UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

"EL CONTROL INTERNO APLICABLE A LA SEGURIDAD DE LA INFORMACIÓN PARA SISTEMAS CONTABLES COMPUTARIZADOS SEGÚN ISO 27001 EN EMPRESAS COMERCIALIZADORAS DE PRODUCTOS DE TELECOMUNICACIÓN DEL ÁREA METROPOLITANA DE SAN SALVADOR".

Trabajo de investigación presentado por:

Fuentes Herrera Amilcar Josué

Gámez Artiga José Francisco

Isio Mejía Stephanie Liliana

Para optar al grado de:

LICENCIADO EN CONTADURÍA PÚBLICA

Noviembre de 2017

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES UNIVERSITARIAS

Rector	:Msc. Roger Armando Arias Alvarado
Secretario General	: Lic. Cristóbal Hernán Ríos Benítez
Decano de la Facultad de Ciencias Económicas	: Msc. Nixon Rogelio Hernández Vásquez
Secretaria de la Facultad de Ciencias Económicas	: Licda. Vilma Marisol Mejía Trujillo
Directora de la Escuela de Contaduría Pública	: Licda. María Margarita de Jesús Martínez de Hernández
Coordinador General de Seminario de Graduación	: Lic. Mauricio Ernesto Magaña Menéndez
Coordinación de Seminario de Proceso de Graduación de la Escuela de Contaduría Pública	: Lic. Daniel Nehemías Reyes López
Docente Director	: Licda. María Margarita de Jesús Martínez de Hernández
Jurado Evaluador	: Licda. María Margarita de Jesús Martínez de Hernández
	: Lic. Daniel Nehemías Reyes López
	: Lic. José Ángel Rodríguez García

AGRADECIMIENTOS

Primeramente a Dios por haberme iluminado y brindado las fuerzas necesarias para salir adelante, a mi mamá Amanda Guadalupe Herrera Girón por ser el soporte que siempre ha estado para mí a pesar de todo y que gracias a sus esfuerzos ahora estoy culminando una etapa más. A mi segunda mamá María Joba Girón que supo guiarme desde pequeño y por estar siempre a mi lado apoyándome en cada momento. A mi hija Eimy Carly Fuentes González que es la razón que hace que día a día me levante y quiera seguir adelante para lograr todo lo que me propongo. A mis compañeros de tesis con quienes logramos superar las adversidades que se presentaron. A todos mis amigos que de una u otra forma estuvieron ahí siempre y siempre estarán apoyándome incondicionalmente. A los docentes de la Universidad de El Salvador que supieron compartir su conocimiento. A todos, gracias.

Fuentes Herrera Amilcar Josué

El logro de esta etapa quiero agradecérselo primero a Dios por darme vida y salud hasta el día de hoy, a mi esposa Ruth Evelin Hidalgo y a mis hijas Tatiana, Dayana por su apoyo, paciencia y amor incondicional que me han dado, a mi madre Dulian Artiga y mi padre Carlos Rivas por sus consejos y a todos quienes en algún momento colaboraron directa o indirectamente en este maravilloso resultado. Gracias a Dios por haberme dado fortaleza y perseverancia para salir adelante en mi carrera.

Gámez Artiga José Francisco

Agradezco a Dios primeramente por darme la oportunidad, fortaleza y sabiduría para guiarme en ésta etapa para culminar una meta más, a mi familia Isio Mejía por el esfuerzo que han realizado para brindarme el mejor ejemplo en todo aspecto, por la educación y apoyo incondicional, a mis amigos incondicionales que me han acompañado en ésta etapa, a mis compañeros de trabajo de graduación por ser perseverantes y cumplir el objetivo planteado, a los docentes de la Universidad de El Salvador por compartir su conocimiento, tiempo y dedicación al ser una guía en este proceso.

Isio Mejía Stephanie Liliana

ÍNDICE

ÍNDICE DE TABLAS Y FIGURAS

RESUMEN EJECUTIVO

El control interno es un elemento sustancial dentro de una buena administración y la información sin lugar a duda el activo más valioso de una entidad. El contar con procedimiento idóneos para resguardar la información cada vez es más necesario en un mercado globalizado, lo que implica adoptar medidas de seguridad adecuadas que resguarden áreas tradicionales y también las que anteriormente no se les daba mucha importancia, como lo es la seguridad de la información la cual, conforme pasa el tiempo adquiere un mayor valor empresarial que se vería afectado si no se cuentan con el resguardo pertinente afectando la confidencialidad, integridad y disponibilidad de la misma.

Fortalecer las capacidades de las empresas del sector comercio dedicado a la venta de productos de telecomunicación en cuanto a la seguridad de la información es el objetivo principal que se persigue el cual, se conseguirá con los procedimientos de control interno propuestos.

