República del Ecuador

Universidad Tecnológica Empresarial de Guayaquil - UTEG

Facultad de Estudio de Posgrados

Tesis en opción al título de Magister en:

Sistemas de Información Gerencial

Tema de Tesis:

MODELO DE GESTIÓN DE RIESGOS DE PROCESOS DE TECNOLOGÍA DE INFORMACIÓN BAJO LA NORMA ISO/IEC 27000 EN EMPRESAS AÉREAS DEL ECUADOR

AUTOR:

Lcda. Madheline Torres Hallo

Director de tesis:

Msc. Xavier Mosquera

Junio 2020

Guayaquil – Ecuador

DECLARACIÓN EXPRESA

“La responsabilidad del contenido de esta Tesis de Grado me corresponde exclusivamente y el patrimonio intelectual de la misma a la Universidad Tecnológica Empresarial de Guayaquil”

Lcda. Madheline Katerine Torres Hallo

CI. 0940890056

DEDICATORIA

A Dios, por la vida y sabiduría para enfrentar cada obstáculo y por la oportunidad de alcanzar mis metas, a mis padres y hermana, porque son mi mayor motivación diaria para cada reto y sobre todo por su apoyo incondicional y presencia en cada logro.

AGRADECIMIENTO

A Dios, por la oportunidad de alcanzar esta meta, a mi familia que siempre me motiva a alcanzar nuevos logros, brindando su apoyo y aliento para cumplir mis objetivos, y a mi tutor, por su tiempo, la atención y guía a lo largo del desarrollo de éste trabajo

RESUMEN

Al desarrollar el presente proyecto, se identifica que en las empresas áreas del Ecuador se determinan deficientes en la seguridad para el almacenamiento y transmisión de información lo que genera pérdida de datos para este tipo de organizaciones, es por ello que se ha visto en la necesidad de implementar un modelo de gestión de procesos de tecnología de información aplicando la Norma ISO/IEC 27000 en las empresas áreas del país, por lo que para ello ha resultado preponderante identificar a la Gestión de Riesgos de Información y a la Seguridad en las Tecnologías como variable dependiente y como independiente respectivamente por lo que al realizarlas estadísticamente se demuestra que existe una correlación positiva moderada entre ellas, por lo que en base a estos resultados obtenidos se estructura la propuesta utilizando la metodología de las Normas ISO 27001 y 27002 que consisten en la aplicación de los Sistemas de Seguridad de la Información y en la Gestión de Seguridad respectivamente. Siendo fundamental determinar políticas de seguridad en base a los riesgos operacional y de reputación que se enfocan hacia el manejo de equipos, impacto de los virus informáticos y pérdida de información confidencial lo que incide en el funcionamiento de las empresas del sector aéreo, siendo fundamental la implementación de un modelo de seguridad de información acorde a la familia de las Normas ISO/IEC 27000.

Palabras claves: Riesgo, información, seguridad, tecnología, datos

ABSTRACT

When developing the present project, it is identified that in the areas of Ecuador companies are determined to be deficient in the security for the storage and transmission of information, which generates loss of data for this type of organizations, which is why it has been seen in need to implement an information technology process management model applying ISO / IEC 27000 in companies in the country, so it has been preponderant to identify Information Risk Management and Technology Security as a variable dependent and as independent respectively, so when performing them statistically, it is shown that there is a moderate positive correlation between them, so based on these results, the proposal is structured using the methodology of ISO 27001 and 27002 which consist of the application of Information Security Systems and Security Management give respectively. It is essential to determine security policies based on operational and reputational risks that focus on the management of equipment, impact of computer viruses and loss of confidential information, which affects the operation of companies in the air sector, being essential the Implementation of an information security model according to the family of ISO / IEC 27000 Standards.

Keywords: Risk, information, security, technology, data

ÍNDICE GENERAL

ÍNDICES DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

El transporte aéreo ha marcado, grandes ventajas a lo largo del siglo siendo una de las más importantes la velocidad la cual supera los 1.000 km, por hora, para dar el servicio aeroportuario es necesario contar con una infraestructura sumamente amplia, lo más importante el uso tecnológico que es necesario manejar para el control de este tipo de servicio, por ende es necesario que se realicen grandes inversiones que es desembolsado por aportación pública y privada, es primordial también definir que en la actualidad el desarrollo de los sistemas informativos ha favorecido agilizar, mejorar la gestión y funcionamiento cubriendo las necesidades de los clientes nacionales e internacionales (Ministerio de Transporte, 2015).

De esta manera el transporte aéreo ha facilitado a los viajeros poder trasladarse a grande distancias en cuestión de horas ya sea por negociación, turismo, migración u otros, de la misma forma ha facilitado al transporte de carga logrando el tráfico de productos que son enviados de manera urgente medicinas, repuestos, correo, permitiendo el abastecimiento de productos y medicinas necesarias a tiempo para evitar problemas sociales.

Bajo esta perspectiva se puede mencionar que el aspecto tecnológico ha permitido el desarrollo empresarial y, social, por ende las organizaciones implementan nueva tecnología, de la misma manera capacitan a su personal con el fin de cubrir las exigencias de los clientes potenciales, permitiendo de esta manera mejorar el posicionamiento dentro de un mercado actual que es altamente competitivo, siendo importante desarrollar un modelo de gestión bajo la Norma ISO/IEC 27000, con el objetivo de evitar problemas tecnológicos al momento de realizar cualquier proceso de servicio y, de esta manera evitar conflictos internos que puede afectar de manera directa al cliente externo causando inconformidad y decrepitación por la aerolínea.

Es importante mencionar que no pueden ocurrir problemas sobre todo en servicio aéreo de carga, mismo que al retrasar vuelos o problemas de logística

puede provocar la pérdida de la mercadería, perjudicando a los ingresos del nivel empresarial, por lo cual es primordial llevar un control de la información que se maneja de forma interna y de esta forma cubrir las necesidades de los clientes nacionales e internacionales que utilizan los servicios aeroportuarios.

Se puede decir que el transporte aéreo en el Ecuador en los últimos años ha incrementado de manera notable esto debido a las características de servicio, es decir el traslado de un lugar a otro en un tiempo más reducido que al realizar en transporte terrestre de manera interna, sin embargo el costo de pasaje es alto debido a la perspectiva de costo de infraestructura y de servicio. Se recalca también que el principal movimiento aeroportuario con el exterior, el tráfico aéreo es intenso y el país ecuatoriano cuenta con dos principales aeropuertos internacionales ubicados en la provincia de Pichincha y Guayas a los que llegan empresas aéreas tanto extranjeras y nacionales, en cuanto al aspecto nacional existen rutas que unen a las ciudades el país como (Ministerio de Transporte, 2015).

- Quito
- Guayaquil
- Cuenca
- Loja
- Máchala
- Salinas
- Tulcán
- Islas Galápagos
- Manta
- Esmeraldas
- Latacunga
- Lago Agrio

Observación: Cabe mencionar que la mayoría de la región oriental al encontrarse con variedad de pozos de petróleo, es también servida por empresas aéreas ecuatorianas que se utilizan en el transporte aéreo, por ende es importante contar con un modelo de gestión de riesgos bajo la norma ISO/IEC 27000, que permitirá brindar un servicio de calidad y seguro.

> Es importante recalcar que la herramienta o la norma ISO/IEC 27000, la cual se relaciona con los procesos de tecnología de información, ha sido favorable para que las organizaciones puedan llevar un mejor control de la información, esto debido al crecimiento, desarrollo y dependencia del avance tecnológico de la información que maneja las organizaciones, por ende es primordial que los sectores productivos protejan sus activos de datos críticos para garantizar la confianza continúa de los clientes potenciales que son parte clave para el desarrollo empresarial, por lo cual las organizaciones están inmiscuidas a salvaguardas datos que son importantes para satisfacer las necesidades de los clientes potenciales , lo ideal es buscar una fidelización, por ende se requiere proteger los siguientes datos o información empresarial (Raya & Domínguez , 2015, pág. 15).

- Asegurar sus activos críticos empresariales, con el fin de lograr cumplir los objetivos empresariales.
- Se debe administrar los riesgos de forma mucho más efectiva, para de esta manera implementar estrategias para poder contrarrestar o cambiar con el fin de lograr las metas de la organización.
- Permite mejorar y mantener la confianza del cliente, a través de la seguridad de la información tecnológica.
- Permite demostrar conformidad con las mejores prácticas internacionales, lograr el desarrollo empresarial.
- Evitar daños de marca, pérdida de ganancias o posibles multas regulatorias, por no poder salvaguardar la información tecnológica.
- Desarrollar su postura de seguridad de la información junto con los desarrollos tecnológicos, para de esta manera lograr fidelizar a los clientes

> dentro de un mercado altamente competitivo (Raya & Domínguez , 2015, pág. 25)

De esta manera la norma ISO/IEC 27000, lo que busca es que exista una protección a los datos informativos que maneja las empresas, con el fin de lograr proteger los servicios y procesos internos, para la cual se implemente tecnología informativa avanzada la cual presta las seguridades para lograr el desarrollo organizacional dentro de un mercado altamente competitivo, por tal razón es importante realizar un modelo de gestión de riesgos con el objetivo de proteger la información para su mejor desempeño.

De esta manera se determina que la norma ISO 27000 permitirá presentar una descripción general de diferentes sistemas de gestión para favorecer a la seguridad de la información y, los términos de cada una de las organizaciones, con el fin de garantizar los datos e información interna, logrando salvaguardar datos importantes de los clientes potenciales, dicha herramienta o norma puede ser utilizado por los siguientes organizaciones

- Pequeñas empresas
- Medianas empresas
- Grandes empresas
- Empresas multinacionales
- Agencias gubernamentales
- Organizaciones sin fines de lucro (Raya & Domínguez , 2015, pág. 32)

El sector aéreo del Ecuador está conformado por un grupo de empresas de transportes aéreos, mismos que brindan un servicio de traslado del personal y de cargamento de un lugar a otro, no obstante, como en toda empresa, existe riesgos en el área de Tecnología, se han identificado pérdidas de información relevante lo que se evidencia como uno de los problemas principales de la seguridad en el almacenamiento de datos. Es por ello, que se desarrolla la actual investigación con la finalidad de establecer un modelo de gestión de riesgos con

el que se posibilite un mejoramiento en la tecnología del sector aéreo, para lo cual, se requiere efectuar un análisis minucioso del SGSI (Sistema de Gestión de Seguridad de la Información), a fin de identificar estándares de seguridad que eviten la pérdida de información.

Por lo tanto, en base a las características del presente estudio, se identifica la siguiente interrogante:

- ¿Cómo es el modelo de gestión de riesgos de procesos de tecnología de información bajo la norma ISO/IEC 27000 en el sector aéreo del Ecuador?

En definitiva, el realizar una adecuada gestión de riesgo bajo la norma ISO/IEC 27000 posibilita a un mejoramiento de seguridad en el almacenaje de datos para las empresas del sector aéreo del Ecuador, por lo que en la investigación actual se obtienen conocimientos de acuerdo a la gestión, seguridad, procesos e información, para que de acuerdo a ello se efectúe un análisis en las empresas en este sector.

CAPITULO I

MARCO TEÓRICO CONCEPTUAL

1.1. ANTECEDENTES

El sector aéreo del Ecuador se conforma por un conjunto de empresas que se dedican a trasladar de un lugar a otro pasajeros o cargamento a través del uso de aeronaves, este tipo de entidades como otras realizan el almacenamiento de información en herramientas o equipos informáticos, por lo cual, es necesario establecer políticas de seguridad para evitar la pérdida de información y, lo primordial garantizar la satisfacción hacia los clientes potenciales que confían en los servicios de la organización.

Es por ello que en el presente trabajo se analiza la Norma ISO 27000, la misma que se conforma por un conjunto de estándares que evalúan la seguridad de la información, y a su vez, se han realizado investigaciones anteriores aplicando el SGSI (Sistema de Gestión de Seguridad de la Información). Uno de estos estudios es el realizado por (Moyano & Suárez, 2017) en las que se concluye la importancia de las autorías en la seguridad para el tratamiento de información, con las que se permite otorgar un mayor control en la seguridad en el sistema que se ha implementado.

1.2. PLANTEAMIENTO DEL PROBLEMA

Se reconoce que en las empresas del sector aéreo del Ecuador se han evidenciado pérdidas de información lo que se demuestran fallas en el almacenamiento de datos, en un 40% (Rosales, 2017) esto a su vez refleja una inseguridad en el procesamiento de información por parte de las compañías que pertenecen a este sector, por lo cual no se brinda una información efectiva hacia los clientes. Los directivos que administran a este tipo de entidades, determinan la existencia del problema propuesto, pero no se han tomado las medidas correctivas con las que sea posible otorgar una solución válida ante la pérdida

de datos, esto en realidad incrementa las posibilidades de riesgos para las empresas y con ello, la disminución de sus ventajas competitivas frente a negocios que deseen captar un mayor posicionamiento en el mercado.

Por lo tanto, el problema principal que es objeto de la investigación actual es:

Inadecuado manejo de los riesgos en la seguridad de las tecnologías de información del sector aéreo del Ecuador

La actual investigación se desarrolla con la finalidad de establecer un modelo de gestión de riesgos con el que se posibilite un mejoramiento de la seguridad en las tecnologías de la información (TI) bajo las normas ISO/IEC 27000 del sector aéreo del país. Para ello se requiere efectuar un análisis minucioso del SGSI (Sistema de Gestión de Seguridad de la Información), a través del cual se identifiquen estándares de seguridad que eviten la pérdida de información.

1.2.1. Síntomas

La falta de seguridad en el almacenamiento de información de las empresas que conforma el sector aéreo del Ecuador presenta un conjunto de síntomas que afectan el buen funcionamiento de las compañías por lo que es necesario identificarlas cada una de ellas por separado:

- **Pérdida de ingresos.** Al disponer información empresarial en poder de terceras personas no autorizadas, posibilita a que se compartan estos datos con las compañías de la competencia, por lo que a su vez este tipo de negocios desarrollan nuevos servicios buscando una mayor participación de mercado. De tal manera que como resultado de ello, las entidades del sector aéreo del Ecuador reflejan una reducción de sus niveles de ingresos dentro de un corto plazo.
- **Daño en la reputación de la marca.** Las empresas que mantienen un alto posicionamiento en el mercado poseen mayores posibilidades de obtener ingresos a través de sus ventas, sin embargo, al perder información valiosa que es compartida por personas ajenas a la organización se podría hacerles creer a los clientes potenciales que la compañía estaría brindando un servicio pésimo, lo que genera desconfianza en las próximas compras.

- **Incremento de costos.** La pérdida de información de las empresas en el sector aéreo del Ecuador posibilita al incremento de costos dentro de un mediano plazo, costos que se reflejan en el Estado de Resultados de las compañías, lo que disminuye directamente los beneficios para sus inversionistas ya sea por la reducción de su presencia en el mercado o por el incremento de nuevos servicios diseñados por iniciativa de las empresas competidoras.

1.2.2. Causas

Las principales causas que conllevan a la pérdida de información están dadas por errores humanos de los trabajadores de las empresas, por fallos mecánicos o eléctricos, por virus informáticos y por el robo de equipos. En este caso resulta necesario y hasta fundamental explicar cada uno de ellos en los párrafos siguientes:

- **Errores humanos.** En las empresas del sector aéreo al igual que en otro tipo de negocios, se han evidenciado problemas de borrado accidental de archivos lo que se otorga como resultado la pérdida de datos al no disponer de una copia de seguridad de la información.
- **Fallos mecánicos o eléctricos.** La falta de mantenimiento de los equipos informáticos y la ausencia de actualización en softwares específicos ha provocado problemas en el almacenamiento de la información. A más de ello, las fallas eléctricas que se han dado en las instalaciones de las empresas inciden también en la pérdida continua de datos lo que se tiene como consecuencia un incremento de sus costos.
- **Virus informáticos.** Al estar las empresas conectadas al internet posibilita a que se intercambie información ya sea entre trabajadores, clientes y proveedores, sin embargo, el estar conectados a una red virtual también ocasiona la proliferación de virus informáticos que pretenden recabar datos importantes de las compañías, lo que a su vez afecta no solo al almacenamiento de la información sino también a la pérdida de equipos utilizados.

- **Robo de equipos.** La información que se almacena en los discos duros de las computadoras de las empresas es más valioso que el costo de los equipos, puesto que se registran datos que son confidenciales sobre el funcionamiento del negocio para el diseño de un nuevo servicio, proyectos que se pretenda desarrollar dentro de un futuro próximo.

1.2.3. Pronóstico

La ausencia de un manejo adecuado en la gestión de riesgos de las tecnologías de la información perjudica a las ventajas competitivas de las empresas del sector aéreo que suelen ser únicas en el mercado, pues la pérdida de datos incide a que no se puedan desarrollar el diseño de nuevos productos o sus modificaciones para captar un mayor posicionamiento de marca.

El robo de información es calificado como un delito en el Ecuador pues se establecen sanciones para las personas que se apropien de forma fraudulenta por medios electrónicos según como lo señala el Código Orgánico Integral Penal (COIP, 2017, Art. 190), sin embargo, esto no es suficiente para enfrentar las técnicas maliciosas utilizadas para la obtención de datos sin autorización, por lo que de mantenerse esta tendencia en el largo plazo se identifica como consecuencia que la mayoría de compañías ejecuten actos ilícitos para obtener información cuya finalidad sea la de mantener una ventaja competitiva con la que se permita sobresalir al resto de entidades similares.

1.3. FORMULACIÓN DEL PROBLEMA

¿Qué impacto tendría en la seguridad de la información del sector aéreo del Ecuador, la aplicación de un modelo de gestión de riesgos bajo la norma ISO/IEC 27000?

1.4. Sistematización del problema

¿Qué impacto presentará la seguridad de la información?

¿Cómo influye la seguridad de la información para brindar calidad de servicio?

¿La Norma ISO/IEC 27000, permita un control de la seguridad de la información?

1.4. OBJETIVOS

1.4.1. Objetivo general

- Establecer el modelo de gestión de riesgos de procesos de tecnologías de información bajo la norma ISO/IEC 27000 en el sector aéreo del Ecuador

1.4.2. Objetivos específicos

- Determinar las características de la gestión de riesgos, de la norma ISO/ICE 27000 y del Sistema de Gestión de Seguridad de la Información (SGSI)
- Analizar la gestión del riesgo en la seguridad de información de las empresas del sector aéreo
- Diseñar el modelo de gestión de riesgos en relación a la seguridad bajo la norma ISO/IEC 27000 en el sector aéreo del Ecuador.

1.5. JUSTIFICACIÓN

1.5.1. Justificación teórica

La importancia de la investigación actual se fundamenta en la obtención de conocimientos sobre riesgos informáticos, gestión de procesos y principalmente sobre el manejo de la seguridad en las tecnologías de la información en base a la Norma ISO/IEC 27000, en la cual se determinan estándares para el buen manejo de los datos de las empresas, estándares que son aplicables para cualquier organización, ya sea pública o privada.

El obtener un mayor conocimiento sobre los riesgos informáticos posibilita a establecer medidas de corrección ante posibles eventos de pérdida de información que pudieren ocurrir en cualquier tipo de negocio inclusive en los hogares de las familias, lo que favorece una mayor seguridad informática, principalmente al navegar por internet como un medio de comunicación virtual ya sea en las instalaciones de las empresas o fuera de ellas.

A más de ello, al disponer de amplios conocimientos sobre la gestión de riesgos en las empresas se facilita la prevención de accidentes operacionales a través de tácticas previamente establecidas que resguardan la salud de los trabajadores, favoreciendo también el intercambio de información que garantice su seguridad al ser utilizada por miembros autorizados de la organización.

En definitiva, la justificación teórica en el presente estudio concierne a la obtención de conocimientos suficientes de las Normas ISO/IEC 27000 para la seguridad de las tecnologías de la información, el análisis de los riesgos informáticos en las herramientas utilizadas y la gestión de riesgos que al conocer a profundidad posibilita la reducción de pérdidas durante el uso de equipos tecnológicos.

