo está conformado por las empresas de transporte marítimo y aéreo ubicadas en el área metropolitana de San Salvador que están autorizadas por la Dirección General de Aduanas, siendo un total de 129, de las cuales 26 empresas se dedican al transporte aéreo específicamente (Courier) y 108 al transporte marítimo. (Ver anexo 1)

Para la determinación de la muestra se utilizó la fórmula estadística para poblaciones finitas y la selección se realizó por medio del método aleatorio simple con aplicabilidad sobre las empresas de transporte marítimo y aéreo que cumplían las siguientes condiciones:

- Que cuenten con departamento o encargados de TI.
- Que brinden servicio de monitoreo en línea.

La fórmula utilizada para determinar el tamaño de la muestra es la siguiente:

$$n = \frac{N \times Z^2 \times p \times q}{e^2 (N-1) + Z^2 \times p \times q}$$

Donde:

n = Tamaño de la muestra

N = Población

Z = Coeficiente de confianza

p = Probabilidad de éxito de que la problemática exista

q = Probabilidad de fracaso

e = Margen de error

Se tomó un nivel de confianza 90%, indicando que de cada 100 respuestas obtenidas se esperaba que 90 estuvieran dentro de las expectativas de la investigación. El margen de error dispuesto a aceptar fue el 10%.

Sustituyendo:

n =?

N = 129 empresas de transporte marítimo y aéreo.

Z = 1.645 nivel de confianza 90%

p = 75% (probabilidad de éxito)

q = 25% (probabilidad de fracaso)

e = 10% nivel de error

$$n= \frac{129 \times 1.645^2 \times 0.75 \times 0.25}{0.10^2 \times (129-1) + 1.645^2 \times 0.75 \times 0.25}$$

$$n= \frac{65.45}{1.28 + 0.5073}$$

$$n = \frac{65.45}{1.7873} \qquad n = 36.6195$$

La muestra determinada fue de 37 empresas.

3.3.3 Variables e indicadores

Variable independiente:

Modelo de gestión para la seguridad de la información basado en COBIT 5.

Variable dependiente:

Seguridad de la información**.**

Indicadores

Variable dependiente: Seguridad de la información.

- Medir a través de instrumentos técnicos los niveles de seguridad que se alcancen.
- Medir si la entidad ha logrado minimizar de los riesgos al aplicar el modelo de gestión.
- Verificar si la entidad tiene identificados los riesgos.
- Verificar los tipos de controles que implementa la entidad.

Variable independiente**:** modelo de gestión para la seguridad de la información basado en COBIT 5.

- Nivel de conocimiento de la administración del modelo de gestión.

- Factibilidad de aplicación de procedimientos de seguridad.
- Disponibilidad de la administración para la gestión de los riesgos identificados.
- Nivel de riesgo aceptado por la entidad

3.4 Técnicas, materiales e instrumentos

El instrumento que se utilizó para la recolección de información fue la encuesta, la cual se hizo a los profesionales encargados del departamento de TI y gerentes de las empresas de transporte marítimo y aéreo y se formuló con una serie de preguntas enfocadas a la gestión de seguridad de la información. (Ver anexo 2)

3.5 Procesamiento y análisis de la información

La información obtenida por medio de las encuestas fue procesada en Microsoft Office, con lo que se elaboraron tablas y gráficas que facilitaron el análisis e interpretación de los datos, interpretando las variables con los resultados obtenidos, la tabulación de los datos con sus respectivos gráficos, con la intención de medir porcentualmente si la problemática estipulada existe y si hay gestión de riesgos en seguridad por parte de los encargados de TI o gerentes de las empresas de transporte marítimo y aéreo.

3.6 Cronograma de actividades

El desarrollo de las actividades se realizó desde el mes de febrero hasta agosto del año 2017, tal como se muestra en la siguiente tabla.

Tabla 1 Cronograma de actividades

Actividad	2017																											
	Febrero				Marzo				Abril				Mayo				Junio				Julio				Agosto			
Elaboración de anteproyecto																												
CAPITULO I MARCO TEÓRICO																												
Planteamiento del problema																												
Delimitación de la investigación																												
Justificación de la investigación																												
Objetivos de la investigación																												
Marco teórico, conceptual, técnico y legal																												
CAPITULO II METODOLOGÍA DE INVESTIGACIÓN																												
Investigación de campo																												
Recolección de información																												
Tabulación de encuestas																												
Presentación y análisis de resultados																												
Diagnóstico																												
CAPITULO III PROPUESTA																												
Elaboración de propuesta																												
Entrega de propuesta																												
Verificación de propuesta																												
Entrega de propuesta final																												
Elaboración de conclusiones																												
Elaboración de recomendaciones																												
DEFENSA DE TRABAJO DE INVESTIGACIÓN																												

Fuente: Elaboración propia

3.7 Presentación de resultados

3.7.1 Tabulación y análisis de resultados

La tabulación de los resultados obtenidos a través del cuestionario permitió presentar en forma absoluta y porcentual las respuestas por cada pregunta, facilitando así el

análisis de los resultados y relacionándolos con las variables permitió determinar la importancia de la creación del modelo de gestión de seguridad de la información para las empresas de transporte marítimo y aéreo. (Ver anexo 3)

3.7.2 Diagnóstico

El total de la muestra determinada fue de 37 empresas de transporte autorizadas por la Dirección General de Aduana, representando así un 28% del total de la población. Considerando que el cuestionario fue respondido por gerentes generales y encargados de TI, los resultados obtenidos son representativos para toda la población.

El objetivo principal de la encuesta fue determinar la importancia de la creación de un modelo de gestión de seguridad para la información, obteniendo un 100% de respuestas favorables, lo que permite concluir que a pesar que solo el 38% de las empresas cuenta con gerente de TI y en el 49% los recursos de TI están bajo responsabilidad del gerente general; todas las empresas están conscientes de la importancia de aplicar procedimientos que permitan asegurar la confidencialidad, integridad y disponibilidad de la información.

La capacitación al personal encargado de la gestión de los recursos de TI es muy importante e indispensable para asegurar que los riesgos a los que están expuestas las empresas, sean mitigados hasta un nivel aceptable, solo el 49% de la población encuestada capacita al personal, determinando así la importancia de contar con un modelo de gestión de seguridad integral, el cual será de mucha utilidad, a pesar que el porcentaje de empresas que brindan capacitación a su personal es bajo, dentro de las que si lo hacen, se determinó que el área donde se brinda mayor capacitación es en lo

relacionado a la seguridad de la información con un 21%, seguido con un 18% en lo relacionado a la ética y la confidencialidad.

La gestión de riesgos se puede realizar solo si se tienen identificados, por lo que es muy importante que las empresas mantengan un portafolio actualizado de todos los riesgos a los que están expuestos con énfasis a los relacionados al servicio de monitoreo en línea para poder brindar seguridad y satisfacción a los clientes, a pesar de la importancia de mantener identificados los riesgos, solo el 62% de las empresas tiene una lista en la cual se detallan las deficiencias en seguridad, la adecuada gestión de riesgos permite que los clientes puedan tener confianza en la información que se les brinda, esto se logra aplicando controles que permitan asegurar la integridad de la información, el 38% de las empresas encuestadas no posee procedimientos que le garanticen que datos mostrados sean íntegros y fiables.

La información es un recurso importante para las empresas y deben aplicar controles que les permitan mantenerla segura e inaccesible a personas ajenas a la entidad, estos controles deben incluir planes de acción que les permitan mitigar riesgos a un nivel aceptable y asegurar el resguardo de la información, estos procedimientos deben establecer medidas en caso de modificación, pérdida o robo, a pesar de la importancia de estos controles solo el 49% de las empresas encuestadas implementa planes de contingencia en caso de que pueda ocurrir un incidente.

Mantener la confidencialidad de la información es una de las prioridades que deben tener las empresas, esto se logra gestionando eficientemente las claves, contraseñas y límites de accesos a los usuarios según sus funciones, tanto para empleados como para los clientes, para que las contraseñas sean seguras se debe definir un periodo de actualización de claves y los caracteres que estas deben incluir, el 35%

de las empresas no cuenta con directrices y lineamientos específicos para el registro y control de los usuarios que utilizan el servicio de monitoreo en línea, una de las medidas de seguridad que las empresas pueden implementar es el límite de intento de acceso, al ingresar su clave errónea en varias ocasiones el usuario debe ser bloqueado, además se debe desarrollar un procedimiento para gestionar la reactivación del usuario.

Para que la información sea útil a los usuarios, esta debe estar disponible en el momento y lugar que se necesite, de lo contrario aun que los datos sean íntegros y fiables no les sarán útiles para la toma de decisiones, por lo tanto, dentro de la gestión de recursos de TI, los responsables de la seguridad deben asegurarse que la información sea accesible para todas las partes interesas y en el momento oportuno, para poder lograr que los usuarios puedan acceder en cualquier momento a la aplicación de monitoreo en línea y verificar la ubicación de sus mercancías, se debe asegurar la conexión a internet, la actualización de datos permanentemente y que los usuarios tengan los permisos necesarios para poder monitorear sus envíos desde sus computadoras, laptops o móviles, solo el 54% de las empresas se asegura de mantener la disponibilidad de la información y es necesario que las empresas implementen procedimientos para brindar buen servicio.

Esto permite evidenciar que mantener la información segura es muy importante para las empresas de transporte marítimo y aéreo, ya que en el desarrollo de sus operaciones se procesa y se brindan datos a través del servicio de monitoreo en línea, confidencial e importante, para poder mantener la confidencialidad, disponibilidad e integridad de la información, se debe gestionar los recursos de TI e implementar procedimientos en todos los procesos e involucrar a todo el personal para aplicarlos eficientemente. Por lo anterior, es de mucha utilidad implementar un modelo de gestión

de seguridad que incluya buenas prácticas, tales como las descritas en Cobit 5 Para la Seguridad de la Información, de las empresas encuestadas de manera unánime se obtuvo respuesta favorable en la utilidad de un modelo integro que involucre a la empresa de extremo a extremo en todos los procesos. Además puede aseverarse que el modelo será de mucha utilidad para empresas pequeñas o nuevas en el sector ya que al gestionar sus recursos de TI de forma práctica y eficiente tendrán más oportunidad de competir con empresas transnacionales, las cuales cuentan con más recursos para implementar modelos de seguridad de la información.

CAPITULO IV PROPUESTA DE SOLUCIÓN

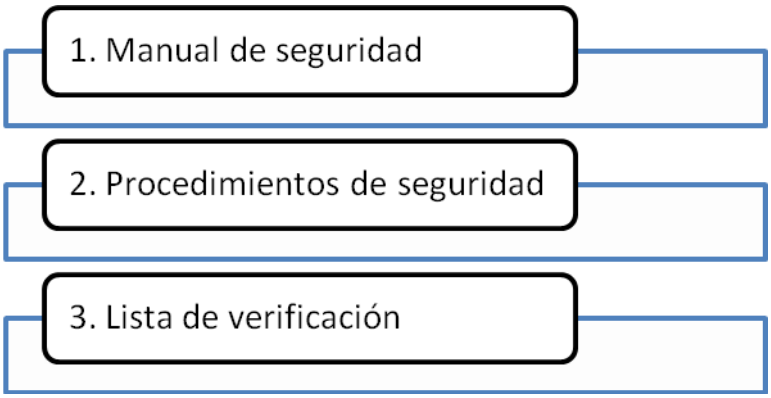
4.1 Planteamiento del caso

El modelo para la gestión de seguridad de la información fue elaborado tomando como marco de referencia los objetivos de control para información y tecnologías relacionadas, COBIT 5 Para la Seguridad de la Información, ha sido diseñado para la implementación en empresas de transporte marítimo y aéreo que brindan el servicio de monitoreo en línea. Para el desarrollo del trabajo se han tomado como objeto de estudio las empresas ubicadas en el área metropolitana de San Salvador. El objetivo del modelo es desarrollar procedimientos que permitan minimizar los riesgos relacionados a la información a los que están expuestas este tipo de empresas, ya que una adecuada gestión del riesgo permite anticipar eventos que al ocurrir ocasionarían un impacto significativo, tales como: la pérdida de ella, debido que al brindar el servicio de monitoreo en línea, la cantidad de datos que se procesa a través de sistemas informáticos es muy delicada e indispensable para el funcionamiento y continuidad de las empresas.

La implementación del modelo será de mucha importancia para la gestión de riesgos y permitirá la creación de valor con la optimización de recursos. Adicionalmente se reducen costos, mejora de la imagen empresarial, mayor relación con los clientes, proveedores y demás partes interesadas y cumplimiento de los requisitos legales tal como el resguardo de información por un periodo de tiempo establecido. Los procedimientos descritos en COBIT 5 para la seguridad de la información han sido adaptados a los procesos y actividades propias de las empresas de transporte, lo cual permitirá alcanzar los objetivos que la dirección ha implementado.

El modelo de gestión de riesgos en seguridad propuesto denominado ‘’Modelo de gestión para seguridad de la información para las empresas de transporte marítimo y aéreo que brindan servicio de monitoreo en línea’’ está integrado en tres partes, sugeridas por COBIT 5, permitiendo la aplicación de manera integral, según su principio número dos ‘’cubrir la empresa de extremo a extremo’’, las cuales se muestran en la siguiente figura.

Figura 8: Contenido de la propuesta de solución



Manual de seguridad: Documento que describe en materia de seguridad alcance, objetivos, responsabilidades, políticas y directrices principales de la compañía.

Procedimientos de seguridad: Descripción de las acciones específicas a realizar por la compañía con la intención de reducir los riesgos a los que está expuesta la información asegurando a su confidencialidad, integridad y disponibilidad.

Lista de verificación: Descripción de procedimientos específicos con la intención de verificar que se aplique lo establecido por la compañía, con el propósito de identificar las deficiencias y limitantes en la gestión de riesgos, e implementar cambios de mejora a fin de reducir los riesgos a un nivel aceptable.

4.2 Estructura del plan de solución

La estructura y contenido del modelo propuesto denominado ‘’**Modelo de gestión para la seguridad de la información para las empresas de transporte marítimo y aéreo que brindan servicio de monitoreo en línea’’** es el siguiente

CONTENIDO	REFERENCIA COBIT 5
1. Manual de seguridad	APO13
1.1 Objetivo	APO13.01
1.2 Alcance	APO13.01
1.2.1 Seguridad	
1.2.2 Cubrir todos los procesos	
1.3 Políticas	APO13.01
1.4 Responsabilidades	APO13.01
1.5 Identificación de riesgos	APO12.03
1.6 Parámetros de medición	APO13
1.7 Mejora continua	APO13.03
1.8 Definiciones	
2. Procedimientos de seguridad `	APO11.02, APO12.05
2.1 Confidencialidad	
2.1.1 Gestión de la seguridad para los usuarios finales	DSS05.03

2.1.1.1 Creación de usuarios	DSS05.03
2.1.1.2 Gestionar la integridad de la información	DSS05.03
2.1.1.3 Gestionar el acceso y control remoto	DSS05.03
2.1.2 Gestión de usuarios y credenciales	DSS05.04
2.1.2.1 Administración de usuarios	DSS05.04
2.1.2.2 Control de accesos	DSS05.04
2.1.2.3 Pistas de auditoría	DSS05.04
2.1.3 Gestión de acceso físico a activos de TI	DSS05.05
2.1.3.1 Registro y controles de acceso	DSS05.05
2.1.3.2 Políticas de acceso	DSS05.05
2.1.3.3 Medidas de seguridad preventivas	DSS05.05

2.2 Integridad

2.2.2 Protección de software malicioso	DSS05.01
2.2.2.1 Actualización de antivirus	DSS05.01
2.2.2.2 Capacitación al personal sobre el uso de correo e internet	DSS05.01
2.2.2.3 Encriptación de datos	DSS05.01
2.2.3 Gestión de salida de información sensible	DSS05.06
2.2.3.1 Control de dispositivos móviles	DSS05.06
2.2.3.2 Control de correos electrónicos	DSS05.06
2.2.3.3 Procedimientos de destrucción de información	DSS05.06

2.3 Disponibilidad

2.3.1 Gestión de proveedores de servicios de TI	APO10
2.3.1.1 Conocimiento y selección del proveedor	APO10.02
2.3.1.2 Gestión de contratos	APO10.04
2.3.1.3 Gestión de riesgos en suministro	APO10.04
2.3.2 Gestión de continuidad a los servicios	DSS04
2.3.2.1 Desarrollar un plan de continuidad de negocio	DSS04.01

2.3.2.2 Procedimientos de capacitación a usuarios	DSS04.06
2.3.2.3 Gestión de respaldo de información	DSS04.07
2.3.3 Gestión de la seguridad en la red y conexión	DSS05.02
2.3.3.1 Políticas de seguridad	DSS05.02
2.3.3.2 Transmisión de datos en la red	DSS05.02
2.3.3.3 Configuración de equipos en red	DSS05.02

3. Lista de verificación (check list)	APO11.04, APO13.03
3.1 Verificación de confidencialidad	
3.2 Verificación de integridad	
3.3 Verificación de disponibilidad	

4.3 Beneficios y limitantes

4.3.1 Beneficios de la aplicación del modelo de gestión de seguridad

Al utilizar COBIT 5 para Seguridad de la Información en la elaboración del modelo de gestión de riesgos, se cuenta con prácticas claves que proporcionan una serie de procedimientos eficaces relacionados con la seguridad de la información, que al integrarlos en un modelo aplicable a las empresas de transporte, da resultados positivos en la administración de riesgos tales como:

- Integración de la seguridad de la información en todos los procesos de la empresa.
- Facilita la toma de decisiones con conocimiento y conciencia del riesgo.
- Aplicación de medidas de prevención, detección y recuperación de información.
- Facilita la medición del impacto de los incidentes relacionados con la seguridad de la información

- Incentiva a la innovación y la competitividad con el uso eficiente de sistemas de información.
- Concientización de la importancia de implementar medidas de seguridad para información.
- Medición del costo-beneficio en la inversión de medidas de seguridad.
- Gestión eficiente de la infraestructura de TI.
- Proporciona una adecuada respuesta a incidentes.
- Define políticas específicas y eficaces en la gestión de riesgos.
- Integra buenas prácticas de gestión de riesgos relacionados con otros marcos de referencia.