1.5.2. Justificación práctica

La importancia de la investigación a desarrollarse se fundamenta en la ejecución práctica de un modelo de gestión de riesgos de procesos en la seguridad de las tecnologías de información, el cual será aplicable a las empresas que forman parte del sector aéreo del Ecuador. Para ello, se requiere la utilización de las Normas ISO/IEC 27000 (Organización Internacional para la Estandarización y Comisión Electrotécnica Internacional por sus siglas en inglés) con la intencionalidad de establecer estándares para la seguridad de la información e intercambio de datos.

De tal manera, que al aplicarse este tipo de modelo mejorará el almacenamiento de datos ya sea en el corto, mediano y largo plazo, cuyos principales beneficiarios son todos aquellos trabajadores que realizan actividades en la que se utilicen dispositivos tecnológicos, pues se estarían implementando estándares de seguridad que eviten la pérdidas de información.

Por ende, la justificación práctica está dada por la aplicación del modelo de riesgos en la seguridad de información, sus beneficiarios son los colaboradores que utilizan tecnologías para el almacenamiento de datos de las empresas que pertenecen al sector aéreo del país.

1.6. MARCO TEÓRICO

1.6.1. Gestión de riesgos de procesos

1.6.1.1. Gestión y su importancia

Se denomina como gestión el “asumir y ejecutar responsabilidades sobre un conjunto de actividades coordinadas entre sí para llevarlas a cabo de acuerdo a la utilización de recursos disponibles” (Pérez Fernández, 2016, pág. 15)

Es decir, que, de acuerdo a términos empresariales, se establece que la gestión busca cumplir con el desarrollo de actividades que se hayan comprometido estableciendo un uso adecuado de los recursos de la organización, por ende, la gestión se enfoca hacia una correcta utilización de los recursos disponibles mediante la designación previa de responsabilidades para su posterior cumplimiento.

1.6.1.2. Riesgo y su importancia

Por otra parte, los riesgos se definen como la “combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas” (Centro Internacional para la Investigación del Fenómeno de El Niño, 2016)

Desde este enfoque, se conceptualiza como riesgo a la posibilidad que ocurra un acontecimiento negativo. Los principales factores que conforman el riesgo son la amenaza y vulnerabilidad, la primera de ellas se refiere a la potencial ocurrencia de algún tipo de evento dentro de un lugar en particular, mientras que la vulnerabilidad está dada por las deficiencias de seguridad de un sujeto, sistema u organización.

1.6.1.3. Gestión de riesgo

La gestión de riesgo se conoce como el “proceso de identificar, analizar y cuantificar las probabilidades de pérdidas y efectos secundarios que se desprenden de los desastres, así como de las acciones preventivas, correctivas y reductivas correspondientes que deben emprenderse” (Peribáñez, Hernández, & Sánchez, 2017, pág. 108).

A más de ello, se determina como gestión del riesgo al “manejo de los accidentes operacionales, enfermedades, incendios o catástrofes naturales, entre otros, que pueden afectar a la consecución de los objetivos de cualquier organización”.

Por consiguiente, a partir de las definiciones anteriores se establece que la gestión de riesgo se refiere a un análisis de las posibles pérdidas que pudieran ocurrir para que posteriormente se determinen acciones de prevención necesarias con las que se evitarán los eventos catastróficos.

1.6.1.4. Tipos de riesgos en las empresas

Las empresas al realizar actividades que se encaminen hacia la producción o prestación de un servicio se determinan diversos tipos de riesgos entre los cuales se detallan a continuación:

- Riesgo estratégico
- Riesgo de conformidad
- Riesgo financiero
- Riesgo laboral
- Riesgo de reputación
- Riesgo ambiental
- Riesgo operacional (García, 2015)

Por ende, cada uno de ellos es necesario que sean explicados detenidamente puesto que al producirse un evento desfavorable en cualquier tipo de empresa se estaría afectando al alcance de las metas departamentos y los objetivos propios de la organización.

1.6.1.4.1. Riesgo estratégico

Se denomina al riesgo estratégico como “el impacto actual y futuro en los ingresos y el capital que podría surgir de las decisiones adversas de negocios, la aplicación indebida de las decisiones, o la falta de capacidad de respuesta a los cambios de la industria” (Argentina: JP Morgan Chase Bank N.A, 2018).

Desde esta perspectiva, el riesgo estratégico se enfoca en la posibilidad de decisiones incorrectas durante la planificación, implementación o control de las estrategias para dificultar el logro de los objetivos organizacionales, por lo que se otorga una inadecuada distribución de los recursos que se requieren para la ejecución de actividades de calidad.

Los riesgos estratégicos deberán ser controlados por la alta gerencia de las empresas, siguiendo un proceso sistemático para identificar, alinear y controlar el alcance de los objetivos estratégicos, por lo que es indispensable una adecuada planificación y gestión de la organización dentro de un largo plazo.

1.6.1.4.2. Riesgo de conformidad

Los riesgos de conformidad “son aquellos que están sujetos a las regulaciones y reglas legislativas o burocráticas, o aquellos asociados con las mejores prácticas para propósitos de inversión” (Griffin, 2017)

Es decir, que los riesgos de conformidad se caracterizan por la posibilidad de que se determinen sanciones legales realizadas por las entidades públicas ya sea del gobierno central a través de los ministerios o del gobierno local a través de los municipios y juntas parroquiales, por lo que al final estas eventualidades afectan el normal desarrollo de las actividades de las empresas.

1.6.1.4.3. Riesgo operacional

El riesgo operacional es aquel que “puede provocar pérdidas debido a errores humanos, procesos internos inadecuados o defectuosos, fallos en los sistemas y como consecuencia de acontecimientos externos” (Banco Bilvao Vizcaya Argentaria BBVA, 2016)

En base a esta definición, el riesgo operacional es aquel que ocurre al interior de las instalaciones de la empresa debido a posibles fallos internos ocasionados por las máquinas y equipos utilizados inadecuadamente por parte de los trabajadores, los cuales suelen producirse ante la imposibilidad de aplicar de forma correcta los procesos operativos que se hayan establecido.

1.6.1.4.4. Riesgo financiero

El riesgo financiero hace énfasis a la:

> Incertidumbre producida en el rendimiento de una inversión, debida a los cambios producidos en el sector en el que se opera, a la imposibilidad de devolución del capital por una de las partes y a la inestabilidad de los mercados financieros (Banco Bilbao Vizcaya Argentaria, BBVA, 2019)

Bajo esta conceptualización, el riesgo financiero está dado por la incertidumbre para la obtención del rendimiento de las inversiones y la inestabilidad de los mercados financieros.

En el primer caso, el riesgo financiero se relaciona con la pérdida del valor invertido ante los posibles eventos adversos que pudieran ocurrir ya sea dentro o fuera de la organización, de tal manera que a mayor plazo para la obtención de rentabilidades, mayor será el riesgo que se genera para los inversionistas.

Así mismo, la inestabilidad de los mercados financieros genera un mayor tipo de riesgo en la volatilidad del valor accionario de las empresas y de los inversores, lo que posibilidad a obtener mayores beneficios o pérdidas dentro de un menor tiempo del que se haya planificado.

1.6.1.4.5. Riesgos laborales

Se denomina como riesgo laboral a “la relación entre la probabilidad de que un trabajador sufra un determinado daño derivado del trabajo con elementos peligrosos y la severidad de dicho daño” (Organización Internacional del Trabajo, 2018, pág. 20).

Desde este enfoque el riesgo laboral se determina en la incertidumbre de que un colaborador de cualquier tipo de organización sufra algún accidente durante el ejercicio de sus actividades profesionales en su puesto de trabajo.

Es por ello, que las empresas deberán prevenir aquellas situaciones que conlleven a un accidente laboral o la evolución de una enfermedad en los colaboradores ocasionada por las condiciones de trabajo, de tal manera que la

prevención adquiera una mayor importancia para evitar peligros que se transformen en riesgos durante el desempeño de las actividades laborales.

1.6.1.4.6. Riesgos ambientales

A los riesgos ambientales se denominan como la “posibilidad de que por forma natural o por acción humana se produzca daño en el medio ambiente. Es el efecto de incertidumbre, por lo que implica tanto efectos potenciales negativos como positivos, es decir amenazas y oportunidades (Nueva ISO 14001:2015, 2018)

Los riesgos ambientales se caracterizan por la probabilidad de que se produzca un evento natural adverso afectando las instalaciones de la empresa y por ende, la pérdida de bienes del negocio. Esto se denomina también como una amenaza en el entorno externo organizacional puesto que sucede fuera de las instalaciones del negocio, por lo que en caso de que ocurriera no solamente se estarían afectando a una sola compañía, sino también a un conjunto de empresas que se instalen en el mismo sector.

1.6.1.4.7. Riesgo de reputación

Este tipo de riesgo se refiere a la “pérdida de reputación de una compañía o el punto de vista comunitario puede ser el resultado de fallas en los servicios, demandas o publicidad negativa. Las reputaciones toman tiempo para construirse, pero se pueden perder en un día” (Griffin, 2017)

Por lo tanto, el riesgo de reputación se refiere a la pérdida de credibilidad ante los clientes en los bienes y servicios que se comercializan por parte de las empresas, esto podría ocurrir cuando se evidencian fallas en los productos elaborados que ya se encuentran en el mercado.

A más de ello, se identifica también un riesgo de reputación ante la existencia de demandas legales que afecten la marca o imagen de la empresa, puesto que sus clientes mantendrán desconfianza en adquirir sus productos, por lo que es indispensable que se desarrollen campañas de fidelización hacia el consumidor dentro de un largo plazo.

Definición y estructura de una Matriz de Riesgos

> La matriz de riegos se le conoce como una herramienta de gestión, la cual permite definir los riegos existentes dentro de una organización y, lo que se busca es reducir esta problemática beneficiando la seguridad y salud del personal interno y externo que está inmerso a la empresa (Lara, 2015, p. 83).

En la siguiente Gráfico se aprecia una matriz de riesgos, la cual permite conocer de manera clara los procesos que presentan problemas dentro de la organización.

Gráfico 1. Matriz de Riesgos

		PROBABILIDAD				
		Raro	**Poco probable**	**Posible**	**Muy probable**	**Casi seguro**
CONSECUENCIAS	**Despreciable**	Bajo	Bajo	Bajo	Medio	Medio
	Menores	Bajo	Bajo	Medio	Medio	Medio
	Moderadas	Medio	Medio	Medio	Alto	Alto
	Mayores	Medio	Medio	Alto	Alto	Muy alto
	Catastróficas	Medio	Alto	Alto	Muy alto	Muy alto

Fuente: *Tomado del libro Medición y Control de Riesgos* (Lara, 2015, p. 83)
Elaborado por: *La autora*

1.6.1.5. El riesgo y la seguridad en las tecnologías de información

Tanto el riesgo operacional como el riesgo de reputación mantienen una amplia relación con la seguridad de las tecnologías de la información, por lo cual se ha diseñado una tabla en la que se identifiquen los tipos de riesgos que influyan en la pérdida de información:

Tabla 1. Riesgo e inseguridad en las tecnologías de la información

TIPO DE RIESGO	CAUSAS	RESULTADO

Riesgo operacional	• Pérdida de información por errores humanos • Fallas electrónicas de los equipos informáticos	Inseguridad en las tecnologías de información
Riesgo de reputación	• Robo de datos que conlleven a publicidad negativa • Virus informáticos que posibiliten el secuestro de información	

Fuente: (Benjamín, 2016, pág. 487)
Elaborado por: La Autora

1.6.1.6. Proceso y modelo de gestión

Definición

Se conoce como proceso al "conjunto de actividades interrelacionadas con insumos y rendimientos prescritos, que atraviesan los límites funcionales de una organización" (Benjamín, 2016, pág. 487). En base a la conceptuación anterior, se denomina como proceso a la agrupación de actividades consecutivas que se encuentran interrelacionas entre sí en la que se establecen responsabilidades para el desarrollo de programas o proyectos que forman parte de la organización.

A más de ello, se reconoce que a través de un modelo de gestión se "busca simplificar y armonizar la labor de las entidades en la generación y presentación de planes, reportes e informes" (Colombia: Departamento Administrativo de la Función Pública, 2015). Por lo que de acuerdo a esta definición se identifica que un modelo de gestión se encamina hacia la simplificación de actividades con la intencionalidad de optimizar sus tiempos de ejecución con lo que se estaría generando un mayor ahorro en los recursos utilizados dentro de las entidades u organizaciones que apliquen un modelo similar.

En base a ello, tomando en cuenta las características que forman parte del proceso y del modelo de gestión se tiene como resultado, el modelo de gestión de procesos el cual se conceptualiza como el conjunto de acciones consecutivas que simplifican el trabajo de las organizaciones buscando la optimización de sus recursos utilizados.

Tipos de modelos de gestión de riesgos

Existen varios modelos de gestión de riegos, entre los cuales se detalla al riesgo operacional, gestión de riesgos por proyectos y gestión de oportunidades, los cuales favorecen a mitigar los riegos de las organizaciones.

Riesgo operacional

> Se determina que el riesgo operacional, hace referencia al riego de pérdidas que tienen que ver por la falta de adecuaciones o falla en los procesos internos ocasionado por el personal o los sistemas que permiten brindar un servicio o realizar un producto y, lo que busca este modelo es identificar, evaluar, dar un seguimiento y controlar los riegos (Morgan, 2015, pág. 2).

De esta manera se considera que el modelo de riesgo operacional está vinculado a salvaguardar la seguridad del personal de la organización, permitiendo que exista un ambiente laboral adecuado para su desempeño.

Ventajas de riesgo operacional

- Cuenta con políticas de riegos.
- Presenta procedimientos.
- Presenta una infraestructura adecuada.
- Evalúa la vulnerabilidad del espacio de trabajo.
- Adopta medias para los riesgos (Morgan, 2015, pág. 2).

Desventajas de riesgo operacional

- La no existencia de responsabilidad por parte de los trabajadores de la empresa.
- No ejecutar medias para los riesgos a tiempo.
- Falta de presupuesto para implementar las medidas para que no exista un riesgo operacional (Morgan, 2015, pág. 2).

Gestión de Riesgos por proyectos

> Al hablar de la gestión de riegos por proyectos, se define como la identificación, análisis y planificación para poder presentar un control de riego del proyecto, que la organización ponga en marcha con el objetivo de brindar seguridad y salud al personal interno y externo que está inmerso dentro de la entidad (EALDE, 2018)

Ventajas de la gestión de Riesgos por proyectos

- Planificar la gestión de riegos
- Permite identificar los riegos de la organización.
- Realizar un análisis cualitativo y cualitativo de los riegos.
- Planificar el tipo de estrategias.
- Llevar un control de los riegos (EALDE, 2018)

Desventajas de la gestión de Riesgos por proyectos

- No tener la predisposición del personal.
- Falta de presupuesto para implementar.
- No existe un análisis profundo de los riegos.
- No contar con un ambiente idóneo de trabajo (EALDE, 2018).

Modelo de gestión de oportunidades

Al referirnos al modelo de gestión de oportunidades, se define que está relacionado con la "perspectiva organizacional que se enfoca alcanzar los objetivos empresariales contando con una infraestructura adecua para la seguridad y salud de sus trabajadores" (Delaux, 2017, pág. 50).

Ventajas de la gestión de oportunidades

- Primero identifica en que se presenta el riesgo
- Define sus causas y consecuencias.
- Da conocer la procedencia del riesgo.
- Define el impacto de riesgo.
- Determina las escalas de evaluación (Delaux, 2017, pág. 50).

Desventajas de la gestión de oportunidades

- No contar con la predisposición del recurso humano.
- No determinar de manera adecuado los riegos que afecta a los procesos de servicio.
- No presentar escalas de evaluación idóneas a los riegos existentes dentro de la organización (Delaux, 2017, pág. 50).

Bajo esta perspectiva de análisis de los modelos de riegos, se pude determinar que la Gestión de Riesgos por proyectos, es un modelo que permitirá diseñar un modelo de gestión de riesgos de procesos de tecnología de información bajo la NORMA ISO/IEC 27000 en empresas aéreas del Ecuador, permitiendo de esta manera contribuir con la seguridad se sus procesos de servicios**.**

1.6.2. Seguridad en las tecnologías de la información

1.6.2.1. Conceptualización de seguridad y seguridad de la información

En términos generales, se define como seguridad al “estado en el cual los peligros que pueden provocar daños de tipo físico, psicológico o material son controlados para preservar la salud y el bienestar de los individuos, de la comunidad y de las empresas” (Canadá: Instituto Nacional de Salud Pública de Québec, 2019). Por lo tanto, la seguridad se refiere al control de los peligros que puedan estar expuestos las personas y las empresas dentro de las instalaciones o de un territorio claramente especificado.

Además, se identifica como seguridad de la información a la “capacidad de protección de datos de manera que personas o sistemas no autorizados no puedan leerlos o modificarlos” (ISO 25000, 2019). Es decir, que la seguridad de la información involucra el control automático de datos tanto en su utilización, transferencia y almacenamiento de tal manera que nadie de las personas que no dispongan de autorización no podría conocerlos ni realizar algún tipo de modificación.

1.6.2.2. Tecnologías de Información (TI)

Se identifica que las tecnologías de información se refieren a la “utilización de tecnología, específicamente computadoras y ordenadores electrónicos para el manejo y procesamiento de información como la captura, transformación, almacenamiento, protección, y recuperación de datos” (Quetglás, Toledo, & Cerverón, 2015, pág. 78)

Por ende, de acuerdo a este enfoque las tecnologías de la información están dadas por la utilización de datos obtenidos a través de fuentes electrónicas, así como sus formas de almacenamiento, protección y recuperación de información que podría captarse mediante las tecnologías que podrían utilizarse.

1.6.2.3. Norma ISO / IEC 27000

1.6.2.3.1. Definición e importancia

La norma ISO / IEC 27000 se conoce como:

> Al conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña (ISO27000.ES, 2015)

Por lo tanto, tomando en consideración la definición anterior se conoce que la norma ISO/ICE 27000 se conforma por un conjunto de reglamentos que han sido desarrollados por la ISO y por la IEC, con la finalidad de mejorar la gestión de la seguridad de cualquier tipo de organización, ya sea pública o privada.

La importancia de la norma ISO/ICE 27000 está que sirve como una ayuda valiosa para establecer la forma de gestionar la seguridad en una organización empresarial o pública que se encuentran bajo responsabilidad del Estado, es decir, que mediante la implementación de la norma ISO/ICE 27000 identifica

diversos tipos de estándares para establecer normativas de seguridad al interior de las organizaciones.

1.6.2.3.2. Clasificación de la ISO / IEC 27000

Norma ISO 27001

Se conoce a la Norma ISO 27001 como:

> Una solución de mejora continua en base a la cual puede desarrollarse un Sistema de Gestión de Seguridad de la Información (SGSI) que permita evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información de una organización tanto propia como datos de terceros (Organismo de Certificacion Global, 2018, pág. 3)

En relación al párrafo anterior, la norma ISO 27001 se fundamenta en la evaluación de riesgos que intervienen durante la utilización, transferencia y almacenamiento de datos desarrollando un Sistema de Gestión de Seguridad de la Información (SGSI) que se enfoque hacia el mejoramiento continuo en el desenvolvimiento de las empresas.

Norma ISO 27002

A la Norma ISO 27002 se caracteriza por ser “una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información” (Corporación ORCI Inc., 2019)

Es decir, que en la Norma ISO 27002 se enfoca hacia la seguridad de la información estableciendo un manual en el que se especifican los objetivos de control, por ende, se identifica la manera en que se deben tratar los riesgos para el cumplimiento de la norma ISO 27001.

Norma ISO 27003

La Norma ISO 27003 pretende “focalizar su atención en los aspectos requeridos para un diseño exitoso y una buena implementación del Sistema de

Gestión de Seguridad de la Información" (Sistemas en Gestión de Seguridad de la Información, 2015)

Por lo tanto, la norma ISO 27003 se refiere a la aplicación del Sistema de Gestión de Seguridad de la Información utilizando el ciclo PHVA (Planificar, Hacer, Verificar y Actuar) como herramienta principal en la implementación de políticas para el mejoramiento de la seguridad informática.

Norma ISO 27004

La Norma ISO 27004 "posibilita una variedad de mejores prácticas para la medición de los resultados de un Sistema de Gestión de la Seguridad de la Información" (ISO Platform, 2015)

En cuanto a la norma ISO 27004 se determinar las técnicas, instrumentos o herramientas que se utilizan para la cuantificación de los resultados obtenidos en el control del Sistema de Gestión de Seguridad de la Información (SGCI) de acuerdo al ciclo de PHVA (Planificar, Hacer, Verificar y Actuar).

Norma ISO 27005

La Norma ISO 27005 determina:

> Las diferentes directrices para la gestión de los Riesgos en la Seguridad de la Información. Se trata de una norma de apoyo a los conceptos generales que vienen especificados en la ISO 27001 y se encuentra diseñada para ayudar a aplicar, de una forma satisfactoria, la seguridad de la información basada en un enfoque de gestión de riesgos (ISO Tools, 2015)

Por consiguiente, en la Norma ISO 27005 se detalla la conceptualización general de la gestión del riesgo de acuerdo a la seguridad de la información en la que se proporciona una ayuda valiosa para la implementación de la ISO 27001.

Norma ISO 27006

En la Norma ISO 27006 se “específica todos los requisitos para lograr la acreditación de las entidades de auditoría y certificación de Sistema de Gestión de Seguridad de la Información” (Sistema de Gestión de Seguridad de la Información, 2015).

Por lo tanto, el propósito principal de la Norma ISO 27006 se enfoca hacia la acreditación para las empresas que han implementado la Norma ISO 27000 en la seguridad de la información, por lo que para ello se identifican entidades de autoría para la entrega de los correspondientes certificados de sistemas de gestión.

Norma ISO 27007

A la Norma ISO 27007 se la denomina como:

> Un manual de auditoría de un Sistema de Gestión de Seguridad de la Información. Es un estándar Internacional el cual ha sido creado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (ISO Tools, 2015)

En la ISO 27007 se conforma por un catálogo en el cual se determina los estándares de auditoría para el buen funcionamiento del Sistema de Gestión de Seguridad de la Información, en el mismo que se establece como modelo para su implementación, monitoreo y revisión durante el tratamiento de datos que se manejan a través de equipos o herramientas informáticos.

Norma ISO 27032

La Norma ISO 27032 se caracteriza por “ofrecer una orientación que fortalezca el estado de la Ciberseguridad en una empresa, utilizando los puntos técnicos y estratégicos más importantes para esa actividad” (Grupo ACMS Consultores, 2016)

Desde esta perspectiva, se reconoce que en la Norma ISO 27032 posibilita un conjunto de estándares que se aplican para un mayor control en los riesgos durante la navegación virtual, fortaleciendo así el intercambio de información y permitiendo que se utilicen procesos más seguros durante el tratamiento de datos.

La Norma ISO 27032 es aplicable para aquellas empresas que utilicen información que se almacene en equipos o herramientas informáticas, puesto que posibilita a una mayor seguridad en la transferencia y almacenaje de datos entre dos o varios trabajadores de una misma institución.

1.6.2.3.3. Sistema de Gestión de la Seguridad de Información

Definición del SGSI

El Sistema de Gestión de la Seguridad de Información (SGSI) se denomina como aquella que parte del "sistema general de gestión, basada en un enfoque de riesgo comercial para establecer, implantar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información" (Symantec Corporation, 2016)

También se determina que el Sistema de Gestión de la Seguridad de Información (SGSI) consiste en "las políticas, procedimientos, directrices, recursos y actividades asociadas, que se administran colectivamente por una organización protegiendo sus activos de información" (International Organization for Standardization and International Electrotechnical Commission, 2015, pág. 13).

Por ende, de acuerdo a las definiciones anteriores que se especifican, se establece que el Sistema de Gestión de la Seguridad de la Información (SGSI) es un conjunto de procedimientos, normativas y políticas que se interrelacionan entre sí con la finalidad de mejorar la seguridad en la información existente en una entidad pública o privada favoreciendo la protección de activos de la organización. Es por ello que el Sistema de Gestión de la Seguridad de la Información (SGSI) está relacionado con la tecnología pues para el almacenamiento de datos las empresas utilizan herramientas o instrumentos

electrónicos para guardar información, por lo que al no aplicarse las medidas adecuadas se determina un mayor riesgo de perder este tipo de datos, y por ende, información valiosa para la futura toma de decisiones por parte de los directivos de la entidad.

Importancia del SGSI

La importancia del Sistema de Gestión de la Seguridad de información, es que permite realizar un plan de diseño para poder implementar y realizar un mantenimiento de los procesos los cuales influye en la eficiencia de información para el manejo organizado de la entidad.

Se da conocer que en la actualidad los avances tecnológicos han provocado una preocupación al personal directivo de las entidades, sin embargo la importancia del Sistema de Gestión de la Seguridad permitirá garantizar un nivel de disponibilidad confidencial e integridad relacionada con el manejo de información de manera diaria, siendo una principal herramienta que contribuye al desarrollo laboral empresariales de cada una de las organización para poder competir dentro de un mercado objetivo altamente competitivo (Safesociety , 2018).

Es importante también recalcar que las redes y comunicaciones en el mundo cuentan con diferentes amenazas como pueden ser los ataques de ciber delincuentes es decir que buscan información o datos relevantes y confidenciales que son de gran interés comercial, todo ello es ocasionado por intereses económicos, competitividad y comerciales, todo esta problemática actual no solamente afecta a las grandes empresas sino también a pequeña, incluso a los gobiernos o personas están extensas de este tipo de ataque virtual (Safesociety , 2018).

Un dato importante, entre los años 2016 y 2017 se determina que se han presentado 198 millones de ciberataques lo que ha ocasionado pérdidas económicas de las grandes empresas alcanzando un monto de más de 6 mil millones de dólares, bajo esta problemática encontrada se visualiza qué es de importancia implementar una SGSI (Sistema de Gestión de la Seguridad de información) la cual está fundamentada en las Normas ISO 27000, que se

enfoca a establecer los procesos permitiendo de esa manera la protección de información confidencial qué maneja las empresas, por tal razón un Sistema de Gestión de la Seguridad de información permitirá analizar y gestionar riesgos, evitando perjuicios para las organizaciones, de esta manera se define las beneficios que presenta dicha herramienta.

- Puede garantizar un nivel alto de integridad, confiabilidad en relación a información que genera por las empresas de manera diaria.
- Para acceder a la información se debe presentar controles de confiabilidad y seguridad, es decir que únicamente el personal autorizado podrá hacer uso de la información acorde a su conveniencia.
- Permitirá presentar información certera para en base a ello lograr un mejoramiento continuo en relación a los incidentes de información y seguridad, a tiempo para que la empresa sea perjudicada.
- Se logrará que los proveedores y clientes estratégicos de las organizaciones, presenten una confianza alta, esto por la implementación de la herramienta de un Sistema de Gestión de la Seguridad de Información.
- Permite a las organizaciones garantizar el desarrollo económico y social dentro de un mercado altamente competitivo
- El Sistema de Gestión de la Seguridad de Información, permite mantener un margen eficiente de la información que las organizaciones manejan en relación a los proveedores clientes, siendo lo factores más importantes para el desarrollo de las empresas.
- El Sistema de Gestión de la Seguridad de Información, es considerado como un factor diferenciador que genera un plus dentro del mercado qué en la actualidad es altamente competitivo (Safesociety , 2018).

Definición de dominios virtuales

De acuerdo al autor Bobiller & Banquet a conocer que un dominio virtual “se denomina aquellos nombres de domicilios que se encuentran dentro de un servidor virtual en un mismo ordenador con dirección IP” (Bobiller & Banquet , 2015, pág. 397).El tema de análisis del autor Banquet esta direcciona con el uso de sistemas informáticos y de cómo influye para el desarrollo de las

organizaciones, misma que permitirá conocer la idea clara en el diseño de un modelo de gestión de riesgos de procesos de tecnología de información bajo la norma ISO/IEC 27000 en empresas aéreas del Ecuador

De esta manera podemos decir que la gestión de dominios virtuales es una Graficación sencilla, un servidor postfix gestiona un solo dominio de correo, el mismo que debe estar asociado a la empresa, sin embargo puede suceder que desee gestionar varios dominios de correo, este tipo de tareas cumple a la perfección la herramienta de dominios virtuales, es decir que los servidores de alojamiento de internet utilizan los dominios virtuales, con los que puedan gestionar varias cadenas de dominios de clientes en un solo servidor, también es utilizado por la empresas donde el servicio informático gestiona el correo de dos entidades distintas cuando, se realiza una adquisición (Bobiller & Banquet , 2015, pág. 402).

Es importante también recalcar que en la actualidad el dominio es primordial para el desarrollo de las organizaciones, en la cual se da conocer al mercado la imagen o nombre de la organización, en los siguientes ítems se da conocer las recomendaciones para la selección y gestión de un dominio.

- Es importante determinar un nombre corto el mismo que es preferible que sea el nombre de la organización la cual se quiere dar a conocer en el mercado, por lo cual si se tratase de un blog debe ser de 3 a 63 caracteres considerando letras y números fáciles de recordar.
- También es importante evitar el uso de guiones, para que no exista la confusión al momento de requerirlo, se busca que sea entendible y de fácil manipulación por parte de la organización.
- Para manejar un dominio es preferible que lo administre una persona de confianza, para de esta manera evitar problemas que puede causar a la organización, como puede ser económicos o la imagen o marca que tiene a disposición del mercado (Bobiller & Banquet , 2015, pág. 399).

Tipos de dominios virtuales

Dentro de los tipos de dominios virtuales, se determina los siguientes, los cuales son de uso común o más relevantes y utilizados en todo el mundo

com = Sitio comercial.
net = Empresa de servicios de Internet.
org = Organización sin fines de lucro.
info = Sitio informativo.
biz = Sitio de negocios.

Dominio Sitio comercial (com)

Son dominios de sitio comercial la cual está determinado por la sigla (com), que son de fácil identificación para los usuarios o proveedores que tienen relación directa con la organización.

Dominio Empresa de servicios de Internet (Net)

El dominio (NET), identifica a empresas que prestan servicios de internet, de esta manera facilita al cliente para identificar el servicio que pretende solicitar, con el objetivo de cubrir una necesidad.

Organización sin fines de lucro (org)

La siglas ORG, permite a la población identificar la actividad de las organizaciones sin fines de lucro, bajo esta perspectiva el obtener dominios está en beneficiar del posicionamiento de la organización dentro de un mercado altamente competitivo.

Sitio informativo (info)

El dominio INFO, facilita a las personas que navegan, identificar un sitio informativo, acorde a la perspectiva de búsqueda que estén realizando, permitiendo de esta manera encontrar datos con mayor rapidez.

Sitio de negocios (biz)

Dentro de los dominios existentes hay uno que identifica sitios de negocios facilitando de esta manera la interacción de los empresarios que desean conocer aspectos económicos de las organizaciones o su posicionamiento dentro del mercado con el objetivo de buscar invertir.

La gestión de riesgo en un SGSI

Al implementar un diseño de un Sistema de Gestión de la Seguridad de Información (SGSI), es importante requerir de un amplio conocimiento relacionado con la gestión de riegos, mediante la cual se puede tomar decisiones o medidas para contrarrestar los aspectos negativos que puede afectar a la organización las cuales pueden ser sociales o económicas.

Es importante definir que un Risque Management se determina como un proceso que permite minimizar o eliminar riegos los cuales pueden afectar la base de datos de la organización, para evitar esta problemática es importante tomar en cuenta los siguientes factores.

- **Eliminar riesgos.-** Este factor facilitará eliminar riesgos que están asociados dentro de la información de la organización, sin embargo para realizar este proceso es importante contar con un fondo económico que permita solucionar la problemática encontrada.
- **Transferir el riesgo.-** Al hablar de la transferencia de riesgo se refiere a contratar un servicio externo, mismo que permita mitigar problemas internos de la organización, por lo que es importante contar un seguro que respalde siempre y cuando los activos superen al costo de seguro.
- **Asumir el riesgo.-** El asumir el riesgo significa que la organización no tomará medidas para restringir la problemática en relación a la información, sin embargo tendrá que llegar un control para que no exista problemas internos que pueda afectar su estabilidad dentro de un mercado objetivo altamente competitivo.

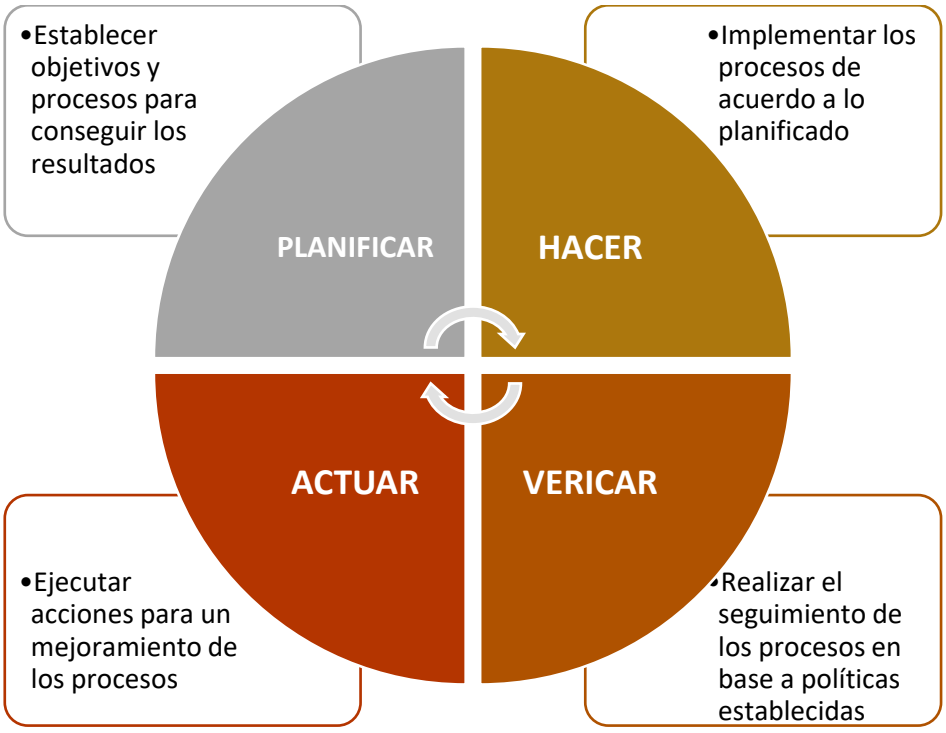
- **Mitigar el riesgo.-** Para poder mitigar el riesgo en la organización, se deberá implementar mediadas o políticas qué permita salvaguardar los activos informativos, las cuales tienen que ser documentadas y, gestionados de manera interna por la empresa (Calder, 2015, pág. 15).

1.6.2.3.4. Ciclo de Deming

El ciclo de Deming o también conocido como PHVA es una "herramienta que se utiliza en las empresas para mejorar su nivel de gestión mediante un control eficiente de sus procesos y actividades tanto internas como externas, lo que posibilita la reducción de errores en la toma de decisiones importantes" (España: Instituto de Productividad Empresarial Aplicada, 2018).

Las siglas PHVA significan Planificar, Hacer, Verificar y Actuar, las mismas que permiten determinar el ciclo de la mejora continua de acuerdo como se observa en la siguiente Gráfico:

Gráfico 2. Planificar, Hacer, Verificar y Actuar



Fuente: *Adaptado del libro de Lean Manufacturing de Hernández y Vizán* (2016)
Elaborado por: *La autora*

Tomando en consideración las cuatro etapas que conforman el ciclo de Deming, es posible aplicar cada una de estas fases en las familias ISO 27000 en relación al Sistema de Gestión de Seguridad de la Información (SGSI):

Tabla 2. Ciclo de Deming en el SGSI

No.	ETAPAS	SUB ETAPAS
1	Planificar	1. Definir la política de seguridad 2. Establecer el alcance del SGSI 3. Realizar el análisis de riesgo 4. Seleccionar los controles 5. Definir competencias 6. Establecer un mapa de procesos 7. Definir autoridades y responsabilidades
2	Hacer	1. Implantar el plan de gestión de riesgos 2. Implantar el SGSI 3. Implantar los controles
3	Verificar	1. Revisar internamente el SGSI 2. Realizar auditorías internas del SGSI 3. Poner en marcha indicadores y métricas 4. Hacer una revisión por parte de la Dirección
4	Actuar	1. Adoptar acciones correctivas 2. Adoptar acciones de mejora

Fuente: Tomado del libro La Norma ISO 27001 (2016)
Elaborado por: La autora

Etapa de planificar

> Según el autor López da conocer que planificar es la identificación de actividades que están provocando problemas en la organización, una vez identificada la problemática se busca mitigar con la implementación de herramientas que permita que la organización mejore sus réditos económicos y sociales (López, 2017, pág. 181).

De esta manera la etapa de planificar permite definir que es necesario implementar un diseño de un modelo de gestión de riegos de procesos de tecnología de información bajo la norma ISO/IEC 27000, en empresas aéreas del Ecuador, con el objetivo de reducir los riegos de seguridad de información.

Etapa de hacer

> La etapa de hacer según el autor Alessandri, da conocer que es la parte primordial para el crecimiento y permanencia de una empresa dentro de un mercado competitivo, por ende es importante definir los parámetros o políticas a cumplir por parte del personal interno, en la cual es importante que se utilice el método de CANVAS, que permitirá obtener un panorama claro de lo que se desea realizar o alcanzar logrando una rentabilidad y posicionamiento para la organización (Ramos, 2017, pág. 28).

De esta manera al diseñar un modelo de gestión de riegos de procesos de tecnología de información bajo la norma ISO/IEC 27000 en empresas aéreas del Ecuador, al analizar la etapa de qué hacer, se da a conocer lo que se pretende implementar dentro de la organización como es el implantar planes de gestión de riesgos, implantar el Sistema de Gestión de la Seguridad de Información (SGSI) y, también llevar un control para su cumplimiento y lograr el beneficio que pretende alcanzar la organización.

Etapa de verificar

> Dentro de la etapa de verificar, permitirá llevar un control de la herramienta a implementar, de esta manera revisar que se cumplan con los procesos, sin embargo si se presentan informales negativos, poder corregir y cumplir con los objetivos que la organización pretende alcanzar (Martínez, 2017, pág. 127).

De esta manera al diseñar un modelo de gestión de riegos de procesos de tecnología de información bajo la norma ISO/IEC 27000, tendrá que revisar de

manera interna el Sistema de Gestión de la Seguridad de Información (SGSI) así como realizar una auditoría, y de esta manera analizar los indicadores y métricas para conocer si es efectivo la implementación del proyecto, todos estos procesos son revisados por la alta gerencia para la toma de decisiones.

Etapa de actuar

> La etapa de actuar, es la que permite comparar las actividades que se desarrollaron dentro de una propuesta, identificando si esta permitirá cumplir con los objetivos o no se cumplió por problemas en los procesos de ejecución, bajo este análisis se actúa con la mejora en la problemática, para de esta manera logras las metas que se quieren alcanzar dentro de un periodo de tiempo (Martínez, 2017, pág. 130)

De esta manera se define que la etapa de actuar, es una de las más favorables para el cumplimiento de los objetivos propuestos, por lo que es importante analizar el motivo por lo que no se cumplió con lo previsto, si es así buscar estrategias para implantar y lograr cumplir con las metas de la organización con el objetivo de lograr su permanencia dentro del mercado competitivo.