4.3.2 Limitantes de la aplicación del modelos de seguridad

A pesar que COBIT 5 para la seguridad de la información es un marco integrado que desarrolla procedimientos eficaces con el enfoque de cubrir la empresa de extremo a extremo, al momento de aplicarlo se presentan las siguientes limitantes:

Tabla 2: Limitantes de la aplicación de modelos de gestión

Limitantes	Descripción
Recursos limitados para inversión en seguridad.	Los recursos con los que cuentan las empresas son limitados y la inversión en medidas de seguridad se ve limitada.
Falta de cultura de gestión de riesgos.	La concientización y capacitación en las empresas en poca o nula por la falta de cultura en la gestión de riesgos.

No se cuenta con una estructura organizativa definida para la toma de decisiones en materia de seguridad.	Para la implementación eficiente de los procedimientos de COBIT 5 para la Seguridad de la Información, es necesario que estén definidos los roles y responsabilidades del gobierno de TI y del personal encargado de la Gestión de TI
Personal encargado de TI no cuenta con las habilidades y competencias necesarias para la aplicación de medidas de seguridad eficaces	El resultado del estudio brindó información que el personal responsable de la gestión de TI es el gerente general, el cual no cuenta con personal capacitado en la gestión de TI.

4.4 Desarrollo del caso

4.4.1 Aspectos generales de la empresa

Consolidation Services, S.A. de C.V., es una empresa dedicada a prestar el servicio de transporte multimodal, siendo el marítimo el 85% de sus operaciones, y entre el aéreo y terrestre el 15% restante, está ubicada en Alameda Roosevelt No 3107, San Salvador.

Es una sociedad de capital alemán, fundada en el año 2012, cuenta con filiales en 105 países alrededor del mundo. Debido a que sus operaciones las realiza en coordinación con proveedores y clientes externos, les es necesario utilizar software que les permitan mantener informado de manera oportuna la ubicación y estatus de sus envíos.

El software en el que se procesa su información e integra toda la operación es Magaya, sistema que incluye los módulos descritos en la siguiente tabla.

Tabla 3: Módulos de Magaya

Consolidations Services S.A de C.V	
Módulos de Magaya	
1	Cuentas por cobrar
2	Cuentas por pagar
3	Almacenaje
4	Magaya TruckLive
5	Reportes financieros
6	Embarques marítimos
7	Embarques aéreos
8	Cotizaciones
9	Tarifas
10	Cheques

Para el servicio de monitoreo en línea Consolidation Services, S.A. de C.V., utiliza el módulo llamado Magaya LiveTrack, el cual a través del número de documento de transporte, (guía aérea, conocimiento de embarque BL) se verifica la ubicación de sus envíos, el estado y sus características. Así mismo, se genera una bitácora que muestra las fechas y la ruta que ha seguido la carga, esto les permite a los clientes anticiparse a la llegada de sus mercancías con documentos necesarios para realizar la nacionalización, tales como manifiesto de carga, facturas, declaración de importación.

1. Manual de seguridad **APO13**

1.1 Objetivo APO13.01

Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos y la estructura de la empresa y verificar que el plan establezca las prácticas de gestión y las soluciones de seguridad claras y apropiadas de acuerdo a los recursos, las responsabilidades y prioridades establecidas por la Dirección de Consolidations Services, S.A. de C.V. y así minimizar los riegos de seguridad de información identificados a un nivel aceptable.

1.2 Alcance APO13.01

Consolidations Services S.A de C.V establece el alcance del manual de seguridad en dos aspectos.

1.2.1 Aplicar procedimientos de seguridad de manera suficiente a fin de asegurar que la información cumpla con tres características de: confidencialidad, integridad y disponibilidad.

1.2.2 Cubrir todos los procesos

Se aplicarán procedimientos de seguridad a todos los procesos de generación de información, considerando que para lograr gestionar de forma integral los riesgos en seguridad, los procedimientos deben aplicarse en todos los niveles de la empresa, considerando así a todo su personal operativo, gerencial, gobierno y terceros que tengan vínculo comercial o legal con Consolidations Services S.A. de C.V.

1.3 Políticas APO13.01

Con la intención de gestionar los riesgos en seguridad de la información Consolidations Services S.A. de C.V. establece las siguientes políticas, que serán aplicables de acuerdo al alcance establecido por la dirección.

Tabla 4 : Políticas para la gestión de riesgo de seguridad de la información

Consolidations Services S.A. de C.V.	
Políticas para la gestión de riesgo de seguridad de la información	
Política	**Descripción**
Seguridad	
P 1 Políticas para la seguridad de la información	La empresa debe definir un conjunto de políticas de seguridad de la información aprobado por la Dirección y comunicarlo a todos los empleados y entidades relacionadas
P 2 Revisión de las políticas para la seguridad de la información	Se debe revisar en períodos de tiempos razonables las políticas de seguridad aplicadas y siempre que hayan cambios significativos a fin de asegurar que los procedimientos que se aplican permitan gestionar los riesgos a un nivel aceptable
Estructura y organización interna	
P 3 Roles y responsabilidades de la seguridad de la información	Todas las responsabilidades de seguridad deben estar asignadas al personal clave, para lo cual se debe elaborar un cuadro en el que se describan las responsabilidades.
P 4 Asignación de funciones	Las funciones conflictivas y las áreas de responsabilidad deben ser asignadas para reducir las oportunidades de modificaciones o uso no autorizado o mal intencionado de los activos de TI.
Contratación de personal	
P 5 Selección de personal	El personal que se contrate debe tener las aptitudes para desempeñarse en el puesto, para lo cual se elaborará un perfil que incluya los conocimientos y experiencia que debe tener el gerente de TI o persona encargada de la gestión de los recursos de TI.
P 6 Contrato individual de trabajo	Los acuerdos contractuales con empleados y contratistas deben establecer las responsabilidades para ambas partes en lo relacionado a la seguridad de la información.
Gestión de recursos de TI	
P 7 Inventario de activos	Los activos con los que cuenta la empresa deben estar registrados y debe realizar un inventario permanente.
P 8 Asignación de equipos	Se debe elaborar un registro en el cual se describa las características y estado de todos los equipos al momento de haberlos asignado al personal.

P 9 Uso de equipos	Los equipos deben ser usados solo para los fines establecidos por la dirección.
Resguardo de información	
P 10 Clasificación de la información	La información debe ser almacenada en términos de su valor, requerimientos legales, sensibilidad y criticidad a modificaciones o divulgación no autorizada.
P 11 Etiquetado de la información	Los medios en los que se almacene la información debe estar nombrado y claramente identificados
Control de acceso	
P 12 Política del control de acceso	Se deben implementar documentar y revisar procedimientos de control de acceso que permitan evitar el acceso a los recursos de TI
P 13 Acceso a redes y servicios de red	Se debe permitir el acceso a la red y servicios de red solo a los usuarios que hayan sido específicamente autorizados.
Gestión de usuarios	
P 14 Registro y anulación de usuarios	Para la asignación de accesos se debe implementar un procedimiento para la creación y anulación de usuarios.
P 15 Gestión de privilegios de derechos de acceso	Se debe restringir y controlar la asignación y uso de los privilegios de acceso
P 16 Cancelación y ajuste los derechos de acceso	Se deben cancelar 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
Seguridad física	
P 17 Perímetro de seguridad física	Se deben definir perímetros de seguridad para proteger áreas que contienen información e instalaciones.
P 18 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.
Equipo	
P 19 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.
P 20 Mantenimiento de equipo	El equipo debe recibir un correcto mantenimiento para asegurar su continuidad, disponibilidad e integridad.
Seguridad de las operaciones	

P 21 Procedimientos de operación documentados	Los procedimientos de operación deben documentarse y estar disponibles a todos los usuarios que lo necesiten.
P 22 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.
Protección de virus y software malicioso	
P 23 Controles contra software malicioso	Se deben implementar controles de detección, prevención y recuperación para protegerse contra software malicioso, así mismo se debe aplicar una apropiada concientización a todos los usuarios.
Copias de seguridad	
P 24 Copia de seguridad de la información	Se deben aplicar procedimientos que permitan mantener copias de seguridad en cualquier momento, este respaldo debe mantenerse confidencial, íntegro y disponible

1.4 Responsabilidades APO13.01

La dirección de Consolidations Services S.A. de C.V., asignará roles y funciones al personal de acuerdo al área en la cual se desempeñen, por lo tanto al momento de contratar se verificarán las competencias de cada persona, para asegurarse que cumplan con el perfil establecido para el desempeño eficiente de sus obligaciones.

Se establecerá un cuadro de roles en el que se muestren de forma específica las responsabilidades en materia de seguridad de la información para cada función. Asimismo, se determinará el perfil que debe cumplir la persona encargada del departamento de TI o responsable de la custodia de los recursos de TI, tal como se muestra en la siguiente tabla.

Tabla 5: Perfil de Gerente de TI

Perfil del Gerente de TI
Conocimiento

* Programas informáticos, políticas, procedimientos

* Estándares de seguridad de la información

* Actividades del negocio

Habilidades técnicas

* Amplia experiencia en operaciones informáticas y aplicaciones online

* Conocimientos sólidos de sistemas operativos Windows/LINUX,

* Métodos de autenticación

* Cortafuegos, enrutadores (router), servicios web.

Habilidades de comportamiento

* Habilidad para la gestión de proyectos y personal

* Sólidas habilidades de comunicación y mediación

* Sólidas técnicas de gestión del tiempo

Fuente: Cobit 5 Para la Seguridad de la Información

El personal clave o de alta gerencia será el responsable que se apliquen los procedimientos de seguridad a todos los procesos, para lo cual se identificará como GG el Gerente general o CEO, GTI el gerente de TI o encargado de recursos de TI, GA Gerentes de ares específicas, tal como se detalla en la siguiente tabla.

Tabla 6 Responsabilidades para la gestión de riesgo

Consolidations Services S.A. de C.V.		
Responsabilidades para la gestión de riesgo de seguridad de la información		
No	**Descripción**	**Responsable**
1	Elaboración y actualización del manual de gestión de riesgos	GG
2	Aplicación del modelo de seguridad	GTI
3	Divulgación del modelo de seguridad	GG
4	Evaluación de la aplicación de procedimientos	GTI
5	Informar del estado de seguridad de la información relacionadas con TI	GTI
6	Recoger y analizar datos del rendimiento y de cumplimiento relativos a seguridad de la información y gestión del riesgo de la información.	GTI

7	Establecer, acordar y comunicar el rol del GTI	GG
8	Desarrollar políticas y procedimientos de seguridad de la información.	GTI
9	Aprobar políticas y procedimientos de seguridad de la información.	GG
10	Validar los requerimientos en seguridad de la información con las partes interesadas, patrocinadores del negocio y clientes	GG
11	Evaluar de necesidad de inversión en activos de TI	GTI
12	Aprobar la inversión en activos de TI	GG
13	Escalar al miembro responsable de seguridad de la información pertinente los problemas identificados en seguridad	GA
14	Aportar la opinión de los especialistas al responsable de seguridad cuando sea relevante, por ejemplo, de representantes de auditoría interna, RRHH, legal, riesgo, oficial de gestión de proyectos, oficial de cumplimiento, Tramitadores Aduanales.	GA
15	Asegurar que la gestión del entorno y de las instalaciones se adhiere a los requerimientos en seguridad de la información.	GTI
16	Gestionar medidas de seguridad para el acceso físico a los activos de TI.	GTI
17	Aprobar medidas de seguridad para el acceso físico a los activos de TI.	GG
18	Gestionar la seguridad de las redes y la conectividad.	GTI
19	Proporcionar formas de mejorar la eficiencia y la eficacia de la función de seguridad de la información (por ejemplo, mediante formación del personal de seguridad de la información; documentación de procesos, tecnología y aplicaciones; y la estandarización y automatización del proceso).	GTI
20	La responsabilidad completa del programa de seguridad de la información de la empresa.	GG

Fuente: Cobit 5 Para la Seguridad de la Información.

1.5 Identificación de riesgos APO12.03

Consolidations Services S.A. de C.V., mantendrá una lista actualizada de los riesgos en seguridad a los que está expuesta, con el objetivo de verificar permanentemente los procedimientos preventivos, de detección y correctivos aplicados identificando su probabilidad y su impacto.

Para lo anterior se clasificará el impacto del riesgo como alto, medio y bajo, utilizando la misma clasificación para su probabilidad de ocurrencia, así mismo, se usa el color rojo cuando se tenga una medición alta, amarillo para el medio y verde para un nivel bajo, como se muestra en la siguiente tabla.

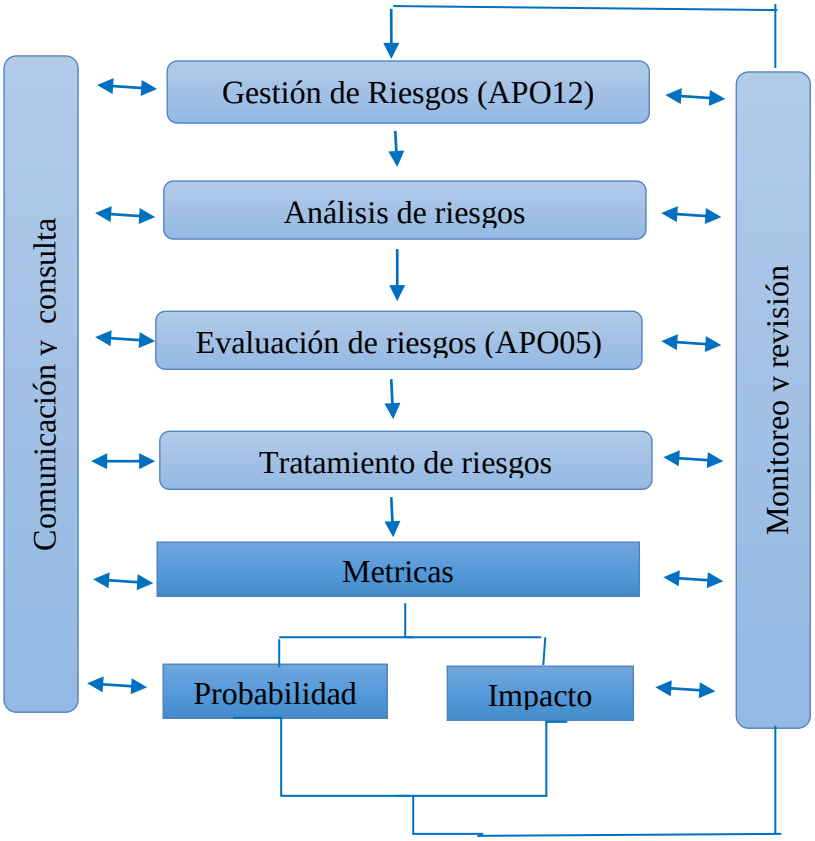
Tabla 7 Lista de riesgos de la información

Consolidations Services S.A. de C.V.			
Lista de riesgos de seguridad			
No	**Descripción**	**Impacto**	**Probabilidad**
1	Pérdida o robo de información	A	M
2	Hackeos o filtraciones	M	B
3	Fallas en la conexión de internet	M	B
4	Incendios, Inundaciones, fallas eléctricas	A	B
5	Daños en los servidores	A	M
6	Intrusión física a áreas restringidas	M	B
7	Fallas en los circuitos de video vigilancia	M	B
8	Fallas en el acceso remoto, redes, canales secundarios, redes privadas virtuales (VPNs)	A	B
9	Falta de recursos para inversión en seguridad	M	B
10	Fuga de información a través de correos electrónicos	M	M
11	Deficiencias en la divulgación del plan de seguridad	M	B

1.6 Parámetros de medición APO13

Para realizar una buena gestión de riesgos con procedimientos efectivos, Consolidations Seriveces S.A. de C.V. medirá el impacto y la probabilidad de ocurrencia de cada riesgo utilizando métricas que permitan obtener un resultado razonable del impacto ocasionado a la compañía al materializarse el riesgo, tomando como lineamiento el esquema de la siguiente figura.