CAPÍTULO II

MARCO METODOLÓGICO

2.1. Tipo de diseño, alcance y enfoque de investigación

2.1.1. Tipo de diseño

Dadas las características del presente trabajo, se ha considerado aplicar la investigación no experimental, el cual se denomina como el “estudio que se realizan sin la manipulación deliberada de variables y en los que sólo se observan los fenómenos en su ambiente natural para después analizarlos” (Hernández Sampieri, Fernández, & Baptista, 2016, p. 149).

En base a esta definición se reconoce que en el estudio a realizarse, la información de los datos obtenidos no será modificada o sufrirán algún tipo de alteración por parte del investigador, puesto que se analizarán los resultados tal y como se presenten con la finalidad de obtener conclusiones válidas sobre la situación actual de las diversas empresas que conforman el sector aéreo del Ecuador, por ende, los resultados que se presenten estarían reflejando la realidad para este tipo de entidades de acuerdo al manejo de los riesgos que se suscitan en las tecnologías de la información.

2.1.2. Alcance de investigación

Al desarrollar el alcance de investigación, se aplican tanto el estudio descriptivo como el estudio exploratorio los mismos que son necesarios en la investigación a realizarse haciendo referencia a los riesgos en la información y a la Norma ISO / IEC 27000:

- **Investigación descriptiva.** Son aquellos que buscan “especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis” (Del Cid, Méndez, & Sandoval, 2015, p. 29), por lo tanto, el estudio es de tipo descriptivo al establecer las características más sobresalientes de las empresas que

forman parte del sector aéreo del Ecuador en relación con el manejo de los riesgos en las tecnologías de información.

- **Investigación exploratoria.** Este tipo de estudios se “efectúa cuando el objetivo es examinar un tema o problema de investigación poco estudiado y del cual se tienen muchas dudas o no se ha abordado antes” (Morán & Alvarado, 2018, p. 8), por ende, el estudio a realizarse es único en su investigación pues hasta el momento no se han realizado trabajos similares que cumplan con una perspectiva en el manejo de los riesgos de información aplicando la Norma ISO / IEC 27000 en las empresas del sector aéreo del Ecuador.

Es decir, el actual estudio por una parte es descriptiva al establecer las principales características de las entidades del sector aéreo, agregando además que es una investigación exploratoria ya que no se han desarrollado estudios en los que se analicen y se efectúe un proceso de implementación sobre los riesgos de información utilizando la Norma ISO / IEC 27000.

2.1.3. Enfoque de investigación

La actual investigación se enmarca desde un enfoque cuantitativo el cual consiste en utilizar “recolección de datos para probar hipótesis, con base en la medición numérica y el análisis estadístico, para establecer patrones de comportamiento y probar teorías” (Hernández Sampieri, Fernández, & Baptista, 2016, p. 4).

Por lo tanto, al obtener los datos sobre el manejo de los riesgos de información en las empresas del sector aéreo del Ecuador se permite realizar un análisis cuantitativo realizando el cálculo de porcentajes como medición numérica de cada grupo de datos recopilados, en base a este conjunto de resultados obtenidos se estaría reconociendo la realidad sobre la información y su tratamiento que existe ante los riesgos inherentes en las organizaciones que se analizan.

2.2. Métodos de investigación

Al efectuar el estudio se aplica el método inductivo – deductivo el cual se fundamenta en la lógica estudiando hechos particulares y luego obteniendo conclusiones relevantes, para que luego de ello en base a los comportamientos identificados se permite establecer soluciones individuales, por lo que en el primer caso se parte de lo particular a lo general y de ahí se enfoca de lo general a lo particular (Bernal, 2016, p. 60).

De acuerdo a la conceptualización anterior, el presente estudio aplica el método inductivo al identificar las causas que conllevan al problema principal que consiste en el Inadecuado manejo de los riesgos en la seguridad de las tecnologías de información del sector aéreo del Ecuador.

Así mismo, considerando el problema identificado se plantean interrogantes que ayudan a determinar la situación actual en el manejo de los riesgos cuyos resultados obtenidos se interpretarán como conclusiones del estudio y con ello establecer las diferentes alternativas de solución enfocándose hacia la aplicación de la Norma ISO / IEC 27000, por lo que ante el cumplimiento de estos eventos consecuentes se establece el método deductivo el mismo que se enfoca desde lo general hacia lo particular.

2.3. Unidad de análisis, población y muestra

2.3.1. Unidad de análisis

Se denomina como unidad de análisis al “conjunto o grupo de personas, empresas, instituciones o cosas que son sujetos de estudio de la investigación que se realiza” (Bernal, 2016, p. 116).

Por ende, en base a ello en el desarrollo del presente estudio la unidad de análisis se conforma por las empresas de aerolíneas que se constituyen como parte del sector aéreo del Ecuador.

2.3.2. Población y muestra

La población se refiere al “conjunto completo de todos los objetos que interesan a un investigador” (Newbold, Carlson, & Thorne, 2017, p. 3), por lo que de acuerdo a esta definición el universo poblacional se determina por 25 empresas de aerolíneas que se dedican al transporte aéreo en el país, por lo que al ser una población pequeña no será necesario realizar el cálculo de la muestra de tal manera que el estudio se estaría realizando a la totalidad del universo poblacional.

2.4. Variables de investigación, Operacionalización

Tabla 3. Variables de estudio

Tipo de variables	**Denominación**
Variable dependiente:	Gestión de riesgos de información
Variable independiente:	Seguridad en las tecnologías de la información
Hipótesis:	
La gestión de riesgos influye en el mejoramiento de la seguridad en las tecnologías de la información del sector aéreo del Ecuador	

Fuente: *Investigación propia*
Elaborado por: *La autora*

2.4.1. Operacionalización de Variables

La Operacionalización se realiza de acuerdo a cada una de las preguntas identificadas, estableciendo las correspondientes dimensiones, indicadores, ítems, técnicas e instrumentos para cada uno de ellos:

Tabla 4. Variable Dependiente: Gestión de Riesgos de Información

Dimensiones	**Indicador**	**Items**	**Técnica / instrumento**
	Margen errores humanos	¿Se han registrado pérdidas de datos que han sido causados por errores humanos?	Encuesta / cuestionario

Riesgo operacional	Margen de fallas electrónicas	¿Han presentado fallas electrónicas en su empresa que conlleven a la pérdida de información?	Encuesta / cuestionario
	Margen desperfectos en equipos electrónicos	¿Han sufrido algún desperfecto los equipos electrónicos de su empresa?	Encuesta / cuestionario
Riesgo de reputación	Margen de virus informáticos	¿Han sido afectados por virus informáticos que incidan en la reputación de su empresa?	Encuesta / cuestionario
	Margen de publicidad negativa	¿Ha sido involucrada su empresa en publicidad negativa que afecte su integridad?	Encuesta / cuestionario
	Margen de pérdida de información confidencial	¿Ha existido robo de información confidencial en su empresa durante los últimos doce meses?	Encuesta / cuestionario

Fuente: *Investigación propia*
Elaborado por: *La autora*

Tabla 5. Variable Independiente: Seguridad en las Tecnologías de la Información

Dimensiones	Indicador	Items	Técnica / instrumento
Seguridad en hardware	Margen de defectos en hardware	¿Se han presentado problemas en la pantalla, teclado o CPU de las computadoras de la empresa?	Encuesta / cuestionario
	Margen de buen estado de hardware	¿Se encuentran en mal estado las computadoras de empresa?	Encuesta / cuestionario
Seguridad en software	Margen de actualización de software	¿Están desactualizadas las computadoras de empresa?	Encuesta / cuestionario
	Margen de confidencialidad en seguridad de datos	¿Se han encontrado programas innecesarios que afectan la confidencialidad de la seguridad de datos?	Encuesta / cuestionario
Seguridad en redes	Margen de transmisión virtuales de datos	¿Se han generado problemas en la redes de internet durante la transmisión de los datos?	Encuesta / cuestionario
	Margen de almacenamiento y seguridad	¿Son confiables las fuentes de almacenamiento virtuales en la seguridad de la información?	Encuesta / cuestionario

Fuente: *Investigación propia*
Elaborado por: *La autora*

2.5. Fuentes, técnicas e instrumentos de investigación para la recolección de información

Las fuentes primarias o secundarias de información que se utilizan en el presente estudio se encuentran las siguientes:

- **Fuentes primarias.** Son aquellas que se tienen una relación directa con el objeto de investigación, entre la cual se encuentra la encuesta que se aplica a los dueños o administradores de las empresas del sector aéreo del Ecuador.
- **Fuentes secundarias.** Se caracterizan por aquellos que no tienen relación directa con el estudio a realizarse, en los que se incluyen libros, periódicos, revistas o páginas web relacionados con la gestión del riesgo, la seguridad de la información y la Norma ISO / IEC 27000.

Considerando lo que se ha explicado con anterioridad se determinan en la tabla siguiente las fuentes, técnicas e instrumentos de información:

Tabla 6. Técnicas e instrumentos de información

Fuente	Técnicas	Instrumentos
Fuentes primarias	Encuesta	Cuestionario de la encuesta
Fuentes secundarias	Libros	Gestión de Riesgos, Seguridad de la Información, Normas ISO / IEC 27000
	Periódicos	El Comercio, El Universo
	Revistas	PC World, IT Ahora, PC Magazine
	Páginas web	www.isotools.org

Fuente: *Investigación propia*
Elaborado por: *La autora*

2.6. Tratamiento de información

Para realizar el tratamiento de información es necesario utilizar software como Microsoft Excel y el software estadístico IBM SPSS (Statistical Product and Service Solutions), en los cuales se utilizarán las correspondientes tabulaciones de los datos que se han recopilado, para que luego de ello se realice las tablas y Gráficos estadísticas.

CAPÍTULO III

RESULTADOS Y DISCUSIÓN

3.1. Análisis de la situación actual

Al desarrollar el presente capítulo de la investigación, se analiza la gestión del riesgo y la seguridad de la información en las empresas aéreas del Ecuador, por lo cual se está enfocándose en el desarrollo del objetivo 2 en el estudio realizado, siendo fundamental iniciar con un análisis univariado en el que se interpretan las variables por separado, mientras que en el análisis bivariado se evalúa el riesgo con la seguridad de la información permitiendo obtener una correlación entre las variables de investigación.

3.1.1. Análisis univariado

El análisis univariado corresponde a la interpretación de cada uno de los resultados que se presenten de forma individual, de tal manera en un inicio el conjunto de valores se evalúen por separado sin que se realice algún tipo de cruce entre los datos de riesgos de información y la seguridad en las tecnologías que se denominan como variables independiente y dependiente respectivamente.

Entre los resultados obtenidos se interpretan cifras de doce preguntas de investigación en las que se analizan cada una de las dimensiones que forman parte de la Operacionalización de variables, siendo necesario también analizar el tiempo en que se ha creado las empresas de aerolíneas permitiéndose determinar así conclusiones conjuntas por todas las compañías que han incidido en la obtención de los resultados. Es decir, que tanto los riesgos de información y la seguridad en las tecnologías de las empresas de aerolíneas se requiere determinar conclusiones específicas por separado sin que exista una comparación entre ambas, esto se aplica con la finalidad de identificar las dimensiones que más influyen dentro de las variables que se presenten

3.1.1.1. Tabulación y análisis de datos

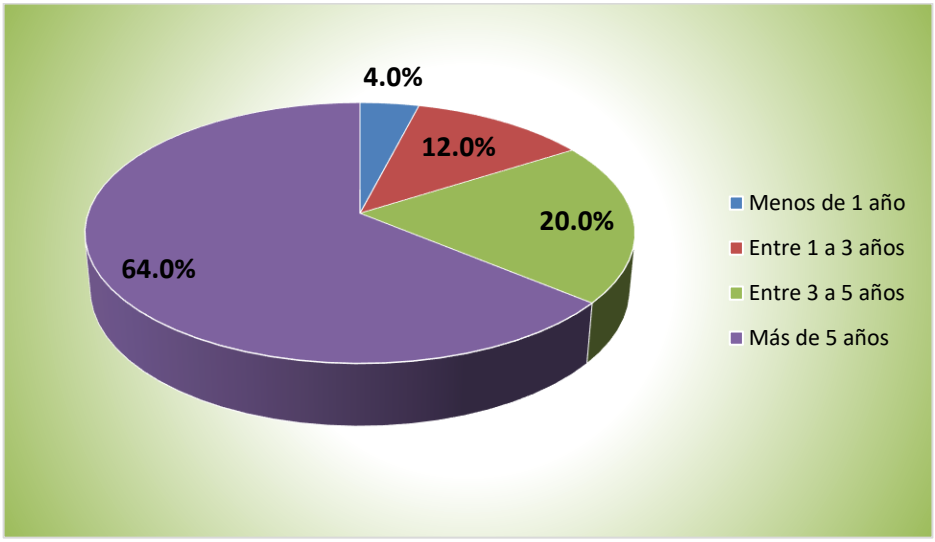
Edad

Tabla 7. Edad

ALTERNATIVAS	TABULACIÓN	PORCENTAJE (%)
Menos de 1 año	1	4,0%
Entre 1 a 3 años	3	12,0%
Entre 3 a 5 años	5	20,0%
Más de 5 años	16	64,0%
TOTAL	**25**	**100%**

Fuente: *Investigación propia*
Elaborado por: *La autora*

Gráfico 3. Edad



Fuente: *Investigación propia*
Elaborado por: *La autora*

Análisis e interpretación:

En base a los resultados esperados, se observa que en la Gráfico y tabla anterior se destaca que el 64,0% de las empresas encuestadas se encuentran en el mercado desde hace más de cinco años, agregando también que el 20,0% se encuentran entre tres a cinco años, es decir que al menos cuatro de cada cinco empresas de transporte aéreo mantienen una mayor presencia en el mercado.

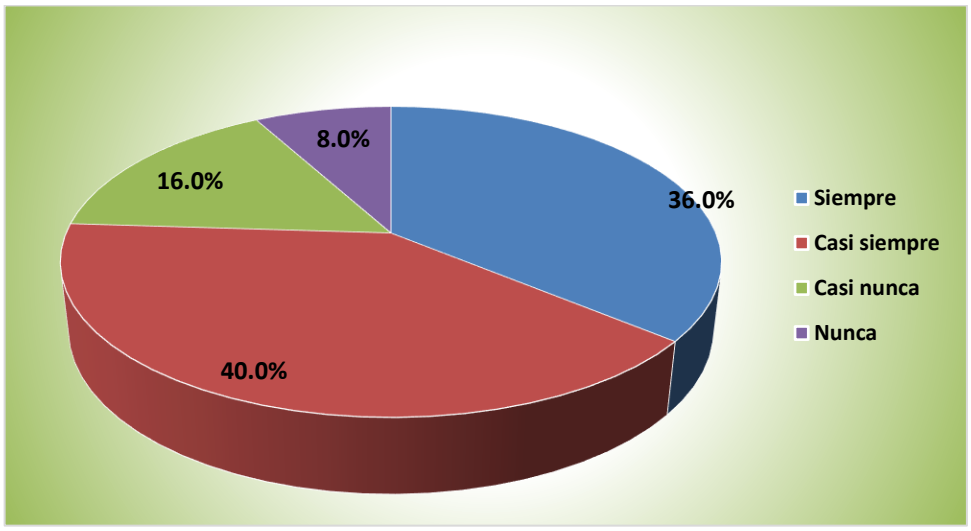
Pregunta 1. ¿Se han registrado pérdidas de datos que han sido causados por errores humanos?

Tabla 8. Pérdida de datos por errores humanos

ALTERNATIVAS	TABULACIÓN	PORCENTAJE (%)
Siempre	9	36,0%
Casi siempre	10	40,0%
Casi nunca	4	16,0%
Nunca	2	8,0%
TOTAL	**25**	**100,0%**

Fuente: *Investigación propia*
Elaborado por: *La autora*

Gráfico 4. Pérdida de datos por errores humanos



Fuente: *Investigación propia*
Elaborado por: *La autora*

Análisis e interpretación:

En la tabla anterior se visualiza que el 76,0% de las aerolíneas encuestadas reconocen que siempre y casi siempre han registrado pérdidas de datos ocasionadas por errores humanos, mientras que el 24,0% restante establece que nunca y casi nunca se han presentado este tipo de inconvenientes. De modo que estas cifras demuestran que casi cuatro de cada cinco empresas presentan pérdidas de información ocasionadas por los colaboradores y directivos que pertenecen a cada una de estas entidades.

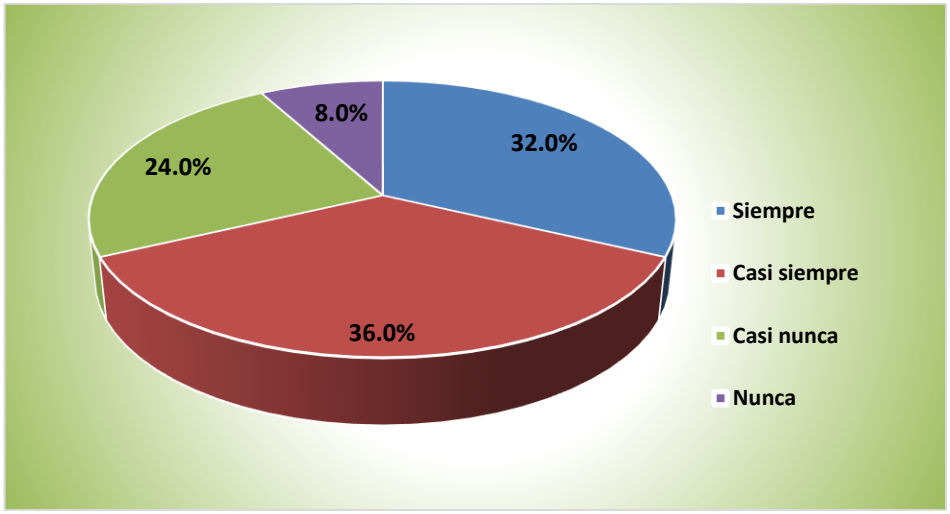
Pregunta 2. ¿Han presentado fallas electrónicas en su empresa que conlleven a la pérdida de información?

Tabla 9. Fallas electrónicas ante la pérdida de información

ALTERNATIVAS	TABULACIÓN	PORCENTAJE (%)
Siempre	8	32,0%
Casi siempre	9	36,0%
Casi nunca	6	24,0%
Nunca	2	8,0%
TOTAL	**25**	**100,0%**

Fuente: *Investigación propia*
Elaborado por: *La autora*

Gráfico 5. Fallas electrónicas ante la pérdida de información



Fuente: *Investigación propia*
Elaborado por: *La autora*

Análisis e interpretación:

De acuerdo a los resultados obtenidos, se tiene que siempre y casi siempre que corresponde al 68,0% de los empresas encuestadas han presentado fallas electrónicas lo que conlleva a la pérdida de información, mientras que el 32,0% restante no se han identificado este tipo de inconvenientes. Esto significa que tres de cada cinco aerolíneas evidencian pérdida de datos debido a errores electrónicos que se han presentado.

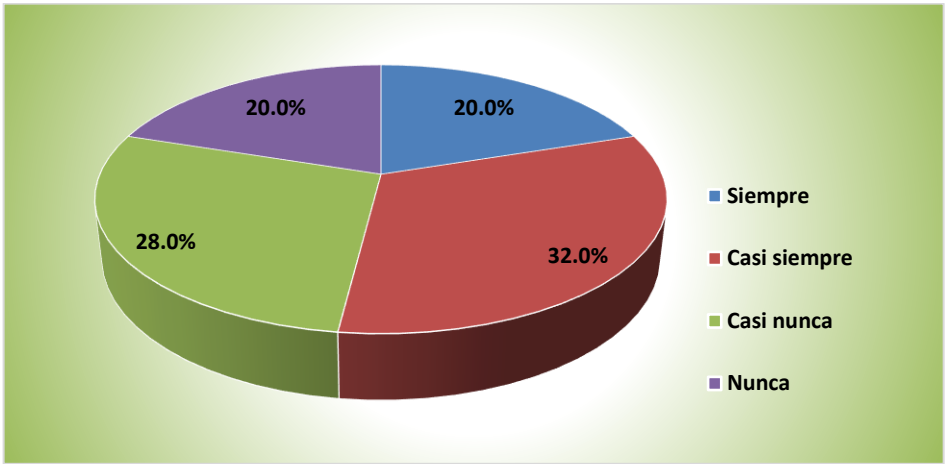
Pregunta 3. ¿Han sufrido algún desperfecto los equipos electrónicos de su empresa?

Tabla 10. Desperfectos en los equipos electrónicos de la empresa

ALTERNATIVAS	TABULACIÓN	PORCENTAJE (%)
Siempre	5	20,0%
Casi siempre	8	32,0%
Casi nunca	7	28,0%
Nunca	5	20,0%
TOTAL	**25**	**100,0%**

Fuente: *Investigación propia*
Elaborado por: *La autora*

Gráfico 6. Desperfectos en los equipos electrónicos de la empresa



Fuente: *Investigación propia*
Elaborado por: *La autora*

Análisis e interpretación:

En base a los resultados, se determina que el 52,0% de las aerolíneas ha sufrido desperfectos en sus equipos electrónicos, por lo que el 28,0% responde que casi nunca y el 20,0% reconoce que nunca. De acuerdo a estas cifras se establece que la mitad de las empresas a las que se ha aplicado la investigación presenta imperfecciones en los equipos utilizados lo que genera inconvenientes en el desempeño de sus actividades, principalmente en el almacenamiento de información.

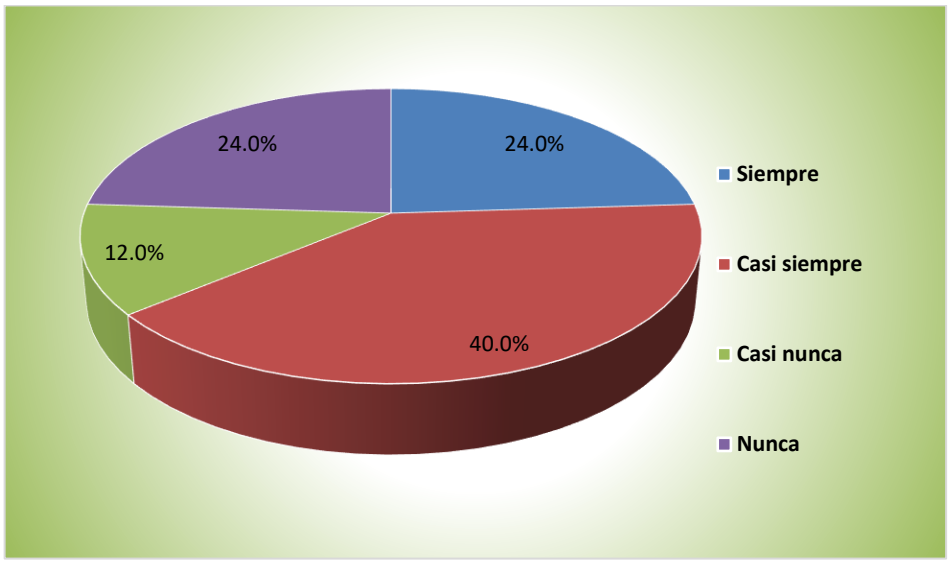
Pregunta 4. ¿Han sido afectados por virus informáticos que incidan en la reputación de su empresa?

Tabla 11. Incidencia de virus informáticos en la reputación de la empresa

ALTERNATIVAS	TABULACIÓN	PORCENTAJE (%)
Siempre	6	24,0%
Casi siempre	10	40,0%
Casi nunca	3	12,0%
Nunca	6	24,0%
TOTAL	**25**	**100,0%**

Fuente: *Investigación propia*
Elaborado por: *La autora*

Gráfico 7. Incidencia de virus informáticos en la reputación de la empresa



Fuente: *Investigación propia*
Elaborado por: *La autora*

Análisis e interpretación:

Luego de obtener los resultados, se identifica que el 64% de las empresas en estudio responden que siempre y casi siempre han sido afectados por virus informáticos, por lo que la diferencia restante que se ubica en un 36,0% informa que nunca y casi nunca se han presentado estos inconvenientes. Por ende, en base a ello se determina que más de la mitad de aerolíneas se evidencian ataque informáticos que d alguna manera ha ocasionado la pérdida de datos y con ello otorgado una cierta dificultad en el posicionamiento de la imagen de la empresa.

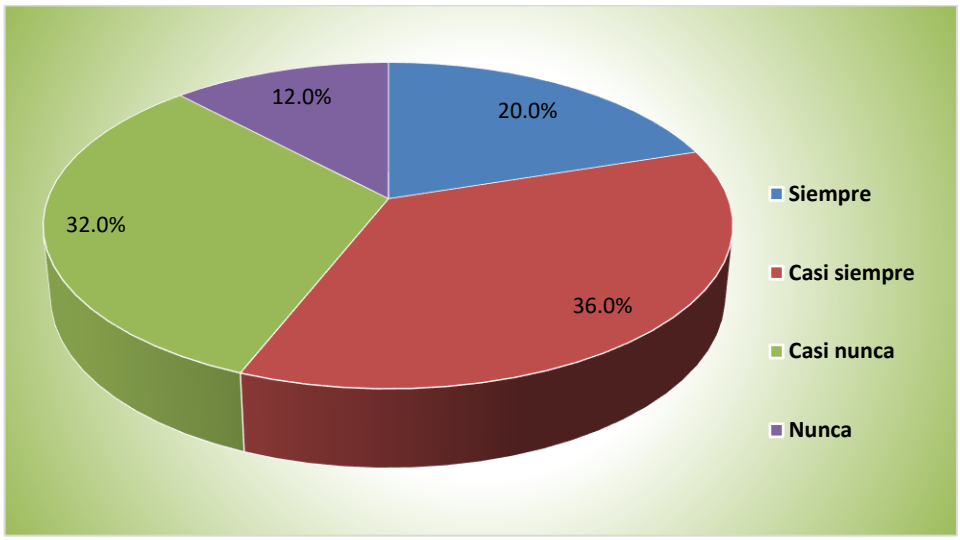
Pregunta 5. ¿Ha sido involucrada su empresa en publicidad negativa que afecte su integridad?

Tabla 12. Publicidad negativa en la empresa

ALTERNATIVAS	TABULACIÓN	PORCENTAJE (%)
Siempre	5	20,0%
Casi siempre	9	36,0%
Casi nunca	8	32,0%
Nunca	3	12,0%
TOTAL	**25**	**100,0%**

Fuente: *Investigación propia*
Elaborado por: *La autora*

Gráfico 8. Publicidad negativa en la empresa



Fuente: *Investigación propia*
Elaborado por: *La autora*

Análisis e interpretación:

En la tabla anterior se tiene que 56,0% de las entidades que forman parte de la presente investigación han sido afectadas por publicidad negativa por las actividades de su negocio, mientras que el 44,0% restante no se han reflejado estos conflictos en sus instalaciones, Con ello, se reconoce que más de la mitad de las aerolíneas ha identificado campañas de promoción y publicidad que inciden de manera negativa en la imagen de su empresa, por lo que los expertos de cada empresa han tomado medidas para resguardar con mayor seguridad los datos confidenciales de su negocio.

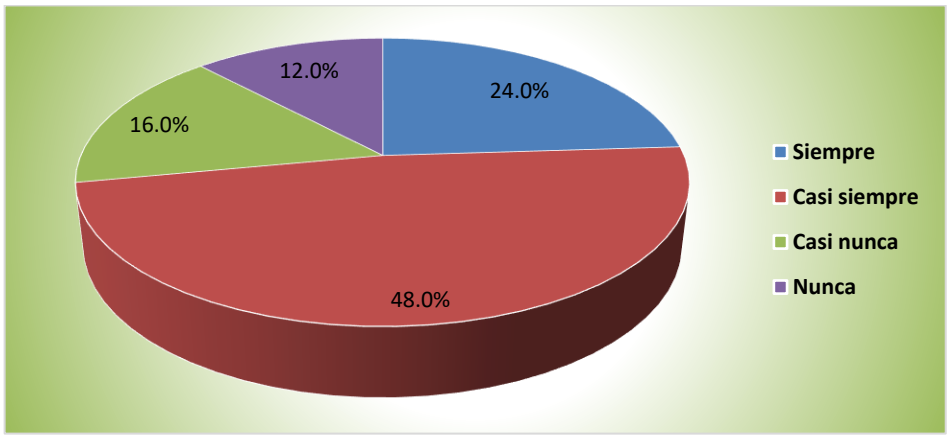
Pregunta 6. ¿Ha existido robo de información confidencial en su empresa durante los últimos doce meses?

Tabla 13. Problemas de robo de información confidencial

ALTERNATIVAS	TABULACIÓN	PORCENTAJE (%)
Siempre	6	24,0%
Casi siempre	12	48,0%
Casi nunca	4	16,0%
Nunca	3	12,0%
TOTAL	**25**	**100,0%**

Fuente: *Investigación propia*
Elaborado por: *La autora*

Gráfico 9. Robo de información confidencial



Fuente: *Investigación propia*
Elaborado por: *La autora*

Análisis e interpretación:

En la Gráfico y tabla anterior, se tiene que el 48,0% de las aerolíneas encuestadas contestan que casi siempre y el 24,0% informan que siempre ha existido robo confidencial de datos, mientras que el 18,0% restante menciona que nunca y casi nunca han existido este tipo de problemática. Con ello se estaría determinando que aproximadamente siete de cada diez compañías evidencian fallos en la seguridad en el almacenamiento de información a pesar de se han buscado implementar medidas correctivas que reducir la perdida de información.

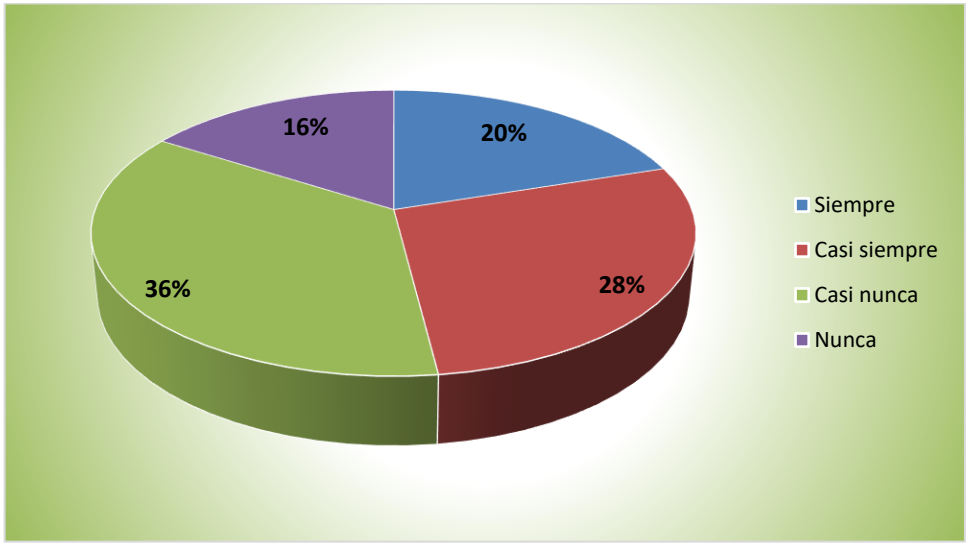
Pregunta 7. ¿Se han presentado problemas en la pantalla, teclado o CPU de las computadoras de la empresa?

Tabla 14. Problema en la pantalla, CPY o teclado de la computadora

ALTERNATIVAS	TABULACIÓN	PORCENTAJE (%)
Siempre	5	20,0%
Casi siempre	7	28,0%
Casi nunca	9	36,0%
Nunca	4	16,0%
TOTAL	**25**	**100,0%**

Fuente: *Investigación propia*
Elaborado por: *La autora*

Gráfico 10. Problema en la pantalla, CPY o teclado de la computadora



Fuente: *Investigación propia*
Elaborado por: *La autora*

Análisis e interpretación:

En los resultados que se reflejan en la tabla y Gráfico anterior, se observa que el 48,0% de las entidades de aerolíneas reconocen que el hardware de sus equipos de computación como la pantalla, el teclado o el CPU han presentado fallos en su funcionamiento, mientras que el 52,0% restante que corresponde para casi nunca y nunca mencionan que no se presentan esta problemática. Por lo tanto, más de la mitad de computadores de aerolíneas se encuentran en un estado aceptable para su buen funcionamiento, aunque la otra mitad restante deberá adquirir nuevos equipos para el resguardo de información.

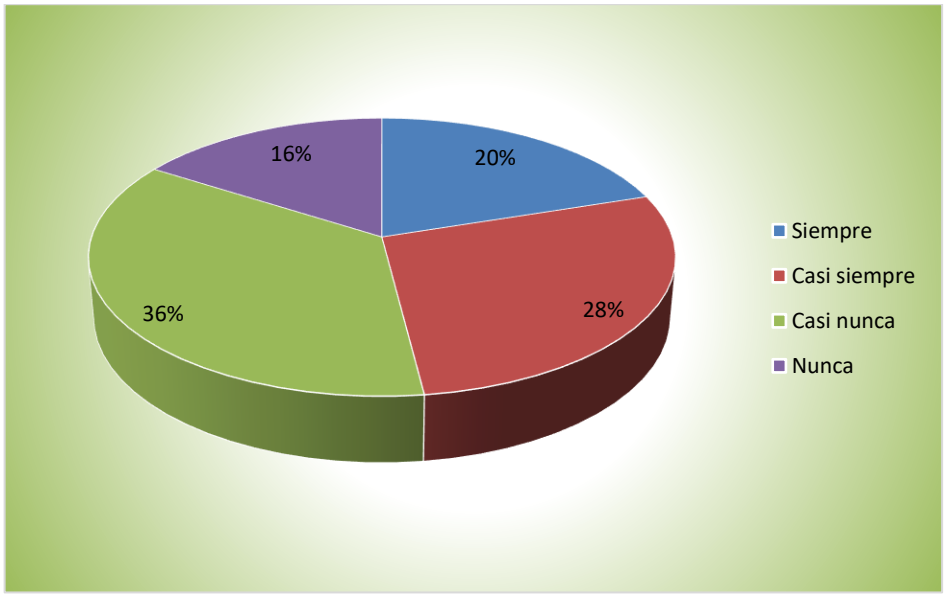
Pregunta 8. ¿Se encuentran en mal estado las computadoras de empresa?

Tabla 15. Mal estado de las computadoras de la empresa

ALTERNATIVAS	TABULACIÓN	PORCENTAJE (%)
Siempre	5	20,0%
Casi siempre	7	28,0%
Casi nunca	9	36,0%
Nunca	4	16,0%
TOTAL	**25**	**100,0%**

Fuente: *Investigación propia*
Elaborado por: *La autora*

Gráfico 11. Mal estado de las computadoras de la empresa



Fuente: *Investigación propia*
Elaborado por: *La autora*

Análisis e interpretación:

Tomando en cuenta los resultados que se visualizan en la tabla y Gráfico anterior, se tiene que el 52,0% de las compañías encuestadas destacan que sus computadoras no se encuentran en mal estado, lo que significa que el otro 48,0% para los negocios que contestaron que siempre y casi siempre sus equipos de cómputo presentan imperfecciones. De acuerdo a estas cifras se entiende que la mitad de aerolíneas no presentan inconvenientes en los equipos de almacenamiento utilizados, mientras que la otra mitad reconocen la existencia de este problema.

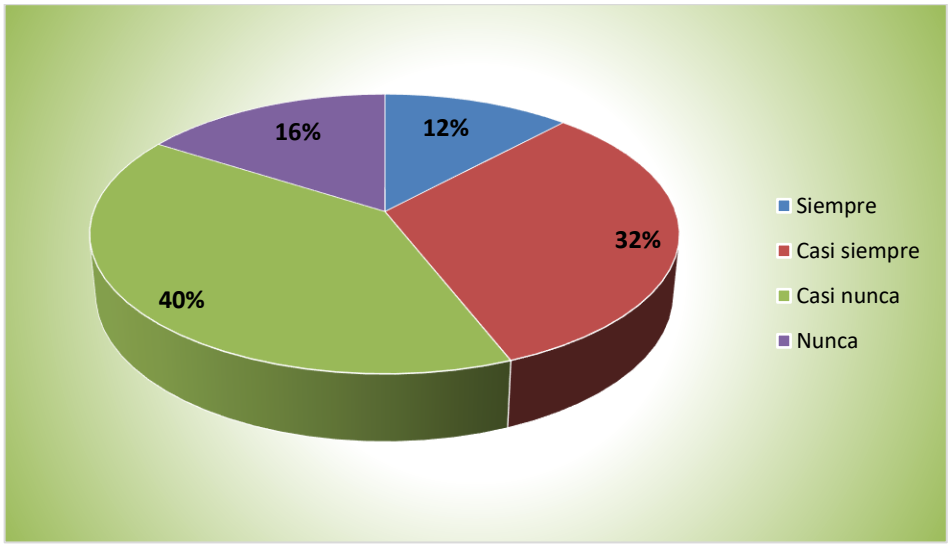
Pregunta 9. ¿Están desactualizadas las computadoras de empresa?

Tabla 16. Desactualización de las computadoras de la empresa

ALTERNATIVAS	TABULACIÓN	PORCENTAJE (%)
Siempre	3	12,0%
Casi siempre	8	32,0%
Casi nunca	10	40,0%
Nunca	4	16,0%
TOTAL	**25**	**100,0%**

Fuente: *Investigación propia*
Elaborado por: *La autora*

Gráfico 12. Desactualización de las computadoras de la empresa



Fuente: *Investigación propia*
Elaborado por: *La autora*

Análisis e interpretación:

Entre los resultados identificados los cuales se observan en la tabla anterior se determina que el 44,0% de las empresas de transporte aéreo responden que siempre y casi siempre sus computadoras están desactualizadas, lo que significa que el otro 56,0% restante menciona que nunca y casi nunca presentan este problema puesto que eventualmente realizan una actualización de todo el sistema operativo de la empresa, con ello se estaría evidenciando que más de la mitad de aerolíneas no aquejan problemas de desactualización de datos.

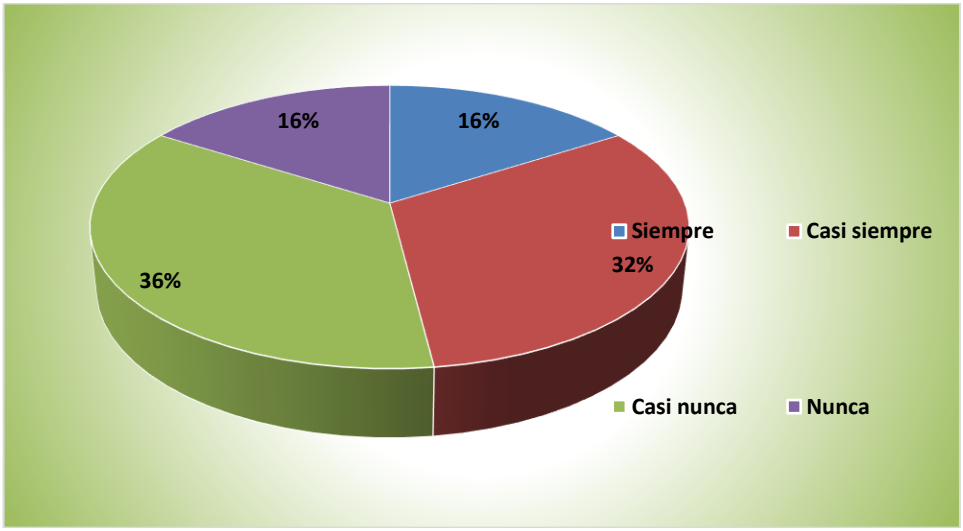
Pregunta 10. ¿Se han encontrado programas innecesarios que afectan la confidencialidad de la seguridad de datos?