Figura 9 Medición de impacto y probabilidad de los riesgos



La empresa deberá diseñar una matriz que permita al gerente de TI el registro y análisis de la eficacia de los procedimientos aplicados por la compañía, para la evaluación de los controles y respuesta al riesgo al ocurrir un evento.

Para efectos prácticos se desarrollarán tres matrices para evaluar un riesgo de cada componente de seguridad de la información, como lo son confidencialidad, integridad y disponibilidad, según se muestra en las siguientes figuras.

Figura 10 Matriz de evaluación de la gestión de acceso y control remoto

MATRIZ DE AVALUACIÓN DE RIESGOS								
Evaluación de: Confidencialidad-Consolidation Services S.A de C.V								
Ref COBIT	Componente	Riesgo	Procedimientos	EVALUACIÓN		MEDICIÓN %		
				EFICIENTE	DEFICIENTE	IMPACTO	PROBABILIDAD	%
DSS05-03	**Confidencialidad** Gestión de acceso y control remoto	Acceso a la aplicacion de monitoreo en linea, hardware e informacion sensible por personal no autorizado	Se aplican los protocolos de seguridad aprobados a las conexiones de red.	X		M	M	50%
			Se hacen pruebas periódicas de acceso a la aplicación de monitoreo en línea	X		B	M	25%
			Se implementan procedimientos sistemáticos para la generación de números a los documentos de transporte (BL, Guía aérea, Carta porte)	X		M	B	25%
			Se le verifica que solo puedan acceder al hardware, redes, software, aplicaciones y software de soporte solo las personas autorizadas	X		A	M	60%
							RESULTADO	40%
Hecho por: Walber Bonilla **Fecha** 18/08/2017					Aceptable	> 50%		
					Medio	50% > 65%		
					Alto	65% >		

Los procedimientos aplicados para controlar el acceso a los recursos de TI, información confidencial e instrucción vía remota se consideran eficientes, ya que minimizan la posibilidad de ocurrencia a un nivel aceptable, estos deben ser evaluados periódicamente a fin de asegurar que en cualquier momento se mantenga la información segura.

En la siguiente figura se evaluaran los procedimientos de control de dispositivos móviles en los que se almacena información confidencial

Figura 11 Matriz de evaluación de los controles para dispositivos móviles

MATRIZ DE AVALUACIÓN DE RIESGOS								
Evaluación de: Integridad-Consolidation Services S.A de C.V								
Ref COBIT	Componente	Riesgo	Procedimientos	EVALUACIÓN		MEDICIÓN %		
				EFICIENTE	DEFICIENTE	IMPACTO	PROBABILIDAD	%
DSS05-06	**Integridad** Control de dispositivos móviles	Pérdida de información almacenada en dispositivos moviles y que sea alterada por personas externas a la empresa	Se Implementan mecanismos de bloqueo en los dispositivos	X		M	M	50%
			Se establece protección física(ubicación) adecuada a los dispositivos		X	M	A	60%
			Se mantiene resguardo de información de todos los dispositivos.		X	M	A	60%
			Se realiza un inventario detallado de los activos, de la información y físicos, con su adecuada clasificación, propiedad, ubicación, tipo de mantenimiento, valor y criticidad	X		M	B	25%
							RESULTADO	49%

Hecho por: Jacqueline Zavala
Fecha 18/08/2017

Aceptable	> 50%
Medio	50% > 65%
Alto	65% >

Los procedimientos establecidos para la gestión de los equipos móviles se consideran eficientes, a pesar que al mantener los dispositivos en una ubicación segura no se aplican controles y se deberían mejorar, el resultado final se considera dentro de límite de riesgo aceptado por Consolidations Services S.A de C.V.

En la siguiente figura se evalúa el riesgo de pérdida de información por daños en los servidores, previniéndose a través de procedimientos como resguardo de seguridad, dichos respaldos deben mantenerse en lugares seguros, ya sea dentro o fuera de las

instalaciones de la empresa, además, es recomendable mantener encriptados los datos almacenados en discos duros, memorias USB, nube, u otro medio de almacenamiento.

Figura 12 Matriz de evaluación de respaldos de información

MATRIZ DE AVALUACIÓN DE RIESGOS								
Evaluación de: Disponibilidad-Consolidation Services S.A de C.V								
Ref COBIT	Componente	Riesgo	Procedimientos	EVALUACIÓN		MEDICIÓN %		
				EFICIENTE	DEFICIENTE	IMPACTO	PROBABILIDAD	%
DSS05-02	**Disponibilidad** Gestión de respaldo de información	Pérdida o extravío de de información o daños a los servidores o dispositivos de almacenamiento	Se hacen respaldos de información y se almacena fuera de las instalaciones de la empresa	X		M	M	50%
			Existe personal directamente responsible de realizar los backups diariamente	X		B	M	25%
			Se gestiona el uso de la nube para que la información este accesible en cualquier lugar o momento que se necesite.	X		M	B	25%
			Se asegura que los backups que sean extraíbles tengan un parámetro de seguridad confiable.	X		A	M	60%
							RESULTADO	40%

Hecho por:	Gabriela Reyes
Fecha	18/08/2017

Aceptable	> 50%
Medio	50% > 65%
Alto	65% >

Los procedimientos aplicados para mantener resguardo de información disponibles para las partes interesas se consideran eficientes, ya que se realizan respaldos de información permanentemente y se almacena en lugares seguros.

1.7 Mejora continua APO13.03

Se revisará el manual de seguridad cada dos años de forma integral, y parcial siempre que haya cambios significativos, que el gerente de TI considere oportuno la actualización de procedimientos que permitan gestionar los riesgos en seguridad de forma eficiente. Dichos cambios puede surgir por aumento de operaciones o prestación

de un nuevo servicio, plan de expansión, inversión en nuevas tecnologías, requerimientos legales o cambio en el gobierno de la entidad.

1.8 Definiciones

Para efectos del presente manual de gestión de riesgos en seguridad se consideran las siguientes definiciones:

Gerente de TI: Responsable de implementar y mantener la estrategia de seguridad de la información, diseñar procedimientos y evaluar su aplicación a fin de asegurar minimizar la probabilidad que los riesgos se materialicen.

Monitoreo en línea: Aplicación mediante la cual se verifica el estatus, ubicación fechas de salida, llegada y características de un envió, identidad cada carga mediante el número del documento de transporte, tales como: Bill of Lading (BL), Carta porte, Guía aérea.

Respaldo de información: Resguardo de información mediante la copia de seguridad (Backup) tanto para información en medios físicos como digitales, asegurando mantener la información siempre disponible.

Riesgo: Posibilidad que un hecho o amanezca se materialice, como incendios, fallas eléctricas, filtraciones, entre otros.

Recursos de TI: Se considera como recurso de TI las Personas, Infraestructura, Aplicaciones e Información,

Procedimiento de seguridad: Medidas implementadas por la compañía para disminuir la probabilidad de ocurrencia de un riesgo en seguridad, tales como la pérdida de información robo o extravió.

2 Procedimientos de seguridad APO11.02, APO12.05

Consolidations Services S.A. de C.V. implementará procedimientos en el nivel operativo, que aseguren que se realiza de forma eficaz la planificación, operación y control de los procesos de seguridad de la información, con la intención de gestionar eficientemente los riesgos y lograr mantener la confidencialidad, integridad y disponibilidad de la información.

2.2 Confidencialidad

Objetivo: Proteger la información contra la divulgación, modificación y revisión de personas no autorizadas.

2.1.1 Gestión de la seguridad para los usuarios finales DSS05.03

Objetivo: Asegurar que los usuarios finales puedan acceder a través de sus equipos de forma segura a información que previamente han sido autorizados, aplicando procedimientos de seguridad definidos para asegurar la información procesada, almacenada o transmitida.

2.1.1.1 Creación de usuarios DSS05.03

Para asegurar que la creación de usuarios se haga bajo un procedimiento organizado Consolidations Services S.A. de C.V. aplicará los procedimientos descritos en la siguiente tabla.

Tabla 8 Creación de usuarios

Área	**2.1 Confidencialidad**	**COBIT 5: DSS05-03**	
Descripción	**2.1.1 Gestión de la seguridad para los usuarios finales**	**Responsable**	
No	2.1.1.1 Creación de usuarios	**Autorizar**	**Hacer**
1	Crear archivos de identificación a cada usuario que incluya: * Nombre del usuario * Número de identificación * Área de trabajo * Contrato de confidencialidad	GG	GTI
2	Usuarios para clientes * Nombre de la empresa * Nombre del usuario * Número de identificación * Autorización del Representante Legal	GG	GTI
3	Asignar a cada una contraseña a cada usuario: * Mínimo de caracteres: 8 * Debe incluir números y letras * Modificar la contraseña cada 60 días * Bloquear contraseña después de 5 intentos *Solicitar reactivación al personal autorizado	GG	GTI
4	Asignar equipos específicos a cada usuario, con aceptación y firma de responsabilidades, según corresponda.	GG	GTI

2.1.1.2 Gestionar la integridad de la información DSS05.03

Objetivo: Proteger la información contra la modificación y destrucción inapropiada con procedimientos de seguridad que incluyan asegurar la autenticidad de la información.

Tabla 9 Gestionar la integridad de la información

Área	**2.1 Confidencialidad**	**COBIT 5: DSS05-03**	
Descripción	2.1.1 Gestión de la seguridad para los usuarios finales	**Responsable**	
No	2.1.1.2 Gestionar la integridad de la información	**Autorizar**	**Hacer**
1	Implementar mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, para evitar que se modifique, se borre y se robe información.	GG	GTI
2	Permitir el acceso a información y a la red de la empresa solo a los dispositivos autorizados. Configurar estos dispositivos para forzar la solicitud de contraseña	GG	GTI
3	Realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.	GG	GTI
4	Realizar pruebas de intrusión periódicas para determinar el nivel de protección de la red.	GG	GTI
5	Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas, documentadas y autorizadas.	GG	GTI
6	Revisar si se mantiene la autenticidad e integridad durante la transmisión e ingreso a Magaya	GG	GTI
7	Estandarizar procesos a fin de asegurar que la información que se muestrea los usuarios este completa.	GG	GTI
8	Asegurar que los usuarios reciben los resultados adecuados de una forma segura y oportuna.	GG	GTI
9	Verificar que todos los datos esperados para su procesamiento sean recibidos y procesados por completo y de una forma precisa y oportuna	GG	GTI
10	Autenticar la fuente de las transacciones y verificar que él o ella tienen la autoridad para originar las transacciones.	GG	GTI

11	Revisar si se crean transacciones por individuos autorizados siguiendo los procedimientos establecidos, incluyendo, cuando sea apropiado, la adecuada segregación de tareas en relación al origen y aprobación de esas transacciones.	GG	GTI

2.1.1.3 Gestionar el acceso y control remoto DSS05.03

Objetivo: Aplicar procedimientos de seguridad que permitan el acceso a la aplicación de monitoreo (Magaya LiveTrack) en línea en cualquier momento y asegurar que la información que se muestra es integra y oportuna.

Tabla 10 Gestionar el acceso y control remoto

Área	**2.1 Confidencialidad**	**COBIT 5: DSS05-03**	
Descripción	2.1.1 Gestión de la seguridad para los usuarios finales	**Responsable**	
No	2.1.1.3 Gestionar el acceso y control remoto	**Autorizar**	**Hacer**
1	Aplicar los protocolos de seguridad aprobados a las conexiones de red.	GG	GTI
2	Hacer pruebas periódicas de acceso a la aplicación de monitoreo en línea	GG	GTI
3	Determinar grupos de soporte basados en categorías predefinidas, tales como hardware, redes, software, aplicaciones y software de soporte.	GG	GTI
4	Asegurarse que los servicios de acceso remoto y perfiles de usuario (u otros medios utilizados para el mantenimiento o diagnóstico) están activos sólo cuando sea necesario	GG	GTI
5	Verificar si la ubicación y estatus que se brindan en Magaya LiveTrack es el real	GG	GTI
6	Informar a los usuarios cualquier cambio o actualización realizada a Magaya LiveTrack	GG	GTI
7	Implementar procedimiento sistemático para la generación de números a los documentos de transporte (BL, Guía aérea, Carta porte)	GG	GTI

8	Previo entregar de numero de BL, Guía aérea, Carta porte u otro documento de transporte a los usuarios a asegurarse que este procesado en Magaya LiveTrack	GG	GTI
9	Desarrollar mecanismos respuesta inmediata ante reporte de bloqueos o mala conexión.	GG	GTI
10	Instalar aplicativos anti intrusión de personal ajeno a la empresa, para evitar robo, modificación de estatus de las cargas.	GG	GTI
11	Implementar mecanismos de mejora continua que faciliten el monitoreo en línea a sus usuarios	GG	GTI

2.1.2 Gestión de usuarios y credenciales DSS05.04

2.1.2.1 Administración de usuarios DSS05.04

Objetivo: Establecer procedimientos que permitan un mejor uso y administración para los usuarios finales y el uso de credenciales y que estén debidamente documentados y poder establecer diferentes tipos de rango de seguridad para el uso de usuarios.

Tabla 11 Administración de usuarios

Área	**2.1 Confidencialidad**	**COBIT 5: DSS05-03**	
Descripción	2.1.2 Gestión de la seguridad para los usuarios finales	**Responsable**	
No	2.1.2.1 Administración de usuarios	**Autorizar**	**Hacer**
1	Crear un listado de todos los usuarios autorizados para el acceso a Magaya LiveTruck que incluya:	GG	GTI
	* Nombre del titular		
	* Nombre de la empresa		
	* Representante Legal de la empresa		
	* Numero y de contacto		
	* Cuentas de correos electrónicos autenticadas		
	* Nivel de acceso autorizado		
2	Documentar los procedimientos de cambio de contraseñas	GG	GTI

3	Documentar los procedimientos de cancelación o activación de usuarios	GG	GTI
4	Definir rangos de seguridad para cada usuario: C= consulta , M= modificación	GG	GTI
5	Establecer mecanismo de alerta a usuarios ante posibles infiltraciones	GG	GTI

2.1.2.2 Control de accesos DSS05.04

Objetivo: Establecer procedimientos para clasificación de información sensible para Consolidations Services S.A. de C.V. que permitan gestionar el acceso a dicha información.

Tabla 12 Control de accesos

Área	**2.1 Confidencialidad**	**COBIT 5: DSS05-03**	
Descripción	2.1.2 Gestión de la seguridad para los usuarios finales	**Responsable**	
No	2.1.2.2 Control de accesos	**Autorizar**	**Hacer**
1	Asignar contraseña a todos los dispositivos	GG	GTI
2	Nombrar áreas dentro de la empresa	GG	GTI
3	Prevenir el acceso no autorizado a dispositivos específicos	GG	GTI
4	Clasificar la información de acuerdo al grado de importancia como confidencial	GG	GTI
5	Evaluar las categorías, clasificación, nivel de seguridad de la información y sensibilidad para una entidad	GG	GTI

6	Establecer un conjunto de procedimientos para la anulación, retirada o terminación de los derechos o capacidades de seguridad de la información para Magaya LiveTruck	GG	GTI

2.1.2.3 Pistas de auditoría DSS05.04

Objetivo: Implementar procedimientos que aseguren identificar los cambios generados por cada usuarios así como la fecha y hora.

Tabla 13 Pistas de auditoría

Área	**2.1 Confidencialidad**	**COBIT 5: DSS05-03**	
Descripción	2.1.2 Gestión de la seguridad para los usuarios finales	**Responsable**	
No	2.1.2.3 Pistas de auditoría	**Autorizar**	**Hacer**
1	Asegurase que los reportes que se generen incluyan:	GG	GTI
	* Usuario		
	* Fecha de generación		
	* Hora de generación		
	* Nombre del sistema		
2	Verificar que el sistema registre por cada usuario:	GG	GTI
	* Hora de ingreso		
	* Modificaciones		
	* Archivos generados		
	* Archivos borrados		
	* Archivos extraídos		
3	Archivar bitácoras de registros de incidencias	GG	GTI

4	Mantener registro de soluciones a problemas resueltos	GG	GTI
5	Definir y documentar los requerimientos de información de respaldo para soportar los planes, incluyendo planes y documentos en papel así como ficheros de datos y considerar las necesidades de seguridad y almacenamiento en otra ubicación.	GG	GTI
6	Definir un periodo apropiado de conservación de la documentación del cambio, la documentación del sistema antes y después del cambio y la documentación del usuario	GG	GTI

2.1.3 Gestión de acceso físico a activos de TI DSS05.05

2.1.3.1 Registro y controles de acceso

Objetivo: Establecer procedimientos que permitan mantener los recursos de TI seguros ante daños y robo de información.

Tabla 14 Registro y controles de acceso

Área	**2.1 Confidencialidad**	**COBIT 5: DSS05-03**	
Descripción	2.1.3 Gestión de acceso físico a activos de TI	**Responsable**	
No	2.1.3.1 Registro y controles de acceso	**Autorizar**	**Hacer**
1	Mantener registros con fecha y hora de entrada y salida de todo el personal	GTI	GA
2	Mantener vigilancia sobre los servidores y demás recursos donde se almacene información	GTI	GA
3	Revisar los contratos de mantenimiento que impliquen el acceso de terceros a las instalaciones	GG	GTI
4	Establecer el tiempo mínimo necesario para recuperar un proceso de negocio y su soporte de TI, basándose en una duración aceptable de interrupción del negocio y la interrupción máxima tolerable.	GG	GTI

2.1.3.2 Políticas de acceso

Objetivo: Establecer políticas claras de acceso a las áreas donde se encuentra los recursos de TI, que minimicen el riesgo de daño involuntario, robo u alteración de información sensible para Consolidations Services S.A. de C.V.

Tabla 15 Políticas de acceso

Área	2.1 Confidencialidad	COBIT 5: DSS05-03	
Descripción	2.1.3 Gestión de acceso físico a activos de TI	Responsable	
No	2.1.3.2 Políticas de acceso	Autorizar	Hacer
1	Crear carne para visitantes	GG	GTI
2	Toda persona que ingrese debe portar documento de identificación en un lugar visible	GG	GTI
3	Revisar los objetos que ingresen y salen a áreas restringidas	GTI	GA
4	Restringir el acceso de memorias USB	GTI	GA
5	Controlar la salida de información a través de correos electrónicos	GTI	GA
6	Mantener todos los accesos con puertas bajo llave	GTI	GA
7	Proporcionar servicios de alerta y notificación ante amenazas de robo u extravió de información	GG	GTI
8	Asegurar que se limite o impida comer, beber y fumar en áreas sensibles y que se prohíba el almacenamiento de material de oficina y otros suministros que puedan representar un riesgo de incendio cerca de los servidores	GG	GTI/ GA

2.1.3.3 Medidas de seguridad preventivas

Objetivo: Establecer procedimiento de seguridad que permitan reducir la probabilidad de incidentes tales como, pérdida de información por catástrofes naturales

Tabla 16 Medidas de seguridad preventivas

Área	2.1 Confidencialidad	COBIT 5: DSS05-03	
Descripción	2.1.3 Gestión de acceso físico a activos de TI	Responsable	
No	2.1.2.1 Medidas de seguridad preventivas	Autorizar	Hacer
1	Proteger físicamente a la información con medidas tales como: * Circuito cerrado de televisión * Cerraduras * Alarmas * Control de acceso *Almacenamiento externo * Revisión de instalaciones eléctricas * Sistemas de protección contra incendios * Cerraduras con temporizador * Instalación de puertas solidas * Revisión de paredes y techo solido	GG	GTI
12	Revisar periódicamente que el hardware se encuentra en condición segura, para ello, verifique: temperatura adecuada, espacio físico, muebles adecuados, fallas de corrientes eléctricas, etc.	GG	GTI
13	Comprobar el uso de los equipos para el fin previsto	GG	GTI
14	Realizar periódicamente inventarios de todos los activos de TI	GG	GTI
15	Revisar el plan de mantenimiento preventivo para todo el hardware, considerando un análisis coste-beneficio, recomendaciones del proveedor, el riesgo de interrupción del servicio, personal cualificado y otros factores relevantes.	GG	GTI
16	Establecer políticas de compra y adquisición del hardware	GG	GTI
17	Verificar periódicamente que desastres naturales y accidentes provocados por el personal pueden ocurrir y poner en riesgo el área donde se encuentran las instalaciones de TI.	GG	GTI
18	Asegurar que los sitios e instalaciones de TI cumplen de manera sistemática con la legislación, regulaciones, directrices y especificaciones relevantes de seguridad ocupacional y seguridad en el trabajo.	GG	GTI

2.2 Integridad

Objetivo: Proteger la información de Consolidations Services, S.A. de C.V., contra la destrucción o modificación inadecuada, incluyendo asegurar el no repudio y autenticidad de la información.

2.2.1 Protección de software malicioso DSS05.01

Objetivos: Implementar medidas efectivas de detección y correctivas para proteger los sistemas de información y software de Consolidations Services, S.A. de C.V.

Tabla 17 Protección de Software maliciosos y herramientas de seguridad

Área	**2.2 Integridad**	**COBIT 5: DSS05.01**	
Descripción	**2.2.1 Protección de Software maliciosos**	**Responsable**	
No	**2.2.1.1Protección de Software maliciosos y herramientas de seguridad**	**Autorizar**	**Hacer**
1	Instalar herramientas de protección (antivirus) para software	GG	GTI
2	Mantener configuración centralizada en el software de protección	GG	GTI
3	Establecer herramientas de filtros para el uso de internet (páginas web)	GG	GTI
4	Establecer herramientas de filtros para descargas	GG	GTI
5	Instalar firewalls para bloqueo de accesos predeterminados	GG	GTI
6	Revisar regularmente la información sobre posibles amenazas	GG	GA
7	Implementar un conjunto de capacidades y prácticas de gestión para protección de los datos en todos los estados	GG	GTI
8	Desarrollar contramedidas utilizando la gestión de la nube	GG	GA
9	Establecer analizador de paquetes y sensores para la detección de software maliciosos	GG	GTI
10	Planificar, implementar, mantener y mejorar las medidas, contramedidas y actividades, incluyendo, pero no limitado a acciones, procesos, dispositivos o sistemas frente las amenazas y las vulnerabilidades identificadas en las evaluaciones de riesgos de la seguridad de la información. Estar al tanto de tecnologías emergentes	GG	GA

2.2.2.1 Actualización de antivirus DSS05.01

Objetivo: Establecer procedimientos que ayuden a la previsión de acceso control y mantenimiento de antivirus a la empresa Consolidations Services, .S.A. de C.V.

Tabla 18 Actualización de antivirus

Área	**2.2 Integridad**	**COBIT 5: DSS05.01**	
Descripción	**2.2.1Protección de Software maliciosos**	**Responsable**	
No	**2.2.2 Actualización de antivirus**	**Autorizar**	**Hacer**
1	Realizar chequeos de actualización de antivirus	GG	GTI
2	Verificar que los antivirus sean seguros y con licencias originales	GG	GTI
3	Realizar listados de licencias adquiridas para detallar fecha de compra y caducidad	GG	GTI
4	Verificaciones de software para determinar fecha de actualización	GG	GTI
5	Mantener un registro de todas las licencias activas	GG	GTI
6	Asegurase que el número de licencias adquiridas son las necesarias	GG	GTI
7	Verificar que los usuarios den el uso adecuado a los antivirus	GG	GTI
8	Desarrollar lineamientos para la verificación de actualización de antivirus	GG	GTI
9	Establecer medidas de seguridad que determinen que los antivirus están funcionando correctamente	GG	GTI
10	Establecer actualizaciones proporcionadas por el proveedor	GG	GTI

2.2.2.2 Capacitación al personal sobre el uso de correo e internet DSS05.01

Objetivo: Desarrollar planes de capacitación para el uso adecuado del correo electrónico e internet dentro de la empresa Consolidations Services, S.A. de C.V. para la seguridad de la información

Tabla 19 Capacitación al personal sobre el uso de correo e internet

Área	**2.2 Integridad**	**COBIT 5: DSS05.01**	
Descripción	**2.2.2 Protección de Software maliciosos**	**Responsable**	
No	**2.2.2.2 Capacitación al personal sobre el uso de correo e internet**	**Autorizar**	**Hacer**
1	Capacitar al personal dentro de la empresa para el uso de internet estableciendo políticas de seguridad	GG	GTI
2	Realizar capacitaciones al personal para el uso adecuado de software una vez al mes	GG	GTI
3	Capacitar al personal para no instalar software compartidos o no autorizados	GG	GTI
4	Identificar a los usuarios de manera única	GG	GTI
5	Permitir solo al personal autorizado a tener acceso a la información y a la red de la empresa	GG	GTI
6	Proporcionar bases de conocimiento y herramientas de formación para el uso de correo electrónicos	GG	GTI
7	Comunicar los puntos débiles de la seguridad de la información, los comportamientos deseables y los cambios necesarios para hacer frente a estas debilidades.	GG	GTI
8	Proporcionar cursos de formación sobre seguridad	GG	GTI
9	Proporcionar cursos de formación sobre medios sociales de comunicación	GG	GTI
10	Desarrollar y comunicar una visión común al equipo de seguridad de la información que esté en línea con la declaración de visión corporativa	GG	GTI

2.2.2.3 Encriptación de datos

Objetivo: implementar procesos que permitan que la información esté debidamente resguardada y el uso restringido para el personal autorizado.

Tabla 20 Encriptación de datos

Área	**2.2 Integridad**	**COBIT 5: DSS05.01**	
Descripción	**2.2.2 Protección de Software maliciosos**	**Responsable**	
No	**2.2.2.3 Encriptación de datos**	**Autorizar**	**Hacer**
1	Instalar software de encriptación automática	GG	GTI
2	Clasificar la información encriptada por áreas	GG	GTI
4	Verificar el uso adecuado de los software de encriptación	GG	GTI
5	Cifrar la información almacenada de acuerdo a su clasificación	GG	GTI
6	Cifrar la información en tránsito de acuerdo con su clasificación.	GG	GTI

2.2.3 Gestión de salida de información sensible

Objetivo: Utilizar medidas de seguridad y procedimientos de gestión para proteger la información en todos los modos de conexión

Tabla 21 Gestión de la información

Área	**2.2 Integridad**	**COBIT 5: DSS05.06**	
Descripción	**2.2.3 Gestión de salida de información Sensible**	**Responsable**	
No	**2.2.3.1 Gestión de la información**	**Autorizar**	**Hacer**
1	Cada aplicación o software debe contar con contraseña de seguridad	GG	GTI
2	Configurar los sistemas operativos de forma segura	GG	GTI
3	Asignar a una persona encargada para la validación y salida de información	GG	GTI

4	Asignar privilegios de acceso a documentos e información sensible	GG	GTI
5	Proteger los dispositivos y la salida de información	GG	GTI
6	Proporcionar medidas y actividades para la seguridad de la información específicas de dispositivo.	GG	GTI
7	Proporcionar sistemas adecuados para el protocolo de transferencia de archivos	GG	GTI

2.2.3.2 Control de dispositivos móviles

Objetivo: establecer controles para el uso adecuado de dispositivos móviles.

Tabla 22 Control de dispositivos móviles

Área	**2.2 Integridad**	**COBIT 5: DSS05.06**	
Descripción	**2.2.3 Gestión de salida de información Sensible**	**Responsable**	
No	**2.2.3.2 Control de dispositivos móviles**	**Autorizar**	**Hacer**
1	Implementar mecanismos de bloqueo en los dispositivos	GG	GTI
2	Establecer protección física(ubicación) adecuada a los dispositivos	GG	GTI
3	Establecer un inventario de documentos sensibles y de dispositivos	GG	GTI
4	Establecer procedimientos para el uso adecuado de dispositivos móviles	GG	GTI
5	Establecer salvaguardas físicas apropiadas sobres dispositivos móviles	GG	GTI
6	Mantener resguardo de información de todos los dispositivos.	GG	GTI
7	Proporcionar un inventario detallado de los activos, de la información y físicos, con su adecuada clasificación, propiedad, ubicación, tipo de mantenimiento, valor y criticidad	GG	GTI

Fuente: Elaboración propia

2.2.3.3 Control de correos electrónicos

Objetivo: desarrollar procesos que brinden procedimientos para el uso adecuado del correo electrónico dentro de la empresa Consolidations Services, S.A. de C.V.

Tabla 23 Control de correos electrónicos

Área	**2.2 Integridad**	**COBIT 5: DSS05.06**	
Descripción	**2.2.3 Gestión de salida de información Sensible**	**Responsable**	
No	**2.2.3.3 Control de correos electrónicos**	**Autorizar**	**Hacer**
1	Establecer accesos adecuados para el uso de correo electrónico	GG	GTI
2	Proporcionar cursos de formación sobre la importancia del correo electrónico	GG	GTI
3	Establecer servicios de autenticación de contraseña para el uso de correos electrónicos	GG	GTI
5	Realizar Backus de correo electrónico para resguardar información importantes	GG	GTI
6	Verificar que el uso de la red sea adecuado para obtener información y uso del correo de manera eficiente y adecuada	GG	GTI
7	Gestionar que el uso de correo electrónico sea solo con fines laborales	GG	GTI

2.2.3.4 Procedimientos de destrucción de información

Objetivo: Implementar procesos adecuados dentro de Consolidations Services, S.A. de C.V. que determinen la destrucción adecuada de información para evitar que esta sea utilizada inadecuadamente.

Tabla 24 Destrucción de la información

Área	2.2 Integridad	COBIT 5: DSS05.06	
Descripción	2.2.3 Gestión de salida de información Sensible	Responsable	
No	2.2.3.4 Destrucción de la información	Autorizar	Hacer
1	Establecer procedimientos para el uso, resguardo o eliminación y destrucción de formularios especiales y dispositivos de salida, dentro y fuera de la empresa.	GG	GA
2	Destruir la información de salida sensible que pueda perjudicar a la empresa	GG	GA
3	Destruir de manera oportuna la información sensible	GG	GA

2.3 Disponibilidad

Objetivo: Asegurar el acceso y uso a tiempo y fiable de la información.

2.3.1 Gestión de proveedores de servicios de TI APO10

Objetivo: Implementar métodos que le permitan a la empresa Consolidations Services, S.A. de C.V. tener un control de todos los servicios de TI adquiridos desde la selección de sus proveedores, la gestión de los contratos, revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuado.

2.3.1.1 Conocimiento y selección del proveedor APO10.02

Objetivo: Antes de seleccionar a los proveedores realizar una lista de chequeo de los requisitos con los que debe contar dicho proveedor, y estos deben estar optimizados con las aportaciones de nuevos proveedores potenciales.

Tabla 25 Conocimiento y selección del proveedor

Área	**2.3 Disponibilidad**	**COBIT 5: APO10.02**	
Descripción	2.3.1 Gestión de proveedores de servicios de TI	**Responsable**	
No	2.3.1.1 Conocimiento y selección del proveedor	**Autorizar**	**Hacer**
1	Solicitar al proveedor un listado de sus clientes para evaluar su competitividad en el medio. *Seleccionar una muestra de clientes. *Realizar llamas telefónicas o envió de correos electrónicos. *Solicitar información acerca del proveedor. *Partir de esas respuestas para la contratación de proveedores.	GG	GTI
2	Investigar que tan frecuente suceden incidentes por falta de control de seguridad.	GG	GTI
3	Actualizar nuestra lista de requisitos cada determinado tiempo para obtener un perfil del proveedor adecuado. *Verificar nuevas actualizaciones de proveedores que estén a la vanguardia de la tecnología. *Añadirlas a nuestra lista de requisitos.	GG	GTI

2.3.1.2 Gestión de contratos APO10.03

Objetivo: Verificar que cada contrato con nuestros proveedores cumpla con los requerimientos estipulados por la empresa Consolidations Services, S.A. de C.V. y realizar un análisis para confirmar que el proveedor está cumpliendo con su parte estipulada y con los tiempos de entrega.

Tabla 26 Gestión de contratos

Área	2.3 Disponibilidad	COBIT 5: APO10.03	
Descripción	2.3.1 Gestión de proveedores de servicios de TI	Responsable	
No	2.3.1.2 Gestión de contratos	Autorizar	Hacer
1	Conocer los derechos y obligaciones que posee el contrato.	GG	GTI
2	Asegurarse que el contrato contiene todos los requisitos de la gestión. *Antes de firmar un contrato tener claro el objetivo de la empresa *Verificar que el objetivo este alineado con el contrato del proveedor	GG	GTI
3	Seguimiento de los plazos de entrega y ejecución de tareas. *Consultar con sus clientes el nivel de responsabilidad del proveedor.	GG	GTI
4	Tener un recordatorio en el correo de la fecha en que estos contratos se vencen.	GG	GTI

2.3.1.3 Gestión de riesgos en suministro APO10.04

Objetivo: Identificar los riesgos para medir la capacidad con la que los proveedores proporcionan de manera continua una actualización de información segura, eficaz y eficiente.

Tabla 27 Gestión de riesgos en suministro

Área	2.3 Disponibilidad	COBIT 5: APO10.04	
Descripción	2.3.1 Gestión de proveedores de servicios de TI	Responsable	
No	2.3.1.3 Gestión de riesgos en suministro	Autorizar	Hacer
1	Revisiones previas de los proveedores, utilización de almacenes y transportes seguros	GG	GTI
2	Mejorar las pruebas de detección de vulnerabilidades.	GG	GTI
3	Verificar si el proveedor de internet brinda un ancho de banda para que la aplicación de Magaya Live Track funcione eficientemente.	GG	GTI

4	Asegurarnos que el proveedor tiene la capacidad de soporte en la aplicación de monitoreo en línea para responder de manera oportuna a cada cliente que visite el sitio al mismo tiempo.	GG	GTI
5	La capacidad de respuesta que tiene el proveedor.	GG	GTI

2.3.2 Gestión de continuidad a los servicios DSS04

Objetivo: Implementar un plan que le permita a la empresa Consolidations Services, S.A. de C.V. y a TI responder al momento de que ocurran incidentes e interrupciones en la operación continúa de los procesos críticos para mantener la disponibilidad de la información a un nivel aceptable.

2.3.2.1 Desarrollar un plan de continuidad de negocio DSS04.01

Objetivo: Definir una política de continuidad para empresa Consolidations Services, S.A. de C.V. alineada con los objetivos de ella y de las partes interesadas.