Tabla 17. Baja seguridad de datos por programas innecesarios

ALTERNATIVAS	TABULACIÓN	PORCENTAJE (%)
Siempre	4	16,0%
Casi siempre	8	32,0%
Casi nunca	9	36,0%
Nunca	4	16,0%
TOTAL	**25**	**100,0%**

Fuente: *Investigación propia*
Elaborado por: *La autora*

Gráfico 13. Baja seguridad de datos por programas innecesarios



Fuente: *Investigación propia*
Elaborado por: *La autora*

Análisis e interpretación:

En la Gráfico y tabla anterior, se destaca que el 56,0% de las empresas responden que nunca y casi nunca han encontrado programas innecesarios que alteren la confidencialidad de información, lo que se demuestra que el 48,0% menciona que siempre y casi siempre identifican esta problemática existente. Por ende, más de la mitad de las compañías de aerolíneas reconocen que se han encontrado sistemas informáticos en sus computadores que no tienen relación con las actividades de la empresa, pero que no representan peligro alguno que ocasione la pérdida de información.

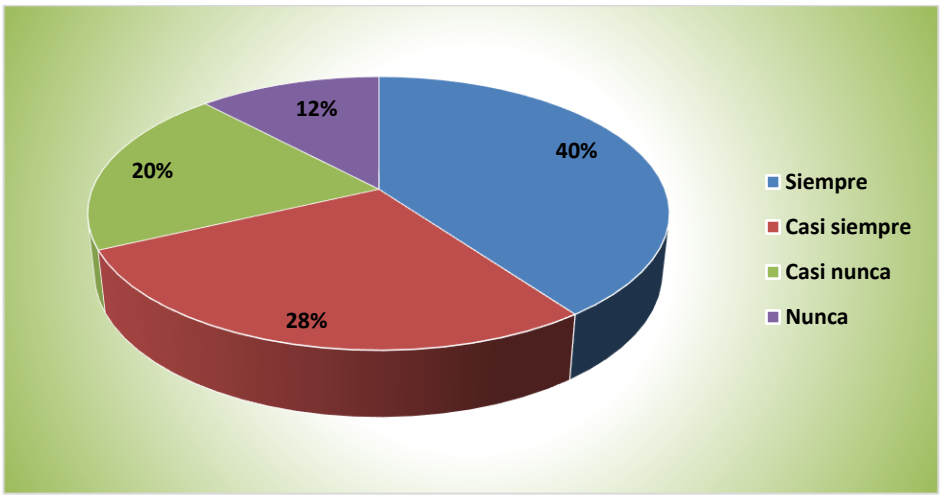
Pregunta 11. ¿Se han generado problemas en la redes de internet durante la transmisión de los datos?

Tabla 18. Problemas en las redes de Internet

ALTERNATIVAS	TABULACIÓN	PORCENTAJE (%)
Siempre	10	40,0%
Casi siempre	7	28,0%
Casi nunca	5	20,0%
Nunca	3	12,0%
TOTAL	**25**	**100,0%**

Fuente: *Investigación propia*
Elaborado por: *La autora*

Gráfico 14. Problemas en las redes de internet



Fuente: *Investigación propia*
Elaborado por: *La autora*

Análisis e interpretación:

En la Gráfico y tabla que se observa anteriormente, se destaca que el 68,0% de las empresas encuestados reconocen que existen problemas en las redes de internet durante la trasmisión de datos, lo que significa que el 32,0% restante no se evidenciado este tipo de fallas al mantener una comunicación digital y almacenamiento de información. De esta forma, se detecta que el problema es aún mayor pues se interpreta que al menos siete de cada diez aerolíneas presentan fallos en las redes de conexión virtual, lo que puede ser el indicio de una posible pérdida de datos en el futuro incrementando así el riesgo ante la pérdida de posicionamiento de imagen de marca de las aerolíneas.

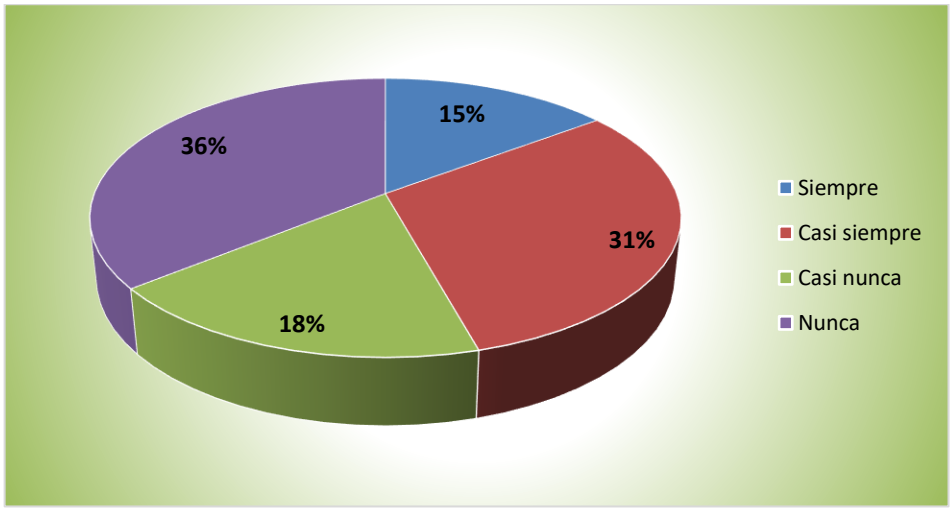
Pregunta 12. ¿Siente desconfianza en las fuentes de almacenamiento virtuales en la seguridad de la información?

Tabla 19. Desconfianza en las fuentes de almacenamiento de información

ALTERNATIVAS	TABULACIÓN	PORCENTAJE (%)
Siempre	2	14,8%
Casi siempre	8	30,9%
Casi nunca	9	18,5%
Nunca	6	35,8%
TOTAL	**25**	**100,0%**

Fuente: *Investigación propia*
Elaborado por: *La autora*

Gráfico 15. Desconfianza en las fuentes de almacenamiento de información



Fuente: *Investigación propia*
Elaborado por: *La autora*

Análisis e interpretación:

En esta interrogante, se establece que el 54,3% de las compañías participantes informan que nunca y casi nunca sienten desconfianza en las fuentes de almacenamiento virtuales, lo cual demuestra que el 45,7% restante contestan que siempre y casi siempre tienen una falta de confianza al almacenar los datos de la empresa. Con ello significaría que la mitad de aerolíneas disponen de dispositivos adecuados con los que se garantice la seguridad de información generando una mayor confianza hacia ellos, pues la otra mitad restante se requiere que los dispositivos utilizados sean actualizados constantemente.

3.2. Análisis comparativo, evolución, tendencias y perspectivas

3.2.1. Análisis bivariado

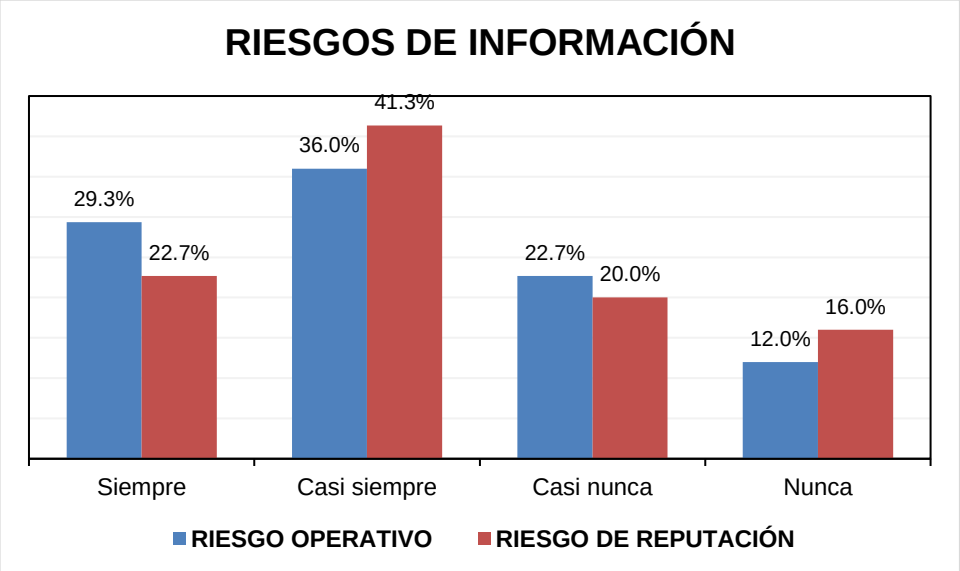
El análisis bivariado se determina en función de las variables identificadas agrupándolas de acuerdo al tipo de dimensión a la que pertenezcan, favoreciendo a la interpretación de resultados comparativos entre los riesgos de información y la seguridad en las tecnologías que se han identificado como variable independiente y dependiente respectivamente.

3.2.1.1. Comparación de variables similares

Dada las variables que se han identificado a lo largo del presente trabajo de investigación, resulta necesario efectuar un comparativo de las dimensiones que formen parte de una misma variable estableciendo sus porcentajes para todos ellos.

Por lo tanto, la variable independiente corresponde a los riesgos de información, entre los cuales se tiene tanto los riesgos operativos y de reputación, los mismos que se identifican sus porcentajes en la Gráfico siguiente de acuerdo las cuatro alternativas pre señaladas como son siempre, casi siempre, casi nunca y nunca:

Gráfico 16. Riesgos de información

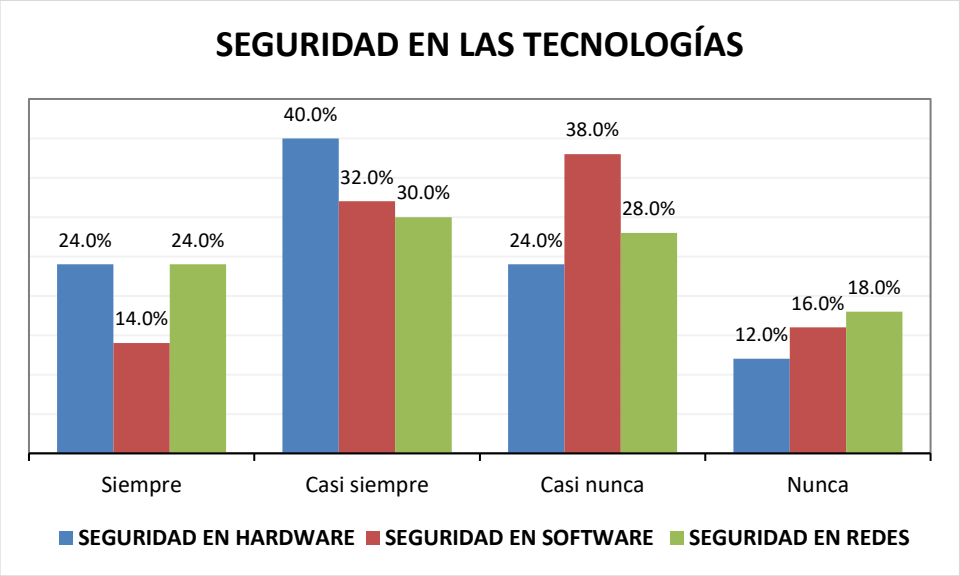


Fuente: *Investigación propia*
Elaborado por: *La autora*

En la Gráfico anterior se conoce que el riesgo de reputación entre sus alternativas siempre y casi siempre suman un 64,0% mientras que para el riesgo operativo es de 65,3% lo que se estaría demostrando que en ambos casos se evidencia una mayor incertidumbre ante la posibilidad de una pérdida de información en las empresas de aerolíneas, pues las alternativas nunca y casi nunca tienen un total de 34,7% y 36,0% para el riesgo operativo y riesgo de reputación respectivamente.

Así mismo que en cuanto a la variable dependiente que corresponde a la seguridad en las tecnologías tanto se han agrupado sus dimensiones entre las que se encuentran la seguridad en hardware, en software y en redes digitales, cuyos resultados obtenidos se determinan en porcentajes:

Gráfico 17. Seguridad en las tecnologías



Fuente: *Investigación propia*
Elaborado por: *La autora*

En base a la Gráfico anterior se destaca que en cuanto a las alternativas siempre y casi siempre las empresas de aerolíneas en total suman un 64,0% para la seguridad en hardware, seguido de la seguridad en redes con un 54,0% y con 46,0% para la seguridad en software, por ende en base a estos resultados las compañías que han sido objeto de estudio se identifican mayores problemas en la pantalla, el teclado o el CPU que corresponden al hardware de los equipos de computación utilizados, no obstante, las fallos en la conexión de internet también han generado inconvenientes en el momento de la transmisión de los datos.

En definitiva, al analizar las dimensiones de la variables de investigación se reconoce que el riesgo operativo y el riesgo de reputación mantienen similar representatividad en las compañías de aerolíneas, agregando también que los conflictos ocasionados en las redes de comunicación virtual y la falta de mantenimiento en el hardware de los computadores son dos problemas evidentes que ocasionan inseguridad en el almacenamiento de datos.

3.2.1.2. Comparación correlacional

Para realizar un análisis comparativo entre la variable dependiente e independiente es necesario recurrir a la correlación de Pearson mediante las cuales se otorgan comparativos por dimensiones identificadas, dando lugar a diferentes interpretaciones según los resultados que se presenten:

Tabla 20. Rangos de correlación de Pearson

Tipo	Coeficiente	Interpretación
Positiva	r = 1	Correlación perfecta
	0,8 < r < 1,0	Muy alta
	0,6 < r < 0,8	Alta
	0,4 < r < 0,6	Moderada
	0,2 < r < 0,4	Baja
	0,0 < r < 0,2	Muy baja
Indiferente	r = 0	Nula
Negativa	0,0 < r < -0,2	Muy baja
	-0,2 < r < -0,4	Baja
	-0,4 < r < -0,6	Moderada
	-0,6 < r < -0,8	Alta
	-0,8 < r < -1,0	Muy alta
	r = -1	Correlación perfecta

Fuente: *Investigación propia*
Elaborado por: *La autora*

Tabla 21. Correlación de las variables

Correlaciones

		VI_RIESGO_OPERACIONAL	VI_RIESGO_DE_REPUTACIÓN	VD_SEGURIDAD_EN_HARDWARE	VD_SEGURIDAD_EN_SOFTWARE	VD_SEGURIDAD_EN_REDES
VI_RIESGO_OPERACIONAL	Correlación de Pearson	1	,640**	,368	,305	,367
	Sig. (bilateral)		,001	,071	,138	,071
	N	25	25	25	25	25
VI_RIESGO_DE_REPUTACIÓN	Correlación de Pearson	,640**	1	,622**	,476*	,485*
	Sig. (bilateral)	,001		,001	,016	,014
	N	25	25	25	25	25
VD_SEGURIDAD_EN_HARDWARE	Correlación de Pearson	,368	,622**	1	,618**	,537**
	Sig. (bilateral)	,071	,001		,001	,006
	N	25	25	25	25	25
VD_SEGURIDAD_EN_SOFTWARE	Correlación de Pearson	,305	,476*	,618**	1	,567**
	Sig. (bilateral)	,138	,016	,001		,003
	N	25	25	25	25	25
VD_SEGURIDAD_EN_REDES	Correlación de Pearson	,367	,485*	,537**	,567**	1
	Sig. (bilateral)	,071	,014	,006	,003	
	N	25	25	25	25	25

Fuente: *Investigación propia*
Elaborado por: *La autora*
***. La correlación es significativa en el nivel 0,01 (2 colas).*
**. La correlación es significativa en el nivel 0,05 (2 colas).*

Para el desarrollo del análisis correlacional ha sido necesario establecer un nivel de significancia de 0,05 siendo necesario determinar también las dimensiones que pertenecen a la variable dependiente como independiente, reconociendo que el riesgo de reputación mantiene una correlación positiva moderada de 0,622; de 0,476 y de 0,485 para las variables dependientes como son seguridad en hardware, software y en redes de internet respectivamente.

3.2.1.3. Comprobación de hipótesis

Para realizar la comprobación de la relación entre las variables de estudio, se requiere identificar la hipótesis nula (H0) e hipótesis alternativa (H1) las cuales son:

H0 = Los riesgos de información no influye en el mejoramiento de la seguridad en las tecnologías de la información del sector aéreo del Ecuador

H1 = Los riesgos de información influye en el mejoramiento de la seguridad en las tecnologías de la información del sector aéreo del Ecuador

Se añade además como estadístico de prueba se ha decidido utilizar la correlación de Pearson y un nivel de significancia de 0,01 por ser el más preciso ante la determinación de los niveles de probabilidad, es por ello que al agrupar las dimensiones de la variable dependiente e independiente se obtienen los siguientes resultados:

Tabla 22. Correlación entre gestión riesgo y seguridad tecnología

Correlaciones

		VII_GESTION_RIESGO_INFORMACION	VDD_SEGURIDAD_TECNOLOGIA_INFORMACIÓN
VII_GESTION_RIESGO_INFORMACION	Correlación de Pearson	1	,654**
	Sig. (bilateral)		,000
	N	25	25
VDD_SEGURIDAD_TECNOLOGIA_INFORMACIÓN	Correlación de Pearson	,654**	1
	Sig. (bilateral)	,000	
	N	25	25

**. La correlación es significativa en el nivel 0,01 (2 colas).

Fuente: *Investigación propia*
Elaborado por: *La autora*

Al tener una probabilidad de 0,000 se determina que este valor es inferior al 0,01 (0,000 < 0,01), por lo que se interpreta que se rechaza la hipótesis nula y se acepta la hipótesis alternativa, es decir, los riesgos de información influyen en el mejoramiento de la seguridad en las tecnologías de la información del sector aéreo del Ecuador

Nótese también que existe una correlación positiva alta entre ambas variables de investigación pues el coeficiente es de 0,654, lo que significa que los riesgos de información que existen en las compañías de aerolíneas influyen directamente en la seguridad de las tecnologías utilizadas, siendo fundamental proponer un modelo de gestión con el que permita mejorar la seguridad en los dispositivos electrónicos para el almacenamiento de información.

3.3. Presentación de resultados y discusión

En los resultados obtenidos se destaca que aproximadamente un 76,0% de las empresas de aerolíneas han registrado pérdidas de datos en algún momento que han sido causados por errores humanos, agregando también que el 64,0% de los negocios han sido afectados por virus informáticos, con ello se demuestra que más de la mitad de este tipo de compañías presentan problemas en el manejo de los riesgos para el tratamiento de la información, no obstante, en el trabajo realizado por (Guerrero & Gómez, 2015) destaca que un escenario de riesgo tecnológico está dado por el mal funcionamiento en los sistemas de información pero que provee las herramientas necesarias para la medición de datos al interior de las organizaciones.

Así mismo, entre los resultados analizados se destaca que el 68,0% de las aerolíneas del país han reflejado inconvenientes en las redes virtuales de comunicación lo que ocasiona una alta inseguridad para el almacenamiento de datos, de la misma manera si se toma en consideración el trabajo desarrollado por los autores (Fernández, Sánchez, García, Toval, & Hernández, 2016) se identifica la importancia ante el resguardo de contraseñas informáticas, lo cual se reconoce que el 22,2% de los trabajadores en el ámbito laboral sanitario implementan Buenas Prácticas de Seguridad (BPS) para el adecuado almacenamiento de la información quienes son las personas mayores de 30 años con un 86,7% pues ellos consideren la creación de contraseñas más robustas

ante el tratamiento de información confidencial. Por ende, esto al final genera preocupación entre sus directivos ante la posible pérdida de imagen de marca de su compañía en el mercado el cual está relacionada con el riesgo de reputación, siendo indispensable identificar los fallos electrónicos que se origen en el tratamiento, transmisión y almacenamiento de datos.

En definitiva, la seguridad en hardware, software y de redes de internet se encuentran ampliamente relacionados con el riesgo de reputación de las empresas de aerolíneas puesto que sus correlaciones son favorablemente significativas entre ambas variables, lo que se demuestra que los riesgos de información influyen en la mejora para la seguridad de tecnologías.

CAPÍTULO IV

PROPUESTA

4.1. Justificación

La importancia de aplicar un Modelo de Gestión de Riesgos en las Tecnologías de Información, se enfoca en garantizar la seguridad en el tratamiento de datos para las empresas aéreas del país, de modo que se reduzcan las posibilidades de pérdida de información identificando políticas para el almacenamiento, envío y transmisión de los datos.

A más de ello, la aplicación correcta del documento actual posibilita un mayor aprendizaje para los colaboradores que forman parte de las empresas aéreas, principalmente en los directivos quienes son los encargados de implementar las políticas de seguridad informática, cuyos conocimientos obtenidos facilitarían el desarrollo de nuevos modelos de gestión que se encaminen hacia la mejora del funcionamiento organizacional.

4.2. Propósito general

El propósito de implementar un modelo de gestión está en reducir los niveles de riesgos operativos y de reputación que han sido ocasionados por los equipos y software informáticos instalados. Bajo esta realidad, se busca implementar diversas políticas de seguridad cumpliendo el esquema estructural que se ha establecido según la familia de la Norma ISO/IEC 27000, por lo que en el proyecto actual se ha aplicado la ISO 27001 que se enfoca hacia los Sistemas de Seguridad de la Información y la ISO 27002 en base a las Buenas Prácticas para la Gestión de la Seguridad de la Información.

A más de ello, entre los factores y subfactores de riesgo se determinan acciones de prevención y corrección, la primera de ellas se encargarán de anticiparse a los posibles eventos adversos que pudieran ocurrir, mientras que las medidas de corrección se focaliza hacia la implementación de nuevas actividades para modificar el modelo de gestión con el que se ha obtenido los resultados esperados.

4.3. Desarrollo

4.3.1. Introducción del proyecto

El presente Modelo de Gestión de Riesgo en tecnologías de información se estructura de acuerdo al ciclo de Deming en el cual se identifican las etapas de planear, hacer, verificar y actuar, destacando que cada una de ellas se establece un esquema en el que se incluyen a aquellas sub etapas consecutivas que conforman el documento a desarrollar según lo dispuesto por la familia de la Norma ISO/IEC 27000, las mismas que se enuncian de la siguiente manera:

Tabla 23. Ciclo de Deming PHVA

PHVA	ESQUEMA	SUB ETAPAS
Planear	Crear	• Introducción • Objetivos y campo de aplicación • Términos y definiciones • Sistema de gestión de seguridad de la información (análisis de riesgos, política de seguridad)
Hacer	Implementar y operar	• Responsabilidad de la dirección
Verificar	Supervisar y revisar	• Revisión del SGSI por la dirección
Actuar	Mejorar	• Mejorar el SGSI

Fuente: *Investigación propia*
Elaborado por: *La autora*

4.3.2. Objetivos y campo de aplicación

Al diseñar un Modelo de Gestión de Riesgos para mejorar la seguridad de la información en empresas aéreas del Ecuador mediante la norma ISO/IEC 27000, resulta fundamental determinar los objetivos del documento, el campo de aplicación, así como además los términos y definiciones que se utilizan en el proyecto actual.

4.3.2.1. Objetivo del proyecto

Objetivo general

- Mejorar la seguridad de la información bajo la norma ISO/IEC 27000 para empresas aéreas del Ecuador

Objetivos específicos

- Disminuir el riesgo operacional a través de la implementación de políticas de seguridad informática para las empresas aéreas del Ecuador
- Reducir el riesgo de reputación mediante el uso de políticas de seguridad informática para empresas del Ecuador

4.3.2.2. Campo de aplicación

El Modelo de Gestión de Riesgos que se busca implementar está enfocado hacia su campo de aplicación en la seguridad de la información, de tal manera que se permita generar una mayor confianza en la transmisión y almacenamiento de datos en las compañías aéreas del Ecuador, tanto al interior de la organización como fuera de ellas, con ello se podría evitar que la información de cada empresa se utilice propósitos malintencionados que puedan afectar la imagen de las organizaciones.

4.3.3. Términos y definiciones

- **Gestión de riesgos.** Se refiere a las políticas y actividades coordinadas para planificar, organizar, dirigir y controlar una compañía con la finalidad de reducir los riesgos y la incertidumbre de la entidad (Corporación HEFLO, 2017).
- **Política de seguridad.** Es aquella que protege la información confidencial estableciendo medidas de seguridad que sean aplicados por los usuarios del sistema mediante el uso de nuevas aplicaciones u otras ya existentes. (Corporación IBM Knowledge Center, 2019)

- **Probabilidad.** Es la posibilidad de algo que suceda siendo medido de manera objetiva o subjetivamente mediante la utilización de términos generales o matemáticos (Corporación ISOTools, 2019).
- **Severidad.** Se refiere al valor que se asignada al daño más probable que se produciría en caso de que se materialice (Damani, 2019, p. 148).

4.3.4. Sistema de gestión de la seguridad de la información

4.3.4.1. Análisis de riesgos

Al realizar el análisis de riesgos resulta fundamental determinar los niveles de probabilidad y severidad obteniendo así los diversos niveles de amenazas como son muy alto, alto moderado y bajo en base al punto obtenido, es por ello que la calificación de cada uno de los riesgos del modelo de gestión está dado de acuerdo a la siguiente tabla que se observa de la siguiente manera:

Tabla 24. Matriz de riesgos propuesta

		Severidad		
		Mínima (4)	**Marginal (6)**	**Crítica (8)**
Probabilidad	**Poco probable (3)**	Bajo (12)	Bajo (18)	Moderado (24)
	Probable (5)	Bajo (20)	Moderado (30)	Alto (40)
	Muy probable (9)	Moderado (36)	Alto (54)	Muy alto (72)

Fuente: *Investigación propia*
Elaborado por: *La autora*

Por lo tanto, tomando en consideración cada uno de los factores y subfactores de riesgo es posible establecer las posibles consecuencias de cada uno de ellos, estableciendo así una calificación de acuerdo a sus niveles de probabilidad y severidad para de esta manera obtener sus categorías de riesgos y en base a ello, identificar los correspondientes tipos de políticas que son necesarias implementarse en el SGSI (Sistema de Gestión de Seguridad de la Información):

Tabla 25. Riesgos identificados y políticas de segudidad

Factor de riesgo	Subfactores de riesgo	Descripción	Probabilidad	Severidad	Evaluación del riesgo	Nivel de riesgo	Políticas de seguridad
Riesgo operacional	Errores humanos	Pérdida de datos ocasionados por los trabajadores	9	6	54	Alto	Política de retención de registros
Riesgo operacional	Fallas electrónicas	Instalaciones eléctricas inadecuadas	9	8	72	Muy alto	Políticas de almacenamiento de información
Riesgo operacional	Desperfectos en equipos electrónicos	Mal estado de los equipos informáticos	5	6	30	Moderado	Política de uso de equipos informáticos
Riesgo de reputación	Virus informáticos	Virus maliciosos en programas informáticos	5	6	30	Moderado	Política de software no autorizado
Riesgo de reputación	Publicidad negativa	Publicidad negativa por información compartida	5	8	40	Alto	Política intercambio de datos con otras organizaciones
Riesgo de reputación	Pérdida de Información confidencial	Robo de datos confidenciales de los equipos informáticos	5	8	40	Alto	Política de protección de datos y privacidad

Fuente: *Investigación propia*
Elaborado por: *La autora*

4.3.4.2. Políticas de seguridad

Políticas de retención de registros

Las políticas de retención de registros se determinan con la finalidad de evitar una nueva pérdida de datos por parte de los trabajadores, estableciendo tiempo en que se retienen los documentos de respaldo, este tipo de políticas se describen en la tabla siguiente:

Tabla 26. Políticas de retención de registros

Factor de riesgo	Problema	Políticas de retención de registros
Riesgo operacional	Pérdida de datos ocasionados por los trabajadores	• Las áreas o departamentos de la empresa deberán retener la información de los registros digitales e impresos, al menos durante los próximos doce meses y serán eliminados solamente bajo autorización expresa del gerente o jefe departamental. • Luego de transcurrido el tiempo establecido de los doce meses, los registros impresos que contengan información de carácter confidencial deberán eliminarse en una máquina trituradora de papel, siempre y cuando se haya obtenido con anterioridad información relevante que otorguen un aporte significativo en la futura toma de decisiones.

Fuente: *Investigación propia*
Elaborado por: *La autora*

Políticas de almacenamiento de información

Las políticas de almacenamiento de información se plantean a fin de evitar pérdida de datos por fallas de instalaciones eléctricas, las mismas que serán acatadas por todas las áreas departamentales de la empresa:

Tabla 27. Políticas de almacenamiento de información

Factor de riesgo	Problema	Políticas de almacenamiento de información
Riesgo operacional	Instalaciones eléctricas inadecuadas	• Cada una de las computadoras de la empresa deberán estar programadas para que los datos que se ingresen a los sistemas informáticos se almacenen cada 10 minutos, esto se realizarán con el propósito de no perder información ante fallas en las conexiones eléctricas • Los trabajadores deberán comunicar inmediatamente al jefe inmediato o su delegado, los desperfectos eléctricos que se identifiquen en las instalaciones de la empresa en cualquier de sus áreas o departamentos, con la finalidad de que se eviten daños durante el almacenamiento o transmisión de datos.

Fuente: *Investigación propia*
Elaborado por: *La autora*

Política de uso de equipos informáticos

La política de equipos informáticos está centrada en mejorar la utilización de los aparatos utilizados, ya se realizando mantenimiento preventivo para todos ellos y desarrollando la actualización correspondiente, de esta manera se estaría evitando conflictos en los equipos que se utilicen durante el almacenaje de la información:

Tabla 28. Política de uso de equipos informáticos

Factor de riesgo	Problema	Políticas de uso de equipos informáticos
Riesgo operacional	Mal estado de los equipos informáticos	• A los equipos informáticos se les realizará mantenimiento de sus unidades de hardware al menos una vez cada treinta días, o según como el Gerente de Sistemas lo estime conveniente

		• Los programas de software de los equipos informáticos se encontrarán en constante actualización al menos 15 días y se lo realizará por el especialista del área de sistemas de cada empresa

Fuente: *Investigación propia*
Elaborado por: *La autora*

Política de software no autorizado

Debido a que en los softwares informáticos podrían detectarse aun más virus maliciosos, resulta preponderante aplicar las correspondientes políticas de seguridad en las que es indispensable disponer una conexión estable para su actualización, asi como además instalar en los computadores solamente programas que sean aprobados por el departamento de sistemas de la empresa:

Tabla 29. Política de software no autorizado

Factor de riesgo	Problema	Políticas de software no autorizado
Riesgo de reputación	Virus maliciosos en programas informáticos	• Los programas informáticos de antivirus de la empresa deberán actualizarse constantemente por parte del especialista del área de sistemas, siendo necesario solicitar una conexión establece a las redes digitales de información • En las computadoras y demás equipos informáticos de las empresas, se instalarán solamente los programas que sean aceptados por el departamento de sistemas, siendo necesario solicitar su autorización para su uso y funcionamiento

Fuente: *Investigación propia*
Elaborado por: *La autora*

Política intercambio de datos con otras organizaciones

Las políticas de intercambio de datos se establecen con el objetivo de reducir la publicidad negativa de la empresa, por lo que es fundamental que durante el

envío de información se apliquen las medidas necesarias para evitar que estos datos lleguen a personas inescrupulosas que puedan causar daño en la imagen de la entidad.

Tabla 30. Políticas de intercambio de datos con otras organizaciones

Factor de riesgo	Problema	Política de intercambio de información con otras organizaciones
Riesgo de reputación	Publicidad negativa por información compartida	• La información que se envíe hacia otras empresas será encriptada y transmitida de forma confidencial, utilizando correos electrónicos que se dispongan del propio dominio de la empresa. • No se enviará ningún tipo de información de la empresa a través de cualquiera de los servicios de correos electrónicos gratuitos, por lo que este tipo de acciones estarán sujetadas a sanción por parte del jefe inmediato o del gerente general.

Fuente: *Investigación propia*
Elaborado por: *La autora*

Política de protección de datos y privacidad

La política de protección de datos se implementará al interior de las instalaciones de la empresa, puesto todos sus colaboradores deberán aplicarlas correctamente con el propósito de evitar el robo de información desde los propios computadores de la compañía:

Tabla 31. Política de protección de datos y privacidad

Factor de riesgo	Problema	Política de protección de datos y privacidad
Riesgo de reputación	Robo de datos confidenciales de los equipos informáticos	• Todas las computadoras que se utilicen en las instalaciones de la empresa se podrá acceder solamente a través de un usuario y contraseña designado de forma confidencial a cada trabajador por parte del área o departamento de sistemas de cada compañía

		• Bajo ningún concepto se podrá extraer información de la empresa sin la previa autorización otorgada por el jefe inmediato o su delegado, quien de ser necesario deberá comunicar al gerente de área o gerente departamental.

Fuente: *Investigación propia*
Elaborado por: *La autora*

4.3.5. Responsabilidad de la dirección

Los responsables en hacer cumplir cada una de las políticas de seguridad del presente modelo de gestión de riesgo, se reconocen en la siguiente tabla los mismos que forman parte de las áreas departamentales en las instalaciones de la empresa:

Tabla 32. Responsabilidad de la dirección

Factor de riesgo	Subfactores de riesgo	Políticas de seguridad	Responsables
Riesgo operacional	Errores humanos	Políticas de retención de registros	Gerente General
Riesgo operacional	Fallas electrónicas	Políticas de almacenamiento de información	Gerente de Sistemas e Informática
Riesgo operacional	Desperfectos en equipos electrónicos	Política de uso de equipos informáticos	Gerente General
Riesgo de reputación	Virus informáticos	Política de software no autorizado	Gerente de Sistemas e Informática
Riesgo de reputación	Publicidad negativa	Política intercambio de datos con otras organizaciones	Gerente General
Riesgo de reputación	Pérdida de Información confidencial	Política de protección de datos y privacidad	Gerente de Sistemas e Informática

Fuente: *Investigación propia*
Elaborado por: *La autora*

4.3.6. Revisión del SGSI por la dirección

El Modelo de Gestión de Riesgos de las Tecnologías de Información resulta fundamental que sea revisado por los directivos de la empresa aérea al menos una vez al año, entre los que se destacan a los gerentes departamentales y al gerente general con la finalidad de que se pueda asegurar su adecuado cumplimiento.

El propósito de la revisión está en la de implementar de la forma correcta las políticas del Sistema de Gestión de Seguridad de la Información (SGSI), para que de acuerdo a ello se mantenga una eficacia continua durante su aplicación, de tal manera que los resultados de cada una de las revisiones realizadas se encuentren perfectamente respaldados en la documentación respectiva de la empresa siendo almacenada manteniéndose en óptimas condiciones.

4.3.7. Mejora del SGSI

Tabla 33. Mejora del Sistema de Gestión de Seguridad de la Información

Descripción del riesgo	Tipo de medidas	Acciones
Pérdida de datos ocasionados por los trabajadores	Medida preventiva	Revisar a los trabajadores la forma en que utilizan los equipos informáticos
	Medida de corrección	Realizar talleres sobre el buen manejo de equipos informáticos
Instalaciones eléctricas inadecuadas	Medida preventiva	Identificar a los enchufes y toma corrientes en mal estado
	Medida de corrección	Efectuar una reinstalación del sistema eléctrico para eliminar los cortes de energía
Mal estado de los equipos informáticos	Medida preventiva	Realizar mantenimiento a los equipos informáticos que lo necesiten
	Medida de corrección	Adquirir equipos informáticos de la más alta tecnología para el almacenamiento de datos
Virus maliciosos en programas informáticos	Medida preventiva	Actualizar los software informáticos que se hayan instalado en la empresa
	Medida de corrección	Instalar un firewall en la red de computadoras de la empresa
Publicidad negativa por	Medida preventiva	Enviar información encriptada a través de la red de dominio de la empresa

información compartida	Medida de corrección	Instalar un gestor de contraseñas para el resguardo de información
Robo de datos confidenciales de los equipos informáticos	Medida preventiva	Revisar los dispositivos de almacenamiento externo por el área de sistemas
	Medida de corrección	Utilizar dispositivos de almacenamiento externo aprobados por la empresa

Fuente: *Investigación propia*
Elaborado por: *La autora*

4.3.8. Identificación de las políticas de seguridad con las Normas ISO / IEC 27000

Cada una de las políticas de seguridad establecidas, se ha utilizado tres tipos de las familias ISO / IEC 27000 entre las cuales se describen en la tabla siguiente:

Tabla 34. Identificación de la familia de la Norma ISO / IEC 27000 y las políticas de seguridad propuestas

Políticas de seguridad	ISO / IEC	Denominación de la ISO
Política de retención de registros	Normas ISO 27001	Sistemas de Gestión de la Seguridad de la Información
Políticas de almacenamiento de información	Norma ISO 27002	Buenas prácticas para gestión de seguridad de la información
Política de uso de equipos informáticos	Norma ISO 27002	Buenas prácticas para gestión de seguridad de la información
Política de software no autorizado	Norma ISO 27032	Gestión de la ciberseguridad
Política intercambio de datos con otras organizaciones	Norma ISO 27002	Buenas prácticas para gestión de seguridad de la información
Política de protección de datos y privacidad	Norma ISO 27032	Gestión de la ciberseguridad

Fuente: *Investigación propia*
Elaborado por: *La autora*

En la Norma ISO 27000 se ha aplicado la quinta y última versión de febrero 2018, esta se caracteriza por ser la más completa en relación a las generalidades que se especifican en otros componentes de la misma familia de normas y otorgan un amplio vocabulario en cuanto a la seguridad de la información, por lo que además las normas ISO 27001, 27002 y 27032 proporcionan conocimientos suficientes sobre la seguridad, traslado y almacenamiento de datos.

CONCLUSIONES

La norma ISO/ICE 27000 establece objetivos y políticas con las que se permita gestionar la seguridad de información de los datos sean de instituciones públicas o privadas. La ISO/IEC 27000 se clasifica en diversas normas en las que se incluyen desde el 27001 hasta el 27032, por lo que para el desarrollo del presente trabajo de investigación se ha aplicado la Norma ISO 27001 que consiste en la implementación de los Sistemas de Gestión de Seguridad de la Información. la ISO 27002 que está dado en base a las Buenas Prácticas para la Gestión de Seguridad de la Información y la ISO 27032 que se enfoca hacia la Gestión de la Cyberseguridad.

En las empresas aéreas se identifican tanto riesgos operativos como riesgos de reputación lo que se identifica una mayor presencia de ellos al obtener los resultados de evaluación. A más de ello, estas compañías presentan una menor seguridad en sus programas de software y en sus redes digitales de información por lo que están más expuestos a riesgos ante la pérdida durante el envío y almacenaje de datos.

El Modelo de Gestión de Riesgos en las Tecnologías de la Información se desarrollan en base a la familia de las Normas ISO/IEC 27000, cuya estructura se plantea considerando el ciclo de Deming que se conforma por etapas como Planear, Hacer, Verificar y Actuar. En este modelo se han propuesto políticas de seguridad con la finalidad de reducir tanto los riesgos operativos como los riesgos de reputación de imagen de las empresas.