Tabla 28 Desarrollar un plan de continuidad de negocio

Área	**2.3 Disponibilidad**	**COBIT 5: DSS04.01**	
Descripción	2.3.2 Gestión de continuidad a los servicios	**Responsable**	
No	2.3.2.1 Desarrollar un plan de continuidad de negocio	**Autorizar**	**Hacer**
1	Definir el objetivo que queremos lograr y que este de la mano con las políticas de la empresa	GG	GTI

2.3.2.2 Procedimientos de capacitación a usuarios DSS04.06

Objetivo: Implementar capacitaciones con el fin de mantener informados a las partes implicadas de los procedimientos, roles y responsabilidades en caso de disrupción.

Tabla 29 Procedimientos de capacitación a usuarios

Área	**2.3 Disponibilidad**	**COBIT 5: DSS04.06**	
Descripción	2.3.2 Gestión de continuidad a los servicios	**Responsable**	
No	2.3.2.2 Procedimientos de capacitación a usuarios	**Autorizar**	**Hacer**
1	Planificar sesiones que ayuden a intercambiar ideas para crear una lista de amenazas que puedan existir y su impacto negativo.	GG	GTI
2	Al momento de establecer un cambio en un proceso hacerlo saber a las partes correspondientes de la empresa.	GG	GTI
3	Capacitar a los empleados y usuario acerca de las actualizaciones.	GG	GTI

2.3.2.3 Gestión de respaldo de información DSS04.07

Objetivo: Mantener un respaldo de toda la información manejada en Magaya LiveTrack y que esta cumpla con todos los requerimientos de seguridad de la información.

Tabla 30 Gestión de respaldo de información

Área	**2.3 Disponibilidad**	**COBIT 5: DSS04.07**	
Descripción	2.3.2 Gestión de continuidad a los servicios	**Responsable**	
No	2.3.2.3 Gestión de respaldo de información	**Autorizar**	**Hacer**
1	Hacer un backup interno que pueda ser resguardado en un lugar específico de la empresa e incluso que este fuera de las instalaciones por cualquier incidente que ocurra.	GG	GTI

2	Gestionar el uso de la nube para que la información este accesible en cualquier lugar donde se necesite.	GG	GTI
3	Asegurarnos que los Backus que sean extraíbles tengan un parámetro de seguridad confiable.	GG	GTI

2.3.3 Gestión de la seguridad en la red y conexión DSS05.02

Objetivo: Implementar controles respecto a la seguridad para proteger la información en todos los modos de conexión.

2.3.3.1 Políticas de seguridad DSS05.02

Objetivo: Establecer políticas para la conexión de la red.

Tabla 31 Políticas de seguridad

Área	**2.3 Disponibilidad**	**COBIT 5: DSS05.02**	
Descripción	2.3.3 Gestión de la seguridad en la red y conexión	**Responsable**	
No	2.3.3.1 Políticas de seguridad	**Autorizar**	**Hacer**
1	Asegurar que las aplicaciones funcionen eficientemente aun con el ingreso de varios usuarios conectados al mismo tiempo a la aplicación de Magaya Live Track.	GG	GTI
2	Verificar que la instalación eléctrica sea adecuada al voltaje que los equipos necesitan.	GG	GTI

2.3.3.2 Transmisión de datos en la red DSS05.02

Objetivo: Definir métodos de confianza al momento de transmitir datos y que estos sean recibidos.

Tabla 32 Transmisión de datos en la red

Área	2.3 Disponibilidad	COBIT 5: DSS05-02	
Descripción	2.3.3 Gestión de la seguridad en la red y conexión	Responsable	
No	2.3.3.2 Transmisión de datos en la red	Autorizar	Hacer
1	Mantener un control de acceso a los usuarios, que estos solamente tenga acceso a la información que requieran y no a toda en sí.	GG	GTI
2	El acceso a carpetas específicas que contengan información de nuestros clientes o proveedores esté limitados a un cierto número de empleados que estén definidos para ellos.	GG	GTI

2.3.3.3 Configuración de equipos en red DSS05.02

Objetivo: Verificar la protección de la red y nuestro software Magaya LiveTrack.

Tabla 33 Configuración de equipos en red

Área	2.3 Disponibilidad	COBIT 5: DSS05-02	
Descripción	2.3.3 Gestión de la seguridad en la red y conexión	Responsable	
No	2.3.3.3 Configuración de equipos en red	Autorizar	Hacer
1	Existan procedimientos específicos para actividad.	GG	GTI
2	Definir una persona especifica que esté a cargo de verificar que todo se esté llevando a cabo bajo los procedimientos establecidos.	GG	GTI

3 Lista de verificación

Para evaluar si se aplican procedimientos que permitan asegurar y mantener la información segura y reducir la probabilidad que se materialicen los riesgos a un nivel aceptable se elaboró una lista de verificación para cada componente.

3.1 Lista de verificación para asegurar la confidencialidad de la información

La siguiente tabla muestra la lista de verificación de procedimientos para asegurar la confidencialidad de la información.

Tabla 34 Lista de verificación para asegurar la confidencialidad de la información

Consolidations Services S.A. de C.V.				
Lista de verificación para asegurar la confidencialidad de la información				
No	Descripción	Si	No	Comentario
Gestión de usuarios				
1	Se han creado archivos de identificación a cada usuario que incluya			
2	* Nombre del usuario	SI		
3	* Número de identificación	SI		
4	* Área de trabajo	SI		
5	* Contrato de confidencialidad	SI		
6	Las contraseñas asignadas incluyen:			
7	* Mínimo de caracteres: 8	SI		
8	* Números y letras	SI		
9	* Modificar la contraseña cada 60 días		NO	
10	* Bloquear contraseña después de 5 intentos	SI		
11	* Solicitar reactivación al personal autorizado	SI		
12	Se han asignado equipos específicos a cada usuario	SI		
13	Se posee un documento con firma de recibido que detalle las condiciones del equipo			
Controles de accesos				
14	Se permite el acceso a información y a la red de la empresa solo a los dispositivos autorizados	SI		
15	Se han implementado mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones	SI		
16	Se hacen pruebas periódicas de acceso a la aplicación de monitorio en línea	SI		
17	Se han determinado grupos de soporte basados en categorías predefinidas, tales como hardware, redes, software, aplicaciones y software de soporte.	SI		
18	se implementan procedimientos sistemáticos para la generación de números a los documentos de transporte (BL, Guía aérea, Carta porte)	SI		

19	Se verifica antes de entregar el número de BL, Guía aérea, Carta porte u otro documento de transporte a los usuarios a asegurarse que este procesado en Magaya LiveTrack	SI		
Pistas de auditoria				
20	Se documentan los procedimientos de cambio de contraseñas	SI		
21	se ha creado un listado de usuarios autorizados para el acceso a Magaya LiveTruck que incluya:			
22	* Nombre del titular	SI		
23	* Nombre de la empresa	SI		
24	* Representante Legal de la empresa	SI		
25	* Numero y de contacto	SI		
26	* Cuentas de correos electrónicos autenticadas	SI		
27	* Nivel de acceso autorizado	SI		
28	Se archivan las bitácoras de registros de incidencias		No	
29	El sistema registra por cada usuario:			
30	* Hora de ingreso	SI		
31	* Modificaciones	SI		
32	* Archivos generados	SI		
33	* Archivos borrados	SI		
34	* Archivos extraídos	SI		
35	Los reportes que se generen incluyen:			
36	* Usuario	SI		
37	* Fecha de generación	SI		
38	* Hora de generación	SI		
39	* Nombre del sistema	SI		
Control de acceso físico				
40	Se mantienen registros con fecha y hora de entrada y salida de todo el personal	SI		
41	Se mantiene vigilancia sobre los servidores y demás recursos donde se almacene información	SI		
42	Se han creado carné para visitantes	SI		
43	Se revisan los objetos que ingresan salen de áreas restringidas	SI		
44	Se restringe el acceso de memorias USB	SI		
45	Las personas que ingresan portan documento de identificación en un lugar visible	SI		
46	Se limita o impide comer, beber y fumar en áreas sensibles y que se prohíba el almacenamiento de material de oficina y otros suministros que puedan representar un riesgo de incendio cerca de los servidores		No	
47	Se mantienen todos los accesos con puertas bajo llave	SI		
48	Se controla la salida de información a través de correos electrónicos	SI		

49	Se protege el acceso físicamente a la información con medidas tales como:	SI		
50	* Circuito cerrado de televisión		NO	
51	* Cerraduras	SI		
52	* Alarmas	SI		
53	* Control de acceso	SI		
54	*Almacenamiento externo	SI		
55	* Revisión de instalaciones eléctricas	SI		
56	* Sistemas de protección contra incendios	SI		
57	* Cerraduras con temporizador	SI		
58	* Instalación de puertas solidas	SI		
59	* Revisión de paredes y techo solido	SI		

3.2 Lista de verificación para asegurar la integridad de la información

En la siguiente tabla se muestran procedimientos a evaluar para verificar si la empresa aplica control destinados a garantizar la integridad de la información.

Tabla 35 Lista de verificación para asegurar la integridad de la información

Consolidations Services, S.A. de C.V.				
Lista de verificación para asegurar la integridad de la información				
No.	Descripción:	Si	No	Comentario
	Protección de Software maliciosos			
1	¿Se cuenta con herramientas de protección, como antivirus?	Si		
2	¿Se configuran el software de antivirus adecuadamente?	Si		
3	¿Existen herramientas que filtren páginas adecuadas a la hora de utilizar internet?		No	
4	¿Hay procedimientos o filtros que brinden seguridad cuando se realizan descargas en línea?	Si		
5	¿La empresa cuenta con firewalls que determinen o restringa el uso de internet?		No	
6	¿En la empresa se revisa la información adecuada para detectar posibles amenazas que pongan en riesgo la información interna?	Si		

7	¿Se implementan medidas para enfrentar posibles amenazas?	Si		
	Actualización de antivirus			
8	¿Se cuenta con listado de licencia de antivirus?	Si		
9	¿Se lleva control de vigencia de antivirus?	Si		
10	¿La empresa posee medidas de seguridad que determine que los antivirus funcionan adecuadamente?	Si		
	Capacitación al Personal			
11	¿Se capacita al personal de la empresa para el uso adecuado de internet y redes?	Si		
12	¿Se capacita al personal para que pueda utilizar adecuadamente el software?	Si		
13	¿El personal está debidamente identificado con usuarios únicos?	Si		
14	¿El personal conoce los puntos débiles que hay de seguridad para hacer frente a estas debilidades?		No	
	Encriptación de Datos			
15	¿La empresa cuenta con software de encriptación?	Si		
16	¿En la empresa se cuenta con personal encargado para realizar encriptaciones?	Si		
	Gestión de salida de información			
17	¿Todo acceso a información sensible cuenta con usuarios asignados y contraseña?	Si		
18	¿Todos los dispositivos están configurados de manera segura?	Si		
19	¿La empresa cuenta con un inventario de dispositivos?	Si		
20	¿Se brindan capacitaciones para el uso adecuado de dispositivos?	Si		
21	¿Se resguarda la información de manera segura en todos los dispositivos?	Si		
22	¿El personal de la empresa sabe el uso adecuado que se le debe dar al correo electrónico?	Si		
23	¿Se realizan Backus de correo electrónico e información?	Si		

24	¿Se gestiona el uso adecuado de correo electrónico?	Si		
25	¿La empresa cuenta con accesos adecuados para el uso de correo electrónico?	Si		
26	¿La empresa cuenta con procedimientos adecuados para la eliminación, destrucción de información sensible?	Si		
27	¿Se destruye la información de salida que pueda perjudicar o dañar la reputación de la empresa?	Si		
28	¿Se destruye de manera oportuna la información?	Si		

3.4 Lista de verificación para asegurar la disponibilidad de la información

Para poder mantener la información disponible es necesario aplicar procedimientos, los cuales se evalúan en la siguiente tabla.

Tabla 36 Lista de verificación para asegurar la disponibilidad de la información

Consolidations Services, S.A. de C.V.				
Lista de verificación para asegurar la disponibilidad de la información				
No.	Descripción:	Si	No	Comentario
1	Se solicitó al proveedor un listado de sus clientes	Si		
2	Se investigó el número de incidentes que suceden por falta de seguridad	Si		
3	Se ha actualizado la lista con los requerimientos de Consolidations Services, S.A. de C.V. para obtener un perfil adecuado del proveedor	Si		
4	Se dio una revisión minuciosa del contrato	Si		
5	Se verifico que el proveedor cumple con los plazos de entrega y ejecución de tareas	Si		
6	Tiene en su correo actualizados los recordatorios de las fechas en que vencen los contratos	Si		
7	Se realizaron revisiones previas de los proveedores, utilización de almacenes y transportes seguros	Si		
8	Se verifico que el proveedor de internet brinda el ancho de	Si		

	banda adecuado para que la aplicación de Magaya Live Track funcione eficientemente			
9	Se verifico que el proveedor tiene la capacidad de soporte en la aplicación de monitoreo en línea para responder de manera oportuna a cada cliente que visite el sitio al mismo tiempo	Si		
10	Se determinó la capacidad de respuesta que tiene el proveedor?	Si		
11	Se definió el objetivo de lo que quiere lograr Consolidations Services, S.A. de C.V.	Si		
12	Se planificaron sesiones con los empleados		No	
13	Se informó a los empleados y usuarios al momento de implementar un nuevo procedimiento o sistema	Si		
14	Se está realizando un backup para el resguardo de la información	Si		
15	Se está haciendo uso de la nube como backup?	Si		
16	Poseen parámetros de seguridad los backups extraíbles	Si		
17	La aplicación funciona correctamente aun con el uso de muchos usuarios a la vez	Si		
18	La instalación eléctrica es apta para el equipo que se utiliza	Si		
19	Los controles a la transmisión de datos son los correctos	Si		
20	Existen procedimientos específicos para cada actividad a realizar en Consolidations Services, S.A. de C.V.	Si		
21	Hay una persona encarga de verificar que todos los procesos establecidos se estén llevando a cabo	Si		

CONCLUSIONES

- El modelo propuesto facilitará a las empresas de transporte marítimo y aéreo, que brindan el servicio de monitoreo en línea, en los procesos de gestión de los recursos de TI, mantener la información segura.

- COBIT 5 Para la Seguridad de la Información es un marco de referencia integral que permite adaptarse a cualquier tipo de empresa que cuente con recursos de TI, posibilitando así gestionarlos de manera eficiente, y las empresas de transporte marítimo y aéreo, no son la excepción.

- El personal responsable de la gestión de la seguridad de la información debe aplicar procedimientos que le permitan asegurar que la información se mantiene confidencial, es decir que solo puede acceder al personal debidamente autorizado así como integra y disponible.

- Con el aumento del comercio electrónico, las importaciones de materia prima o bienes de consumo, el sector de transporte marítimo y aéreo ha incrementado sus operaciones y para poder brindar información oportuna a sus clientes debe estar a la vanguardia con herramientas tecnológicas que le permitan brindar un buen servicio, por lo anterior las empresas deben implementar modelos para asegurar la información.

RECOMENDACIONES

- Se recomienda que las empresas inviertan recursos en la gestión de riesgos en seguridad de la información ya que esto le permitirá mantener su información de forma íntegra, disponible y manteniendo un grado aceptable de confidencialidad.

- Deben identificar las vulnerabilidades y amenazas a las que están expuestas, ya que esto permitirá invertir sus recursos en áreas donde el impacto de ocurrir un evento o materializarse un riesgo seria mayor, permitiendo así la optimización de recursos, considerando que son limitados.

- La información es un recurso muy importante para todas las empresas, como todo recurso este se debe proteger y asegurar, por lo que se recomienda a las empresas aplicar procedimientos preventivos, correctivos y detectivos, que minimicen los riesgos a un nivel aceptable para la compañía.

- Muchas de las empresas del sector transporte no cuenta con el personal capacitado para la gestión eficiente de los recursos de TI, por lo que las empresas deben capacitar periódicamente en temas como: seguridad de la información, ética y confidencialidad y marcos de referencia tales como cobit 5, Normas ISO, ITIL.

BIBLIOGRAFÍA

COBIT 5 Para la seguridad de la información, ISACA 2012.

Gestión logística integral, Ing. Luis Aníbal Mora

https://www.isaca.org/Journal/archives/2011/Volume-6/Pages/Data-Integrity-Information-Securitys-Poor-Relation-spanish.aspx)

Logística del transporte y distribución de carga, Luis Aníbal Moral, Eco Ediciones pág. 74

Manual de la gestión de logística del transporte y distribución de mercancías, Andrés, Castellanos Ramírez

ANEXOS

ÍNDICE DE ANEXOS

ANEXO 1

Universo de la muestra

Universo de la investigación, empresas de transporte marítimo y aéreo autorizado por la Dirección General de Aduanas a marzo de 2017.

LEY DE SIMPLIFICACIÓN ADUANERA
Artículo 8 letra "B"

La Dirección General deberá publicar por los medios que estime convenientes la lista de los auxiliares de la función pública aduanera autorizados, suspendidos o inhabilitados, así como las direcciones, teléfonos, correos electrónicos u otros datos del lugar en el que ejerzan sus negocios, a efecto de permitirles a los usuarios contactarlos. Asimismo, la Autoridad Aduanera podrá informar por cualquier medio, el listado de los auxiliares de la función pública aduanera, calificados de acuerdo al historial de operaciones en las que hubieran participado y el nivel de riesgo que posean en el sistema.

No.	Código	Empresa	Dirección	Teléfono	Correo electrónico	Estado	Nivel de Riesgo
1	TC244	CARGA URGENTE DE EL SALVADOR, S.A. DE C.V.	CALLE DEL MIRADOR #4420, COL. ESCALON	2246-7777	-	ACTIVO	BAJO
2	TC246	GIGANTE EXPRESS, S.A. DE C.V.	11A C. PTE, # 3971, COL. ESCALON	2200-8200/ 2298-7400	jose.ortiz@mallex.com.sv	ACTIVO	BAJO
3	TC250	TRANS EXPRESS DE EL SALVADOR, S.A. DE C.V.	CALLE Y COL. LA MASCOTA, No. 521-A, SAN SALVADOR	2209-1511/ Fax 2209-1530	-	ACTIVO	BAJO
4	TC252	SISTEMAS AEREOS DE EL SALVADOR, S.A. DE C.V.	AV. BERNAL Y C.CAMAGUEY # 507, COL. YUMURI, S.	2261-0401	-	INHABILITADO	BAJO
5	TC254	SPEEDWAY CONSOLIDADORES, S.A. DE C.V.	7 AV NORTE Y 25 CL PTE No. 17, URB. SON RUA, SAN SALVADOR	2102-6902	speewaysal@integra.com.sv	SUSPENDIDO	BAJO
6	TC258	COURIER INTERNACIONAL S.A. DE C.V.	PASEO GRAL ESCALON, No. 4910, COL. ESCALON	2241-8899/ 2241-8880	-	ACTIVO	BAJO
7	TC264	SERVICIOS EXPRESS, S.A. DE C.V.	BLVD Y COL. LA SULTANA FINAL PJE.MONELCA No1, ANTIGUO CUSCATLAN	2243-7244/ 2243-7277	jccervantes@tesal.com.sv	ACTIVO	BAJO
8	TC266	CARGA LATINOAMERICANA, S.A. DE C.V.	5ª CALLE PTE 7ª AV NTE PLAZA SAN ANGEL, AV. BERNAL CALLE SIGIMILES No.592 LCAL No.208 S. S	2271-2757	-	INHABILITADO	BAJO
9	TC267	ASIMEX, S.A DE C.V	CENTRO COMERCIAL FERIA ROSA 2a. PLANTA EDIF. B LOCAL 207 B, CA.STA TECLA	2212-6100/ 2243-3577	asimex@asimex.com.sv	ACTIVO	BAJO
10	TC268	CONSTRUMARKET, S.A. DE C.V.	AV. ALBERT EINSTEIN N° 17 COL. LOMAS DE SAN FRANCISCO, SAN SALVADOR	2500-0000	-	ACTIVO	BAJO
11	TC273	AGENCIA DE SERVICIOS, S.A. DE C.V.,	79 AV. SUR Y C.CUSCATLAN,EDIF.PZA.CRISTAL, COL ESCALON, LOCAL 2-11	2206-5555	asersa@maritimo.com	INHABILITADO	BAJO
12	TC274	CARGO EXPRESO, S.A DE C.V.	BLVD BAYER, COMPLEJO INDUS. MERLIOT LA LIBERTAD	2210-8800	edwin.escobar@cargoexpreso.com	INHABILITADO	BAJO
13	TC275	GRUPO AMERICA, S.A. DE C.V.	11 C.PTE. N° 3971, COL. ESCALON, SAN SALVADOR	2264-2121	julio.martinez@mallex.com.sv	INHABILITADO	BAJO
14	TC276	QUALITY EXPRESS, S.A. DE C.V.	BLVD.DEL HIPODROMO, PJE 1, CASA 415, COL. SAN BEBITO, S.S.	2241-8787	-	ACTIVO	BAJO
15	TC277	HERMES, S.A. DEC.V.	CENTRO LOGISTICO, BOULEVARD ACERO #12-A, ZONA INDUSTRIAL MERLIOT, ANT. CUSCATLÁN, LA LIBERTAD	2250-9300/ 2250-9349/ Fax 2250-9333	mimistinez@comca.com.sv	ACTIVO	BAJO
16	TC279	COMPAÑÍA PANAMEÑA DE AVIACION, S.A.	EDIF WORLD TRADE CENTER, NIVEL 1, LOAL 107, SAN SALVADOR	2209-2622/ 2505-5555	-	ACTIVO	BAJO
17	TC280	CARGO INTERNATIONAL, S.A. DE C.V.	ALAMEDA MANUEL ENRIQUE ARAUJO, CENTRO COMERCIAL FERIA ROSA, LOCAL 101-1, COL. SAN BENITO	2243-8055/ 2243-3678	mmendoza@cargointernational.com.sv	ACTIVO	BAJO
18	TC281	TACSA DE EL SALVADOR, S.A. DE C.V.	RESIDENCIAL LA CIMA 3 PASAJE 26, CASA No. 44-D, SAN SALVADOR	2273-2031/ FAX 2273-7028	salvador@tacsainc.com	SUSPENDIDO	BAJO
19	TC282	AGENCIA INTERNACIONAL MARITIMA, S.A. DE C.V. (AIMAR, S.A. DE C.V.)	79 AV. NORTE #724, COLONIA ESCALON, SAN SALVADOR.	2263-4624	-	SUSPENDIDO	BAJO
20	TC283	CPS LOGISTICS, S.A. DE C.V.	79 AV. SUR EDIFICIO PLAZA CRISTAL 2do NIVEL LOCAL 2-3, COL. ESCALON, S.A.	2208-3536	kplatero@cpslogistics.com	ACTIVO	BAJO
21	TC284	AVEX EXPRESS, S.A. DE C.V.	URBANIZACION MADRE SELVA, CALLE LLAMA DEL BOSQUE, EDIFICIO AVANTE, 7º. NIVEL, OFICINA 7-02, ANTIGUO CUSCATLAN	2239-4377	lramos@gruporemor.com.sv	ACTIVO	BAJO
22	TC286	GEMMA LOGISTICS	CENTRO PROFESIONAL BUENOS AIRES L-6, CALLE MAQUILISHUAT Y AV 4 DE MAYO, SAN SALCOR	2513-3014	-	ACTIVO	BAJO
23	TC259	DHL EXPRESS (EL SALVADOR), S.A. DE C.V.	URB.Y BLVD.STA.ELENA AVE. APANECA OTE., ANTIGUO CUSCATLÁN	2500-2675/ 2500-2656	elmer.durancalderon@dhl.com	ACTIVO	MEDIO
24	TC278	AEROCASILLAS, DE EL SALVADOR, S.A. DE C.V.	BLVD DEL HIPODROMO, CENTRO COMERCIAL SAN BENITO, ZONA ROSA No. 5, SAN SALVADOR	2500-4067/ 2208-0412	-	ACTIVO	MEDIO
25	TC263	GLOBAL CARGO DE EL SALVADOR, S.A. DE C.V.	63 AV. NET Y 1ra. CALLE PTE AL COSTADO NTE DE PIZZA HUT SALVADOR DEL MUNDO	2530-3030	-	ACTIVO	ALTO
26	TC269	GUTICIA DE EL SALVADOR, S.A. DE C.V.	EDIFICIO FedEx, AV. LAS MAGNOLIAS #130, COL. SAN BENITO, SAN SALVADOR	2250-8800	-	ACTIVO	ALTO

LEY DE SIMPLIFICACIÓN ADUANERA
Artículo 8 letra "B"

La Dirección General deberá publicar por los medios que estime convenientes la lista de los auxiliares de la función pública aduanera autorizados, suspendidos o inhabilitados, así como las direcciones, teléfonos, correos electrónicos u otros datos del lugar en el que ejerzan sus negocios, a efecto de permitirles a los usuarios contactarlos. Asimismo, la Autoridad Aduanera podrá informar por cualquier medio, el listado de los auxiliares de la función pública aduanera, calificados de acuerdo al historial de operaciones en las que hubieran participado y el nivel de riesgo que posean en el sistema.

No.	Código	Empresa	Dirección	Teléfono	Correo electrónico	Estado	Nivel de Riesgo
1	CD001	MUDANZAS INTERNACIONALES, S.A. DE C.V.	C.CHAPARRASTIQUE 34, Z.INDUS.STA.ELENA, ANT.CUSCATLAN	2278-1281	mudisa@mudisa.com	ACTIVO	BAJO
2	CD002	KUEHNE+NAGEL, S.A. DE C.V.	103 AVE. NTE. N° 124,COL.ESCALON	2257-5454	walter.moreira@kuehne-nagel.com	ACTIVO	BAJO
3	CD003	FLAMINGO LINE EL SALVADOR, S.A. DE C.V.	C.SAN ANTONIO ABAD, 19 APTO.27, 2do NIVEL COND. RES. CONSTITUCIÓN, S.S.	2275-4359	ops@ecusal.eculine.net/ pedro@ecusal.eculine.net	ACTIVO	BAJO
4	CD004	DACOTRANS DE CENTROAMÉRICA, S.A.	CALLE ARTURO AMBROGI, N° 8, COL. ESCALON, S.S.	2263-1169/ 2630-3200	dacotrans@integra.com.sv	ACTIVO	BAJO
5	CD005	R. REPRESENTACIONES, S.A. DE C.V.	2A. AVE. NTE. 5-8, SANTA TECLA, LA LIBERTAD	2229-4615	rr@telemovil.com	ACTIVO	BAJO
6	CD006	SERCOGUA EL SALVADOR, S.A. DE C.V.	CALLE RAMON BELLOSO Y CL REPART. FEDERAL DE ALEMANIA NO. 185, COL. ESCALON, SAN SALVADOR	2275-5142	sercoguasal@telesal.net	ACTIVO	BAJO
7	CD007	M.REPRESENTACIONES, S.A. DE C.V.	CALLE ALIRIO CORNEJO, N° 25-C, URB.UNIVERSITARIA NTE. MEJICANOS	2226-0925,	mrsa@navegante.com.sv	ACTIVO	BAJO
8	CD009	C&L CORPORATION, S.A. DE C.V.	JARDIES DE MERLIOT, CALLE AYAGUALO, No. 4M, SANTA TECLA, LA LIBERTAD	2278-4005/ 2278-3993	ctochez@cylcorp.com	INHABILITADO	BAJO
9	CD010	ABC LOGISTICS AND TRANSPORTATION SOLUTIONS, S.A. DE C.V.	79 AV.SUR,Y CL. CUSCATLAN, EDIF.PLAZA CRISTAL LOCAL 2-11, COL. ESCALON, S.S.	2206-5555/ 2206-5488	Jaime.vasquez@gmaritimo.com	ACTIVO	BAJO
10	CD011	AGENCIA DE SERVICIOS, S.A. DE C.V.	79 AV.SUR, Y CL. CUSCATLAN, EDIF.PLAZA CRISTAL LOCAL 2-11, COL. ESCALON, S.S.	2206-5555/ FAX. 2206-5488	Jaime.vasquez@gmaritimo.com	ACTIVO	BAJO
11	CD012	MT CARGA-EXPRESO DE EL SALVADOR, S.A. DE C.V.	KM. 9.5, CARRETERA AL AEROPUERTO, CENTRO COMERCIAL SANTORINI, L 1-A, SAN MARCOS	2207-5757	salvador.monico@grupologistico.com.sv	ACTIVO	BAJO
12	CD014	CORPORACION SALVADOREÑA DE LOGISTICA, S.A. DE C.V.	FINAL 49 AV SUR, COND. BRIGAS DE SAN FRANCISCO, APTO. 2A-3, SAN SALVADOR	2230-6231/ 2230-6232	cslogistic@navegante.com.sv	ACTIVO	BAJO
13	CD016	AIMAR LOGISTIC, S.A. DE C.V.	79 AVE. NTE, N ° 724, COL. ESCALON, SAN SALVADOR.	2209-7900	alfonso-zelada@aimargroup.com	ACTIVO	BAJO
14	CD017	CARGA GLOBAL, S.A. DE C.V.	AVE. REVOLUCION, C. CIRCUNVALACIÓN, # 101, LOCAL 3, COL. SAN BENITO	2275-6290/ 2275-6294	nzacapasal@cargaglobal.com	ACTIVO	BAJO
15	CD019	SISTEMAS INTEGRADOS LOGISTICOS, S.A. DE C.V.	65 AVE.SUR, EDIF. MONTREGOR, L-1A, COL. ESCALON, S.S.	2208-7544	jcmiranda@sil.com.sv	INHABILITADO	BAJO
16	CD022	CARGA URGENTE DE EL SALVADOR, S.A. DE C.V.	CALLE EL MIRADOR, N° 5353, COL. ESCALON, S.S.	2246-7777/ FAX 2246-7799	paviles@quickshipping.com	ACTIVO	BAJO
97	CD134	GEMMA LOGISTICS, S.A. DE C.V.	CALLE MAQUILISHUAT Y AVENNIDA 4 DE MAYO CENTRO PROFESIONAL BUENOS AIRES L-6 SAN SALVADOR	2513-3014	gerencia@gemmalogistics.com	ACTIVO	BAJO
98	CD135	IDEA EL SALVADOR, S.A DE C.V.	KILOMETRO 36 1/2 CARRETERA PANAMERICANA PARQUE INDUSTRIAL AMERICAN PARK EDIFICO G4 CIUDAD ARCE LA LIBERTAD	2340-8120	albertoramirez@idealc.com	ACTIVO	BAJO
99	CD136	TRANSPORTE DE CARGA GLOBAL, SOCIEDAD ANONIMA DE CAPITAL VARIABL	1 CALLE PONIENTE ENTRE 89 Y 91 AV NORTE, No. 4650 COL. ESCALON SAN SALVADOR	2205-4300	guillermo@tcgelsalvador.com	ACTIVO	BAJO
100	CD137	TRANSPORT SERVICE INTERNATIONAL GROUP, S.A. DE C.V.	URB, INDUSTRIAL PLAN DE LA LAGUNA LOTE 21, ANTIGUO CUSCATLAN, LA LIBERTAD	2239-4378	mmotta@gruporemor.com.sv	ACTIVO	BAJO
101	CD138	ALMADISA EL SALVADOR, S.A.	CALLE RAMON BELLOSO Y CALLE REPUBLICA FEDERAL DE ALEMANIA, No. 185, COLONIA ESCALON, SAN SALVADOR.	2557-9674	almadisaelsalvador@gmail.com	ACTIVO	BAJO
102	CD139	PORT TO PORT EL SALVADOR, S.A. DE C.V.	89 AV NORTE Y CALLE EL MIRADOR, EDIF. WTC, TORRE 1 PISO 2 COL. ESCALON, SAN SALVADOR	2254-6646/ 2289-2477	scabezas@central-law.com	ACTIVO	BAJO
103	D001	STAUDT INTERNATIONAL, S.A. DE C.V.	EDIFICIO KIMAX, 5 CL. PONIENTE, No. 3970, COL. ESCALON, SAN SALVADOR	2257-9707/ 2257-9710	staudtsadecv@yahoo.com/ s.lara@bertrand-pineda.com	INHABILITADO	BAJO
104	D002	DUG CARGO EL SALVADOR, S.A. DE C.V.	EDIF WORLD TRADE CENTER, TORRE 1 NIVEL 2, No. 201, colonia escalon, san salvador	2254-6649/ 7038-2232	-	ACTIVO	BAJO
105	CD061	MUNDI CARGA EXPRESS, S.A. DE C.V.	BLVD. CONSTITUCIÓN NO.450, SAN SALVADOR.	2262-1227/ 2262-3342	mundi.carga@navegante.com.sv	INHABILITADO	MEDIO
106	CD035	SISTEMAS AEREOS DE EL SALVADOR, S. A. DE C. V.	AVENIDA BERNAL CALLE SIMILES No. 592 COLONIA YUMURY, SAN SALVADOR	2500-4000	roger@sistemasaereos.com	ACTIVO	ALTO
107	CD089	GRUPO CRISOL, S.A. DE C.V.	AV MANUEL ENRIQUE ARAUJO, CENTRO COMERCIAL FERIA ROSA, LOCAL 230-B, S.S.	2563-3022/ 7927-4911	massintermodal@gmail.com	INHABILITADO	ALTO
108	CD102	GUTIERREZ COURIER & CARGO, S.A. DE C.V.	EDIF. FEDEX. AV. LAS MAGNOLIAS, No. 130, COLO. SAN BENITO, SAN SALVADOR	2250-8811/ 2250-8800/	ada@Guticla.com.sv	ACTIVO	ALTO

Fuente: Direccion General de Aduana.

ANEXO 2

Cuestionario de investigación

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE CONTADURÍA PÚBLICA

CUESTIONARIO

DIRIGIDO A: Profesionales encargados del departamento de TI y gerentes generales de las empresas de transporte marítimo y aéreo.