RECOMENDACIONES

Es recomendable que para una mayor implementación de las políticas de seguridad, se apliquen además otras normas que también forman parte de la familia ISO/IEC 27000 dependiendo del tipo de entidad al que pertenece, con ello se podría garantizar aún más el buen funcionamiento de un SGSI (Sistema de Gestión de Seguridad de la Información).

Los estudios con los que se permitan establecer la situación actual, deberán aplicarse al menos una vez al año con la finalidad de reconocer la evidencia de nuevos riesgos que incidan en el normal funcionamiento de las empresas del sector aéreo, con ello, se podrían aplicar políticas de seguridad acordes a los posibles eventos que pudieran ocurrir.

Las políticas de seguridad de información que requieran ser modificadas, es recomendable que también se revisen por parte de los profesionales externos especializados en el manejo y uso de redes informáticas, cuyo aporte será valioso para definir los nuevos reglamentos y normatividad en el tratamiento de los datos que se almacenan en los dispositivos y equipos electrónicos de las compañías.

BIBLIOGRAFÍA

Argentina: JP Morgan Chase Bank N.A. (16 de agosto de 2018). Obtenido de Riesgo Estratégico: https://www.jpmorgan.com/jpmpdf/1320694345279.pdf

Banco Bilvao Vizcaya Argentaria BBVA. (16 de mayo de 2016). Obtenido de Riesgo Operacional: https://accionistaseinversores.bbva.com/microsites/bbva2012/es/Gestiondelriesgo/Riesgooperacional.html

BBVA. (03 de mayo de 2019). *Banco Bilbao Vizcaya Argentaria, BBVA*. Obtenido de Qué es el riesgo financiero? 5 consejos para evitarlo: https://www.bbva.com/es/finanzas-para-todos-el-riesgo-financiero-y-sus-tipos/

Benjamín, E. (2016). *Organización de Empresas 5ta ed.* México: Mc Graw Hill Educación.

Bernal, C. (2016). *Metología de la Investigación: Administración, economía, humanidades y ciencias sociales 3ra ed.* Quito: Pearson Educación.

Bobiller, S., & Banquet , P. (2015). *Preparación para la certificación.* Barcelona : ENI.

Calder, A. (2015). *Nueve pasos para el éxito, una versión conjunta para la aplicación de las ISO.* Madrid: IT.

Canadá: Instituto Nacional de Salud Pública de Québec. (27 de febrero de 2019). Obtenido de Definición del concepto de seguridad: https://www.inspq.qc.ca/es/centro-collaborador-oms-de-quebec-para-la-promocion-de-la-seguridad-y-prevencion-de-traumatismos/definicion-del-concepto-de-seguridad

Centro Internacional para la Investigación del Fenómeno de El Niño. (18 de octubre de 2016). Obtenido de Aproximación para el cálculo de riesgo: http://www.ciifen.org/index.php?option=com_content&view=category&layout=blog&id=84&Itemid=336&lang=es

Colombia: Departamento Administrativo de la Función Pública. (17 de mayo de 2015). Obtenido de Modelo de Gestión: http://www.funcionpublica.gov.co/eva/es/www.funcionpublica.gov.co/web/eva

Corporación HEFLO. (24 de julio de 2017). Obtenido de Qué es la gestión de riesgos?. Propósitos y concepto: https://www.heflo.com/es/blog/gestion-de-riesgos/que-es-gestion-de-riesgos/

Corporación IBM Knowledge Center. (20 de marzo de 2019). Obtenido de Política y objetivos de seguridad: https://www.ibm.com/support/knowledgecenter/es/ssw_ibm_i_73/rzaj4/rzaj40j0securitypolco.htm

Corporación ISOTools. (13 de noviembre de 2019). Obtenido de Cuál es la terminología que utiliza la nueva ISO 31000: https://www.isotools.org/2018/02/28/la-terminologia-utiliza-la-nueva-iso-31000/

Corporación ORCI Inc. (17 de febrero de 2019). Obtenido de ISO / IEC 27002: http://orcilatam.com/labs/isoiec-27002/

Damani, N. (2019). *Manual de Infection Prevention and Control 4ta ed.* abril: Kindle.

Del Cid, A., Méndez, R., & Sandoval, F. (2015). *Investigación, Fundamentos y Metología 2da ed.* México: Pearson Educación.

Delaux, H. (2017). *Modelo de gestión estrategica* . Madrid : REDACTUM .

EALDE. (28 de Febrero de 2018). *La gestión de riesgos en proyectros* . Obtenido de https://www.ealde.es/gestion-de-riesgos-proyectos/

España: Instituto de Productividad Empresarial Aplicada. (14 de julio de 2018). Obtenido de PDCA, PHVA, Deming o círculo de mejora continua: https://www.ipeaformacion.com/mejora-continua/pdca-phva-deming-circulo-mejora-continua/

Fernández, J., Sánchez, A., García, V., Toval, A., & Hernández, I. (13 de marzo de 2016). *Gaceta Sanitaria*. Obtenido de Estudio sobre la importancia y la seguridad de uso de las contraseñas en el ámbito laboral sanitario: http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S0213-91112015000100016

García, J. (01 de Enero de 2015). *Metodos de evaluación* . Obtenido de http://repositorio.uchile.cl/tesis/uchile/2005/garcia_j2/sources/garcia_j2.pdf

Griffin, D. (25 de abril de 2017). *La Voz de Houston*. Obtenido de Tipos de riesgos de negocios: https://pyme.lavoztx.com/tipos-de-riesgos-de-negocios-4231.html

Grupo ACMS Consultores. (17 de octubre de 2016). Obtenido de Norma ISO 27032: Gestión a la Cyberseguridad: https://www.grupoacms.com/norma-iso-27032

Guerrero, M., & Gómez, L. (13 de agosto de 2015). *Revista Estudios Gerenciales: Universidad ICESI - Colombia*. Obtenido de Gestión de riesgos y controles en sistemas de información: del aprendizaje a la transformación organizacional: https://www.redalyc.org/pdf/212/21226279012.pdf

Hernández Sampieri, R., Fernández, C., & Baptista, M. (2016). *Metodología de la Investigación 6ta ed.* México: Mc Graw Hill Education.

Hernández, J. C., & Vizán, A. (2016). *Lean Manufacturing: Conceptos, Técnicas e Implementación.* Madrid - España: Fundación Escuela de Organización Industrial.

International Organization for Standardization and International Electrotechnical Commission. (2015). *Information technology — Security Techniques Information Segurity Managements Systems Overview and Vocabulary 3ra ed.* Gienbra - Suiza: International Standard.

ISO 25000. (17 de febrero de 2019). Obtenido de Seguridad: https://iso25000.com/index.php/normas-iso-25000/iso-25010/25-seguridad

ISO Platform. (15 de agosto de 2015). Obtenido de ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Measurement: https://www.iso.org/obp/ui/#iso:std:iso-iec:27004:ed-1:v1:en

ISO Tools. (21 de enero de 2015). Obtenido de La Familia de normas ISO 27000: https://www.isotools.org/2015/01/21/familia-normas-iso-27000/

ISO27000.ES. (17 de septiembre de 2015). Obtenido de El portal de ISO 27001: http://www.iso27000.es/iso27000.html

La Norma ISO 27001. (2016). Madrid - Estaña: ISO Tools Excellence.

Lara, A. (2015). *Medición y control de riesgos financieros.* México: LIMUSA.

López, J. (2017). *Planificar la formación con calidad.* Madrid: EPISE.

Martínez, S. (2017). *Metodología de Implantación.* Madrid: ESIC.

Ministerio de Transporte. (05 de Mayo de 2015). *Navegación aérea*. Obtenido de https://www.educar.ec/edu/dipromepg/4eess/u7/7.8.htm

Morán, G., & Alvarado, D. (2018). *Métodos de Investigación.* México: Pearson Educación.

Morgan, j. (2015). *Gestión del Riesgo Operacional.* Buenos Aires: https://www.jpmorgan.com/jpmpdf/1320694344011.pdf.

Moyano, L., & Suárez, Y. (19 de diciembre de 2017). Plan de Implementación del SGSI basado en la Norma ISO 27001:2013. *Trabajo de maestría*. Bogotá, Colombia: Universidad Distrital Francisco José de Caldas.

Newbold, P., Carlson, W., & Thorne, B. (2017). *Estadística para Administración y Economía 6ta ed.* Madrid - España: Pearson Educación S.A.

Nueva ISO 14001:2015. (16 de abril de 2018). Obtenido de Riesgo Ambiental y análisis de los riesgos según la ISO 14001:2015: https://www.nueva-iso-14001.com/2018/04/riesgo-ambiental-segun-la-iso-14001-2015/

Organismo de Certificacion Global. (10 de octubre de 2018). Obtenido de Gestión de Seguridad de la Información: https://www.nqa.com/es-mx/certification/standards/iso-27001

Organización Internacional del Trabajo. (28 de noviembre de 2018). Obtenido de Salud y Seguridad en el Trabajo SST: Aportes para una cultura de la prevención: https://www.ilo.org/wcmsp5/groups/public/@americas/@ro-lima/@ilo-buenos_aires/documents/publication/wcms_248685.pdf

Pérez Fernández, J. A. (2016). *Gestión por Procesos: Cómo utilizar ISO 9001:2000 para mejorar la gestión de la organización.* Madrid - España: ESIC Editorial.

Peribáñez, N., Hernández, M., & Sánchez, M. T. (2017). *Riesgos Laborales relacionados con el Medio Ambiente.* Madrid - España: Asociación de Empresarios del Henares.

Quetglás, G., Toledo, F., & Cerverón, V. (2015). *Fundamentos de Informática y Programación.* Valencia - España: Blackie Books.

Ramos, M. (2017). *Como hacer un plan de empresas.* Barcelona: PROFIT.

Raya, V., & Domínguez , M. (2015). *Gestión de Proyectos Normas ISO.* España: RAMA-SA.

Rosales, S. (16 de enero de 2017). *Superintendencia de Control de Poder de Mercado*. Obtenido de Estudio de Mercado de Transporte Aéreo de Pasajeros: https://www.scpm.gob.ec/sitio/wp-content/uploads/2019/03/Estudio-AEREO-VERSIN-PUBLICA.pdf

Safesociety . (15 de Junio de 2018). *Importancia-de-implementar-un-sgsi.* Obtenido de https://www.safesociety.co/importancia-de-implementar-un-sgsi-en-nuestra-organizacion/

Sistema de Gestión de Seguridad de la Información. (07 de febrero de 2015). Obtenido de ISO/IEC 27006 guía para la certificación del SGSI: https://www.pmg-ssi.com/2014/02/isoiec-27006-guia-para-la-certificacion-del-sgsi/

Sistemas en Gestión de Seguridad de la Información. (17 de enero de 2015). Obtenido de ISO/IEC 27003 – Guía para la implementación de un Sistema de Gestión de Seguridad de la Información: https://www.pmg-ssi.com/2014/01/isoiec-27003-guia-para-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/

Symantec Corporation. (13 de marzo de 2016). *Gestión e Implementación de la Seguridad de la Información*. Obtenido de ISO/IEC 27000: http://www.nhbarcelona.com/area-cliente/ejercicios/presentacion_iso_27000_jun12.pdf

ANEXOS

Anexo 1. Matriz de planteamiento del problema de investigación.

SINTOMAS	CAUSAS	PRONÓSTICO	CONTROL DE PRONÓSTICO
No existe un manejo adecuado de la información tecnológica.	No cuenta con un sistema adecuado de manejo de información.	Pésimo servicio	Modelo de gestión de riesgos de procesos de tecnología de información**.**
Falta de compromiso del personal administrativo	No se implementa, tecnología para salvaguardar la información.	No se lleva un control interno de la información.	Procesos de tecnología de información bajo la norma ISO/IEC 27000
No existe una capacitación idónea de los procesos tecnológicos de información.	Se presenta información de clientes de manera errónea.	Falta de comunicación Interna	Manejo de tecnología bajo las normas ISO/IEC 27000.

Fuente: *Investigación propia*
Elaborado por: *La autora*

Anexo 2. Matriz auxiliar de operación del trabajo de investigación.

<table>
<tr><th>Formulación del problema</th><th>Objetivo general</th><th>Variable Dependiente</th><th>N°</th><th>Dimensión</th><th>Indicador</th></tr>
<tr><td rowspan="2">¿Qué impacto tendría en la seguridad de la información del sector aéreo del Ecuador, la aplicación de un modelo de gestión de riesgos bajo la norma ISO/IEC 27000?</td><td rowspan="2">• Establecer el modelo de gestión de riesgos de procesos de tecnologías de información bajo la norma ISO/IEC 27000 en el sector aéreo del Ecuador.</td><td rowspan="4">Gestión de riesgos de información</td><td>1</td><td>Riesgo operacional</td><td>- Margen errores humanos.
Margen de fallas electrónicas
Margen desperfectos en equipos electrónicos</td></tr>
<tr><td>2</td><td rowspan="2">Riesgo de reputación
Innovación
Relaciones con el cliente</td><td rowspan="2">Margen de virus informáticos

Margen de publicidad negativa
Margen de pérdida de información confidencial</td></tr>
<tr><td>Sistematización del problema</td><td>Objetivos específicos</td></tr>
<tr><td>¿Qué impacto presentará la seguridad de la información?</td><td>• Determinar las características de la gestión de riesgos, de la norma ISO/ICE 27000 y del Sistema de Gestión de Seguridad de la Información (SGSI)</td><td>3</td></tr>
<tr><td rowspan="3">¿Cómo influye la seguridad de la información para brindar una calidad de servicio?</td><td rowspan="3">• Analizar la gestión del riesgo en la seguridad de información de las empresas del sector aéreo</td><td>Variable independiente</td><td>Nª</td><td>Dimensión</td><td>Indicador</td></tr>
<tr><td rowspan="3">Seguridad en las tecnologías de la información</td><td>1</td><td>Seguridad en hardware</td><td>Margen de defectos en hardware
Margen de buen estado de hardware

Margen de confidencialidad en seguridad de datos</td></tr>
<tr><td>2</td><td>Seguridad en redes</td><td>-
Margen de actualización de software
Margen de almacenamiento y seguridad</td></tr>
<tr><td>¿La Norma ISO/IEC 27000, permita un control de la seguridad de la información?</td><td>• Diseñar el modelo de gestión de riesgos en relación a la seguridad bajo la norma ISO/IEC 27000 en el sector aéreo del Ecuador.</td><td>3</td><td>Desarrollo tecnológico</td><td>Margen de actualización de software
Margen de almacenamiento</td></tr>
</table>

Fuente: *Investigación propia*
Elaborado por: *La autora*

Anexo 3. Diagrama de variables del modelo seleccionado

Variable Dependiente	En función	Variables independientes	Dimensiones
Gestión de Riesgos de Información	ISO/IEC 27000	Seguridad en las Tecnologías de la Información	Seguridad en hardware
			Seguridad en software
			Seguridad en redes

Fuente: *Investigación propia*
Elaborado por: *La autora*

Anexo 4. Matriz auxiliar de variables, dimensiones e indicadores

Formulación del problema	Objetivo general	Variable Dependiente	N°	Dimensión	Indicador	Ítems	Instrumentos/Técnica	Procesamiento de datos
¿Qué impacto tendría en la seguridad de la información del sector aéreo del Ecuador, la aplicación de un modelo de gestión de riesgos bajo la norma ISO/IEC 27000?	• Establecer el modelo de gestión de riesgos de procesos de tecnologías de información bajo la norma ISO/IEC 27000 en el sector aéreo del Ecuador.	Gestión de riesgos de información	1	Riesgo operacional	- Margen errores humanos. Margen de fallas electrónicas Margen desperfectos en equipos electrónicos	¿Se han registrado pérdidas de datos que han sido causados por errores humanos?	Encuesta / cuestionario	Sistema SPSS.
			2	Riesgo de reputación Innovación	Margen de virus informáticos	¿Han presentado fallas electrónicas en su empresa que conlleven a la pérdida de información?	Encuesta / cuestionario	Sistema SPSS.
Sistematización del problema	**Objetivos específicos**		3	Relaciones con el cliente	Margen de publicidad negativa Margen de pérdida de información confidencial			
¿Qué impacto presentará la seguridad de la información?	• Determinar las características de la gestión de riesgos, de la norma ISO/ICE 27000 y del Sistema de Gestión de Seguridad de la Información (SGSI)							
¿Cómo influye la seguridad de la información para brindar una calidad de servicio?	• Analizar la gestión del riesgo en la seguridad de información de las empresas del sector aéreo	**Variable independiente**	**Nª**	**Dimensión**	**Indicador**			
		Seguridad en las tecnologías de la información	1	Seguridad en hardware	Margen de defectos en hardware Margen de buen estado de hardware Margen de confidencialidad en seguridad de datos	¿Se han presentado problemas en la pantalla, teclado o CPU de las computadoras de la empresa?	Encuesta / cuestionario	Sistema SPSS.
			2	Seguridad en redes	- Margen de actualización de software Margen de almacenamiento y seguridad	¿Se encuentran en mal estado las computadoras de empresa?	Encuesta / cuestionario	Sistema SPSS.

Formulación del problema	Objetivo general	Variable Dependiente	N°	Dimensión	Indicador	Ítems	Instrumentos/Técnica	Procesamiento de datos
¿La Norma ISO/IEC 27000, permita un control de la seguridad de la información?	• Diseñar el modelo de gestión de riesgos en relación a la seguridad bajo la norma ISO/IEC 27000 en el sector aéreo del Ecuador.		3	Desarrollo tecnológico	Margen de actualización de software Margen de almacenamiento	¿Se han generado problemas en la redes de internet durante la transmisión de los datos?	Encuesta / cuestionario	Sistema SPSS.

Fuente: *Investigación propia*
Elaborado por: *La autora*

Anexo 5. Formato de la encuesta

ENCUESTA DIRIGIDA A LAS EMPRESAS DE AEROLÍNEAS DE TRANSPORTE AÉREO EN EL ECUADOR

Datos personales

Años de funcionamiento en la empresa

Preguntas de investigación

1. ¿Se han registrado pérdidas de datos que han sido causados por errores humanos?
    1. Siempre
    2. Casi siempre
    3. Casi nunca
    4. Nunca

2. ¿Han presentado fallas electrónicas en su empresa que conlleven a la pérdida de información?
    1. Siempre
    2. Casi siempre
    3. Casi nunca
    4. Nunca

3. ¿Han sufrido algún desperfecto los equipos electrónicos de su empresa?
    1. Siempre
    2. Casi siempre
    3. Casi nunca
    4. Nunca

4. ¿Han sido afectados por virus informáticos que incidan en la reputación de su empresa?
    1. Siempre
    2. Casi siempre
    3. Casi nunca

4. Nunca

5. ¿Ha sido involucrada su empresa en publicidad negativa que afecte su integridad?

1. Siempre
2. Casi siempre
3. Casi nunca
4. Nunca

6. ¿Ha existido robo de información confidencial en su empresa durante los últimos doce meses?

1. Siempre
2. Casi siempre
3. Casi nunca
4. Nunca

7. ¿Se han presentado problemas en la pantalla, teclado o CPU de las computadoras de la empresa?

1. Siempre
2. Casi siempre
3. Casi nunca
4. Nunca

8. ¿Se encuentran en mal estado las computadoras de empresa?

1. Siempre
2. Casi siempre
3. Casi nunca
4. Nunca

9. ¿Están desactualizadas las computadoras de empresa?

1. Siempre
2. Casi siempre
3. Casi nunca
4. Nunca

10. ¿Se han encontrado programas innecesarios que afectan la confidencialidad de la seguridad de datos?

1. Siempre
2. Casi siempre
3. Casi nunca
4. Nunca

11. ¿Se han generado problemas en la redes de internet durante la transmisión de los datos?

1. Siempre
2. Casi siempre
3. Casi nunca
4. Nunca

12. ¿Siente desconfianza en las fuentes de almacenamiento virtuales en la seguridad de la información?

1. Siempre
2. Casi siempre
3. Casi nunca
4. Nunca