OBJETIVO: El presente cuestionario pretende recolectar información para sustentar el trabajo de investigación y desarrollo de un modelo de gestión para la seguridad de la información, para empresas dedicadas al transporte marítimo y aéreo que brindan el servicio de monitoreo en línea, ubicadas en el área metropolitana de San Salvador.

INDICACIONES: marque con una "X" la respuesta que considere apropiada.

Nombre de la empresa (opcional): _____

Sello (opcional):

Pregunta 1. ¿Qué tipo de transporte brinda la empresa?

Marítimo____ Aéreo _____ Ambos _____

Pregunta 2: ¿Quién es el responsable directo de la gestión de los recursos informáticos dentro de la empresa?

a) Gerente General

b) Gerente de TI

c) Otro (especifique) _____

Pregunta 3: ¿Se capacita al personal encargado de TI?

SI_____ NO_____

Pregunta 4: ¿En qué áreas se capacita al personal encargado de TI? (Puede seleccionar más de una)

a) Seguridad de la información
b) Gestión de riesgos informáticos
c) Ética y confidencialidad
d) Auditoria de Sistemas
e) Modelos de Gestión de TI (COBIT 5 , ISO, otros)
f) Ninguna de las anteriores

Pregunta 5: ¿La empresa tiene identificados los riesgos en seguridad, relacionados con el monitoreo en línea de mercancías?

SI_____ NO_____

Pregunta 6: ¿La empresa posee una lista de verificación en la implementación de controles, para la mitigación de riesgos de seguridad de la información?

SI_____ NO_____

Pregunta 7: ¿La empresa tiene desarrollados procedimientos claros que le permitan garantizar la confidencialidad de la información, tales como, contraseñas y restricción de acceso a las aplicaciones?

SI_____ NO_____

Pregunta 8: ¿Se asegura la empresa de mantener la información disponible durante las veinticuatro horas del día, para cuando sea requerida por las personas autorizadas?

SI_____ NO_____

Pregunta 9: ¿La empresa posee controles que permitan que la información de monitoreo brindada a sus clientes sea íntegra?

SI_____ NO_____

Pregunta 10 ¿Tiene la empresa planes de contingencia en caso de ocurrir pérdida o robo de información?

SI_____ NO_____

Pregunta 11 ¿Cuenta la empresa con planes de acción a realizar en caso de pérdida de conexión de internet?

SI_____ NO_____

Pregunta 12 ¿Tiene identificado la empresa el impacto económico que ocasionaría la pérdida o modificación de información?

SI_____ NO_____

Pregunta 13 ¿Considera útil el desarrollo de un modelo de gestión que permita identificar los riesgos relacionados a la seguridad de la información y facilite la implementación de controles que los minimicen?

SI_____ NO_____

ANEXO 3

Presentación de Resultados

Pregunta 1. ¿Qué tipo de transporte brinda la empresa?

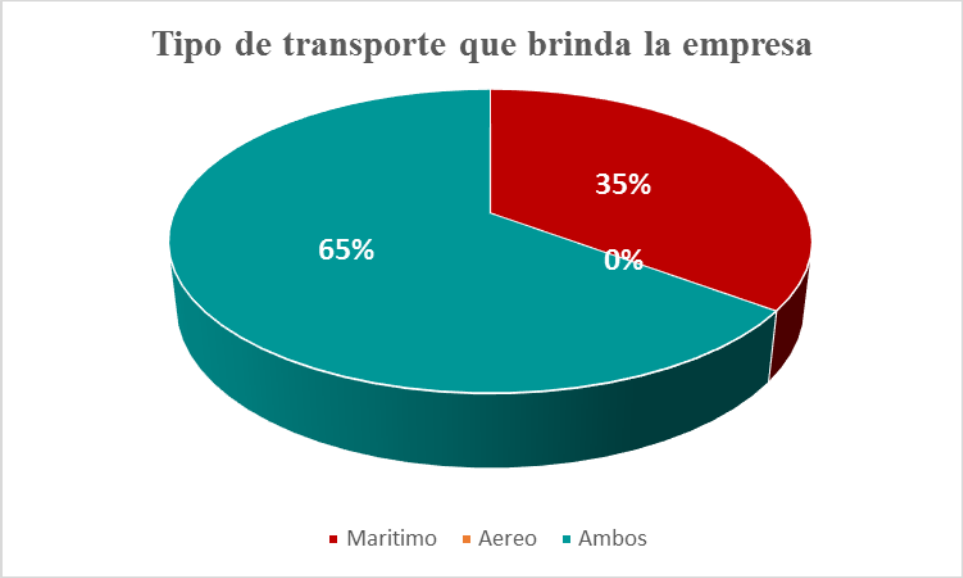
Objetivo: Conocer en cual medio de transporte es más utilizado el servicio de monitoreo en línea con la intención de determinar en cuál es más necesario y enfocar el modelo de acuerdo a las características y exigencias de este tipo de transporte.

Cuadro No 1

Tipo de transporte que brinda la empresa

Tipo de Transporte	Frecuencia absoluta	Frecuencia relativa
Marítimo	13	35%
Aéreo	0	0%
Ambos	24	65%
Total	**37**	**100%**

Gráfico No 1



Fuente: Elaboración propia

Análisis: La demanda que existe actualmente para la importación de mercancías es bastante alta, por lo que es necesario utilizar medios de transporte que brinden rapidez y confianza para transportar dichas mercancías, siendo el transporte marítimo el más utilizado con un 65% y el aéreo con un (35%). Las mercancías transportadas por barco pueden tardar varios días en que arribe, por lo que para este tipo de transporte es más utilizado el monitoreo en línea.

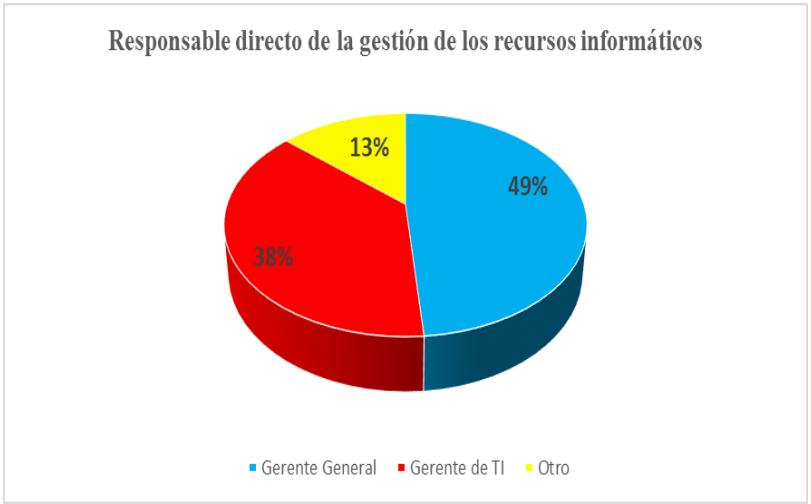
Pregunta 2: ¿Quién es el responsable directo de la gestión de los recursos informáticos dentro de la empresa?

Objetivo: Identificar el personal responsable de la gestión de los recursos informáticos de la empresa y conocer si es el idóneo respecto a la formación académica, para el manejo de los riesgos a que están expuestos tales recursos.

Cuadro No 2
Responsable directo de la gestión de los recursos informáticos

Responsable	Frecuencia absoluta	Frecuencia relativa
Gerente General	18	49%
Gerente de TI	14	38%
Otro	5	14%
Total	**37**	**100%**

Gráfico No 2



Fuente: Elaboración propia

Análisis: Para brindar el servicio de monitoreo en línea eficientemente se utilizan recursos informáticos los cuales dentro de la empresa deben tener a un responsable para su gestión que posea las cualidades y aptitudes necesarias en materia de seguridad, de las empresas encuestadas solo un 38% posee gerente de TI y 49% el responsable es el Gerente General de la empresa, y con un (14%) otra persona como casa matriz dentro de la empresa o agencias fuera del país con afinidad a la empresa y conocimiento en el servicio.

Pregunta 3: ¿Se capacita al personal encargado de TI?

Objetivo: Conocer si las empresas capacitan al personal encargado de los recursos de TI para que estén al día con los conocimientos de las nuevas tecnologías, los riesgos a que se exponen y los controles que se deben implementar.

Cuadro No 3
Capacitación al personal encargado de TI

Se capacita al personal de TI	Frecuencia absoluta	Frecuencia relativa
Si	18	49%
No	19	51%
Total	**37**	**100%**

Gráfico No 3

Fuente: Elaboración propia

Análisis: Estar a la vanguardia de las actualizaciones de recursos e información dentro de una empresa es de suma importancia, para brindar el servicio de monitoreo en línea el personal encargado de TI debe estar constantemente actualizado, como resultado se obtuvo que un 51% de las empresas no capacita a su personal adecuadamente y un (49%) si lo hace.

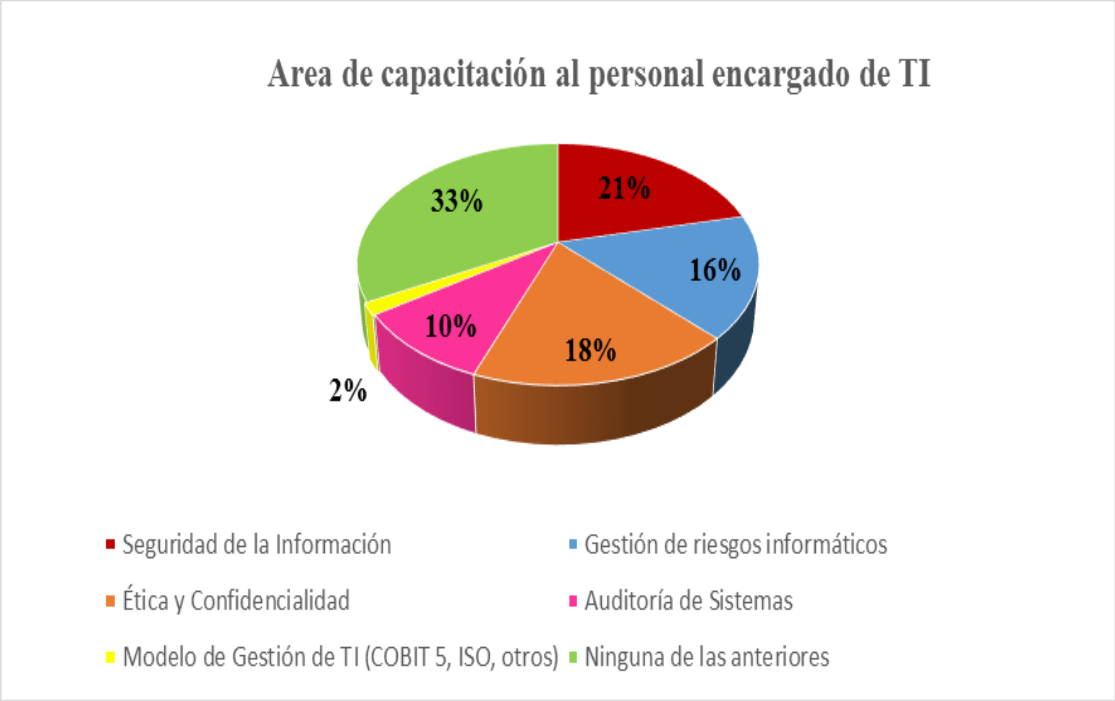
Pregunta 4: ¿En qué áreas se capacita al personal encargado de TI? (Puede seleccionar más de una)

Objetivo: Identificar las áreas en las cuales se capacita al personal encargado de TI con el propósito de fortalecer los controles relacionados a la seguridad.

Cuadro No 4
Áreas que se capacita al personal encargado de TI

Área de capacitación	Frecuencia absoluta	Frecuencia Relativa
Seguridad de la Información	13	21%
Gestión de riesgos informáticos	10	16%
Ética y Confidencialidad	11	18%
Auditoría de Sistemas	6	10%
Modelo de Gestión de TI (COBIT 5, ISO, otros)	1	2%
Ninguna de las anteriores	20	33%
Total	**61**	**100%**

Gráfico No 4



Fuente: Elaboración propia

Análisis: Existen diferentes áreas de capacitación para el uso eficiente e implementación de recursos de TI que permite brindar un mejor servicio de monitoreo en línea, en las empresas dedicadas a brindar este servicio, el personal no está capacitado lo suficiente, a pesar que por los resultados obtenidos se puede observar que el personal ha sido capacitado en diferentes áreas, con un 21% en seguridad de la información, 18% ética y confidencialidad, 16% gestión de riesgos informáticos, 10% auditoría de sistemas y un 2% en COBIT 5 formando esto un (67%) a nivel de las empresas de la zona metropolitana que capacita a su personal y un (33%) que no los capacitan.

Pregunta 5: ¿La empresa tiene identificados los riesgos en seguridad, relacionados con el monitoreo en línea de mercancías?

Objetivo: Conocer si las empresas tienen identificados los riesgos a los que se expone en seguridad, relacionada con el monitoreo en línea para determinar la necesidad de la implementación del modelo.

Cuadro No 5
La empresa tiene identificación de riesgos en seguridad

Identificación riesgos	Frecuencia absoluta	Frecuencia relativa
Si	23	62%
No	14	38%
Total	37	100%

Gráfico No 5

Fuente: Elaboración propia

Análisis: Las empresas para poder gestionar eficientemente la seguridad de la información deben identificar los riesgo a los que están expuestas, con énfasis en los que estén relacionados con el servicio de monitoreo en línea para poder brindar un mejor servicio y satisfacción a los clientes, un 62% de las empresas encuestadas tienen identificados su riesgos y el 38% no cuenta con una lista de identificación de riesgos.

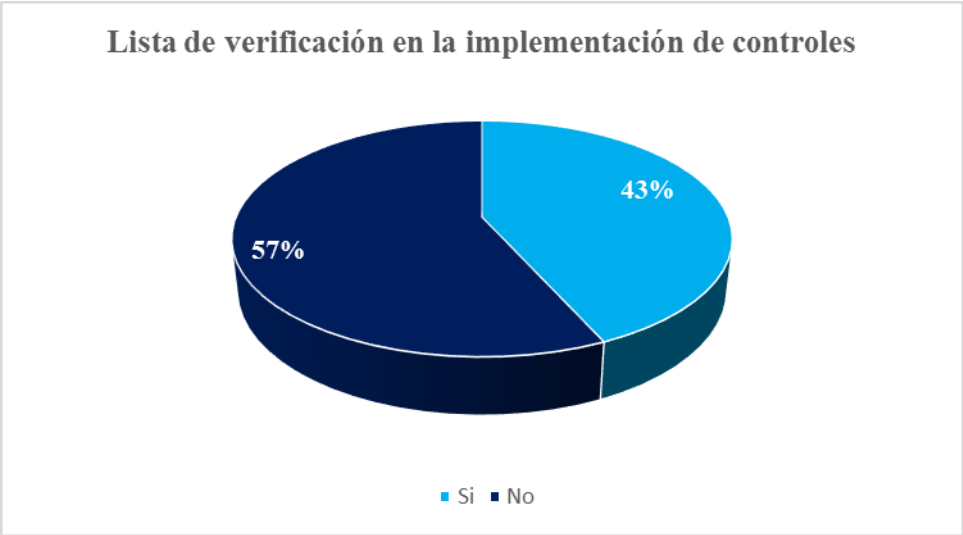
Pregunta 6: ¿La empresa posee una lista de verificación en la implementación de controles, para la mitigación de riesgos de seguridad de la información?

Objetivo: Verificar si la empresa cuenta con controles de mitigación de riesgos para identificar si la empresa aplica procedimientos preventivos relacionados a la seguridad.

Cuadro No 6
Lista de verificación en la implementación de controles, para la mitigación de controles.

Lista de verificación	Frecuencia absoluta	Frecuencia relativa
Si	16	43%
No	21	57%
Total	**37**	**100%**

Gráfico No 6



Fuente: Elaboración propia

Análisis: Para la gestión de la seguridad de la información las empresas deben aplicar procedimientos y controles que le aseguren mitigar los riesgos a los que se está expuesto hasta un nivel aceptable, un 57% de las empresas no posee una lista de

procedimientos que permita la mitigación de riesgos la cual les ayude a gestionar los riesgos y permita aplicación de procedimientos preventivos, solamente un 43% posee una lista de verificación.

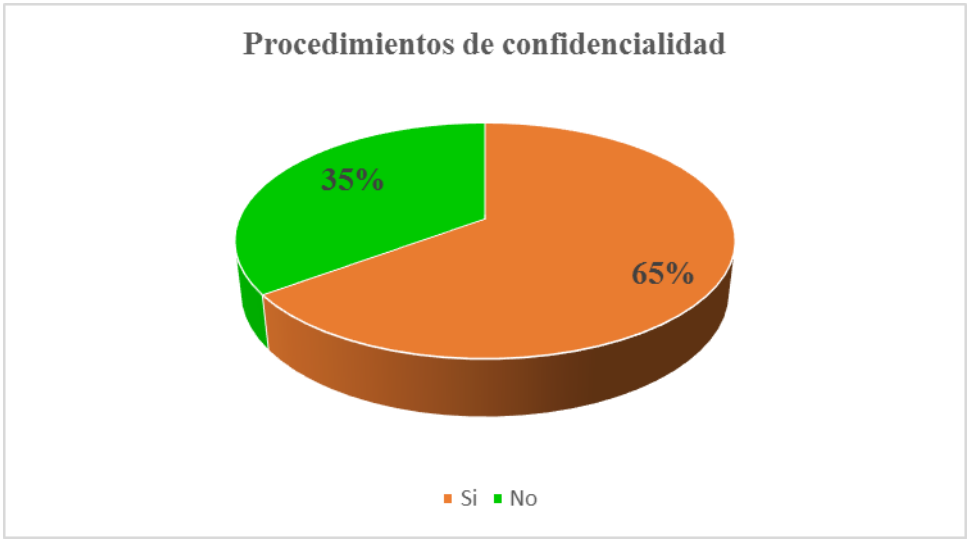
Pregunta 7: ¿La empresa tiene desarrollados procedimientos claros que le permitan garantizar la confidencialidad de la información, tales como, contraseñas y restricción de acceso a las aplicaciones?

Objetivo: Determinar si la empresa cuenta con procedimientos que respalden el buen uso de la información y asegure la no divulgación a personas no autorizadas.

Cuadro No 7
Procedimientos desarrollados de confidencialidad de la información.

Procedimientos desarrollados	Frecuencia absoluta	Frecuencia relativa
Si	24	65%
No	13	35%
Total	37	100%

Gráfico No 7



Fuente: Elaboración propia

Análisis: Toda información es importante dentro de las empresas, por lo que las empresas que brindan el servicio de monitoreo en línea están conscientes de la necesidad de aplicar procedimientos que les permiten garantizar la confidencialidad de la información, tales como brindando contraseñas a sus clientes y procedimientos para el resguardo de la información, un 65% cuenta con procedimientos que garanticen la confidencialidad y un 35% que no.

Pregunta 8: ¿Se asegura la empresa de mantener la información disponible durante las veinticuatro horas del día, para cuando sea requerida por las personas autorizadas?

Objetivo: Verificar si la empresa está capacitada para brindar la información necesaria en el momento oportuno y de esa forma no perder la credibilidad y confianza de sus clientes.

Cuadro No 8
Disponibilidad de la información

Disponibilidad la información	Frecuencia absoluta	Frecuencia relativa
Si	20	54%
No	17	46%
Total	**37**	**100%**

Gráfico No 8

Fuente: Elaboración propia

Análisis: En la actualidad la mayor herramienta en las empresas es el internet, el cual es de suma importancia en el área empresarial, por lo tanto las empresas dedicadas al transporte aéreo y marítimo que brindan el servicio de monitoreo en línea están a la vanguardia de la tecnología, debido a que hoy en día el mantener a sus clientes y usuarios actualizados e informados les permiten tener una mejor relación y confianza con ellos, ya que el hecho de brindar servicio las 24 horas del día permiten un servicio más satisfactorio y de mejor calidad. Aun muchas empresas no están actualizadas debido a que solo un 54% posee el brindar la disponibilidad de la información durante y un 46% aún no se encuentra brindando esta herramienta.

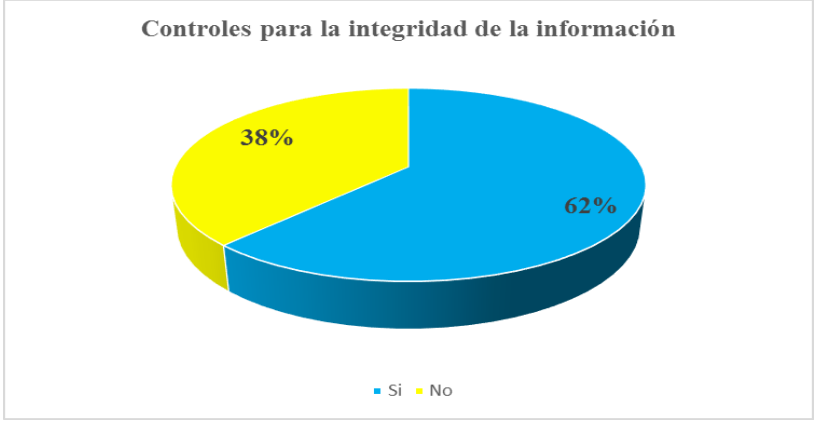
Pregunta 9: ¿La empresa posee controles que permitan que la información de monitoreo brindada a sus clientes sea íntegra?

Objetivo: Conocer si los sistemas de control utilizados por la empresa son aplicados de forma eficiente al momento de brindar información a sus clientes.

Cuadro No 9
Controles para la integridad de la formación

Respuesta	Frecuencia absoluta	Frecuencia relativa
Si	23	62%
No	14	38%
Total	**37**	**100%**

Gráfico No 9



Fuente: Elaboración propia

Análisis: La mayoría de empresa cuenta con controles que les permiten demostrar que la información brindada a sus clientes es integra, el servicio de monitoreo en línea como tal es una herramienta importante para las empresas dedicadas al transporte marítimo y aéreo, debido que por medio de este se mantienen en constante comunicación con su cliente, por lo tanto un 62% de empresa aplican controles que aseguran la integridad de la información y así el cliente pueda tener una mayor confiabilidad a la hora de adquirir servicios, por lo que el 38% no están utilizando correctamente los sistemas de control que poseen para asegurar la integridad de la información, por lo que no cuenta con procedimientos eficientes.

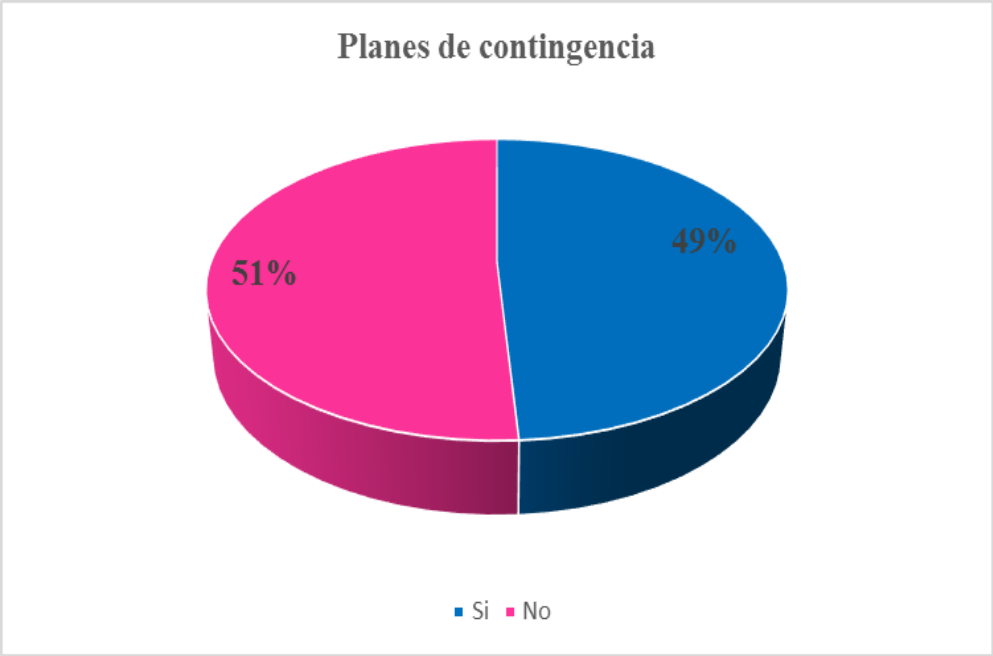
Pregunta 10 ¿Tiene la empresa planes de contingencia en caso de ocurrir pérdida o robo de información?

Objetivo: Conocer si la empresa implementa planes de contingencia en caso de ocurrir incidentes con su información a fin de valorar la importancia en la creación e implementación; que permitan la salvaguarda de información.

Cuadro No 10
Planes de contingencia por pérdida de información

Posee planes de contingencia	Frecuencia absoluta	Frecuencia relativa
Si	18	49%
No	19	51%
Total	**37**	**100%**

Gráfico No 10



Fuente: Elaboración propia

Análisis: El 51% empresas no cuentan con planes de contingencia que les permitan asegurar el resguardo de toda la información procesada, esto puede ocasionarles problemas al momento que pueda ocurrir un incidente ya que la información que se maneja en este tipo de empresas es de suma importancia para el cliente y esto puede llevar a la empresa a tener un bajo prestigio.

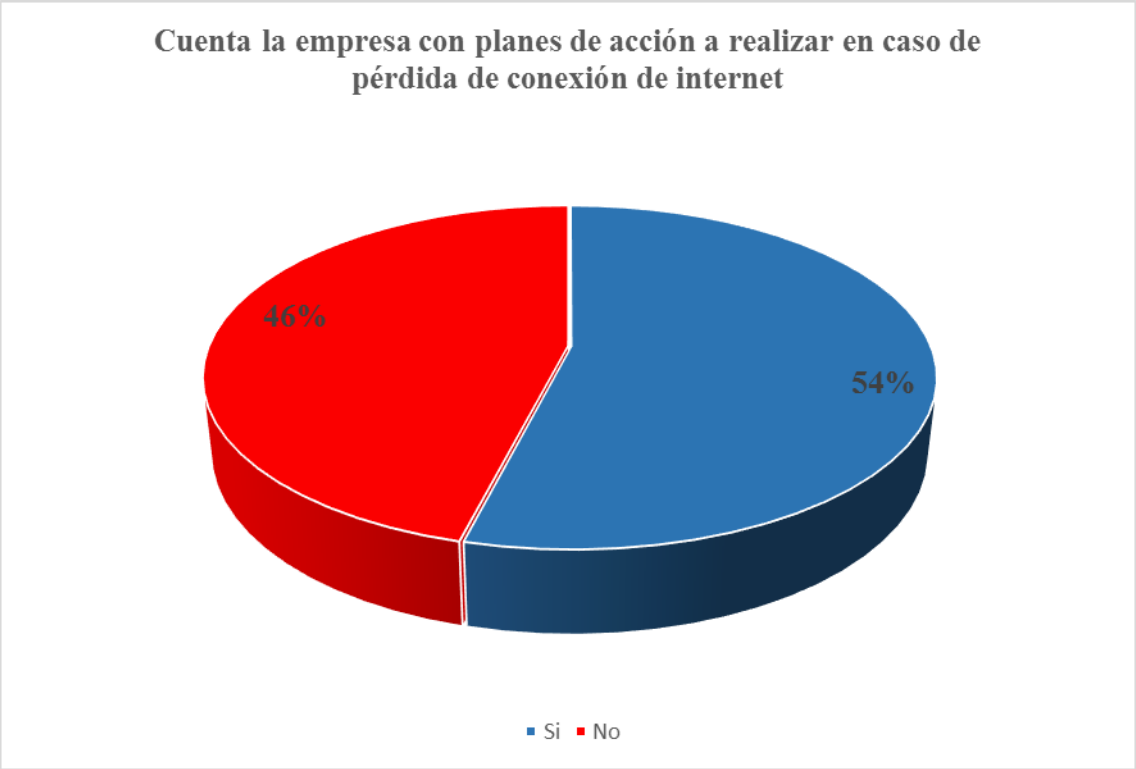
Pregunta 11 ¿Cuenta la empresa con planes de acción a realizar en caso de pérdida de conexión de internet?

Objetivo: Conocer si la empresa cuenta con procedimientos que les permitan actuar en caso de fallas en la conexión de internet, para asegurar la disponibilidad de la información manera continua (7/24/365).

Cuadro No 11
Cuenta la empresa con planes de acción a realizar en caso de pérdida de conexión de internet

Posee planes de acción	Frecuencia absoluta	Frecuencia relativa
Si	20	54%
No	17	46%
Total	**37**	**100%**

Gráfico No 11
Cuenta la empresa con planes de acción a realizar en caso de pérdida de conexión de internet



Fuente: Elaboración propia

Análisis: Para poder brindar el servicio de monitoreo en línea es indispensable mantener la conexión de internet para que el cliente pueda acceder a la información, pero solo un 54% de las empresas cuenta con planes de acción que le garanticen la disponibilidad a dicha información al ocurrir una pérdida de conexión.

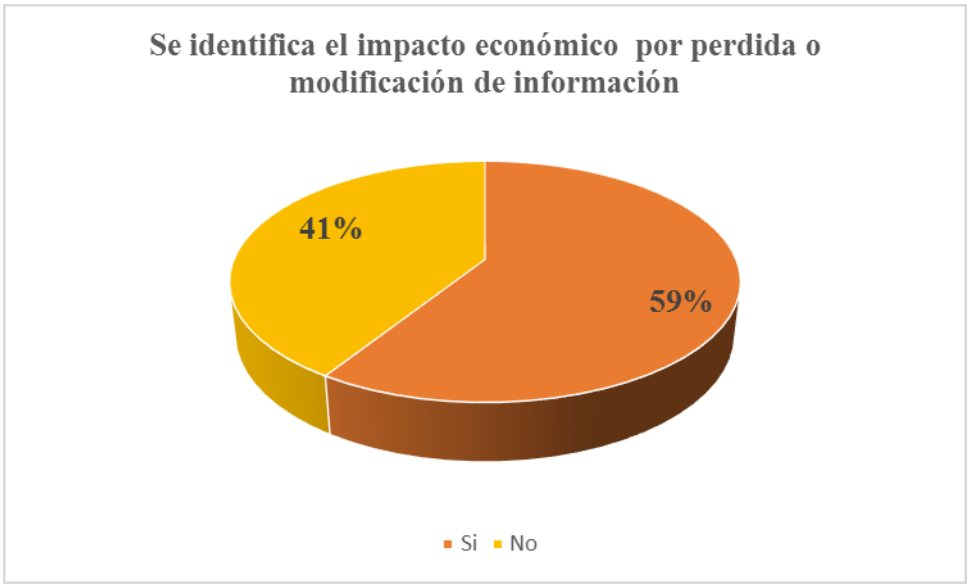
Pregunta 12 ¿Tiene identificado la empresa el impacto económico que ocasionaría la pérdida o modificación de información?

Objetivo: Identificar la necesidad de procedimientos que permitan la medición en términos monetarios, del impacto ocasionado por fallas en la seguridad de la información.

Cuadro No 12
Tiene identificado la empresa el impacto económico que ocasionaría la pérdida o modificación de información.

Se identifica el impacto económico por perdida o modificación de información	Frecuencia absoluta	Frecuencia relativa
Si	22	59%
No	15	41%
Total	**37**	**100%**

Gráfico No 12
Tiene identificado la empresa el impacto económico que ocasionaría la pérdida o modificación de información.



Fuente: Elaboración propia

Análisis: Un número significativo de empresas no posee procedimientos para medir el impacto económico que generaría el tener una falla en la seguridad de la información o que se materialice un riesgo, por lo que al momento de darse esto ocasionaría en la empresa una pérdida significativa ya que el tener identificado el impacto permite la gestión de los recursos eficientemente e invertir en procedimientos preventivos.

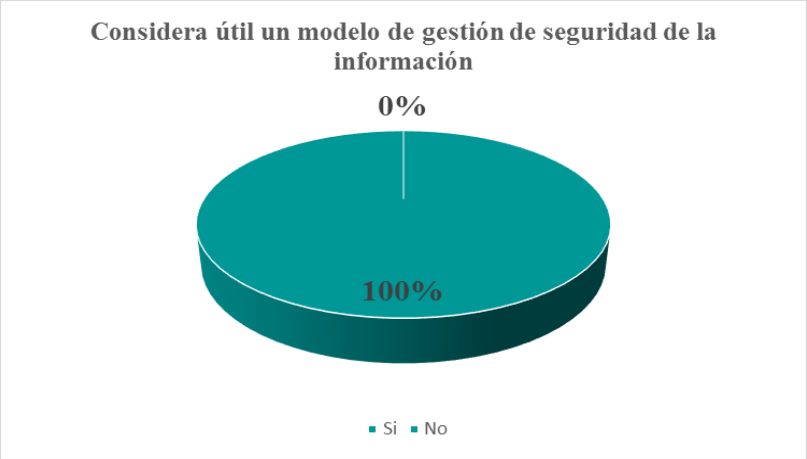
Pregunta 13 ¿Considera útil el desarrollo de un modelo de gestión que permita identificar los riesgos relacionados a la seguridad de la información y facilite la implementación de controles que los minimicen?

Objetivo: Demostrar la necesidad del desarrollo de un modelo de gestión de riesgos en seguridad, para las empresas de transporte marítimo y aéreo que brindan monitoreo en línea.

Cuadro No 13
Se considera útil el desarrollo de un modelo de gestión de seguridad de la información.

Considera útil un modelo de gestión de seguridad de la información	Frecuencia absoluta	Frecuencia relativa
Si	37	100%
No	0	0%
Total	**37**	**100%**

Gráfico No 13
Se considera útil el desarrollo de un modelo de gestión de seguridad de la información.



Fuente: Elaboración propia

Análisis: Todas las empresas coinciden en la importancia que tiene el desarrollo del modelo de gestión de riesgos para la seguridad de la información, ya que al ser adaptado a un marco de referencia de mucho prestigio como lo es COBIT 5, da la posibilidad de aplicar procedimientos prácticos y eficientes que permitirán mantener la información confidencial, integra y disponible y un mejor control y prestigio a la empresa.