Para lograr el objetivo buscado es necesario basar los procedimientos propuestos en una normativa fiable y que presente parámetros de calidad, por ello, se consideró que cumplía con las características buscadas para una implementación el Estándar Internacional ISO/IEC 27001.

Los procedimientos basados en este estándar están enfocados en controles preventivos, de detección y de corrección, los cuales asociados a cada una de las áreas principales de estudio como los son: seguridad lógica, seguridad física, *software*, *hardware*, recursos humanos y procedimiento electrónico de datos, los cuales constituyen una herramienta adecuada a las empresas del sector en estudio para el resguardo de la información del sistema contable

computarizado y mantener la confidencialidad, integridad y disponibilidad de la misma para la toma de decisiones.

Las empresas del sector en estudio cuentan con controles internos ya definidos, pero estos no son debidamente ejecutados y ninguno está destinado específicamente al área de seguridad de la información de los sistemas contables computarizados a pesar de que los profesionales de la contaduría pública consideran necesario fortalecer dicha competencia en el ámbito laboral.

Por lo anterior, es necesario que gerencia incentive una cultura de riesgo capacitando debidamente al personal y apoyando con la implementación de los procedimientos de control adecuados para mantener la confidencialidad, integridad y disponibilidad de la información.

INTRODUCCIÓN

En la actualidad y con la evaluación de las tecnologías, la información y su seguridad ha tomado una importancia significativa en cada empresa a tal punto que ahora forma parte de los activos más importantes de las entidades y asegurarla es un punto esencial para la administración.

Es por esto que el trabajo de investigación parte de la necesidad de gestionar el riesgo asociado a la seguridad de la información para sistemas contables computarizado de las empresas del sector comercio dedicados a la venta de productos de telecomunicación y de la adecuada selección de procedimientos de control basados en el Estándar Internacional ISO/IEC 27001 para agregar valor a las empresas en estudio.

Por lo anterior, el presente documento se desarrolla en cada uno de sus capítulos de la siguiente forma:

En el capítulo I se presenta el planteamiento del problema el cual, contiene la situación problemática, enunciado del problema, justificación de la investigación, los objetivos de la misma y las hipótesis planteadas. También, incluye las limitaciones a las que se enfrentaron los investigadores en la realización del trabajo.

El capítulo II está compuesto por la situación actual de la problemática en la que se desglosan todos los puntos importantes como lo el área de control interno, sus componentes, los roles, la seguridad de la información y los sistemas contables computarizados. También incluye las principales definiciones, la legislación aplicable y la normativa técnica que se utilizó.

El capítulo III contiene la metodología de la investigación en la cual, están los sujetos de estudio, las técnicas y materiales a utilizar, el procesamiento y análisis de la información a través

del cruce de variables, lo cual se utilizó para el desarrollo del diagnóstico de la investigación conforme los indicadores definidos, el cronograma de actividades y una parte muy importante, la presentación de resultados.

En el capítulo IV contiene la propuesta de la investigación en la que se desarrolla los procedimientos que debe de contener un manual de control interno aplicables a la seguridad de la información para sistemas contables computarizados según ISO 27001 en las áreas de mayor interés las cuales incluye: seguridad lógica, seguridad física, recursos humanos, procesamiento electrónico de datos, hardware y software en el contexto de las actividades que se desarrollan en las empresas comercializadoras de productos de telecomunicación del área metropolitana de San Salvador.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Situación problemática.

En el sector comercio enfocado al rubro de las telecomunicaciones, una década atrás, los productos tecnológicos que ofrecían no tenían mucha demanda, debido a que para el mercado se consideraban poco útiles o innecesarios y el uso de los mismos se utilizaba solamente al nivel de las grandes empresas o instituciones gubernamentales además, la gama de productos ofrecidos no era tan amplia y esto ocasionaba que los usuarios no se sintieran atraídos a consumirlos.

Parte del crecimiento en las actividades comerciales se debe a diversos factores externos que han incentivado la compra de los productos que las empresas ofrecen, por ejemplo: la venta de las cámaras de seguridad se incrementan por los altos niveles de violencia en el país, los dispositivos de marcación o puntos de acceso aumentaron con la necesidad de no dejar ingresar a personal ajeno a la empresa y que a manera de prevención de factores adverso la administración de las empresas como parte de sus estrategias han adquirido estos productos, con el fin de dar respuesta a los riesgos que amenazan la continuidad del negocio.

En consecuencia, con el crecimiento de la demanda de los productos, se requiere adaptar y adoptar nuevos controles que cubran áreas de riesgo que evolucionaron con el aumento del mercado por tanto, se ha visto en la necesidad de cubrir no solamente las áreas tradicionales del negocio, sino en involucrar la seguridad de la información a medida que adquiere un mayor valor empresarial y esto se logrará con una protección adecuada de los datos sensibles utilizados para la toma de decisiones.

La falta de controles generan el problema de estudio y a partir de esto surge la necesidad de que las empresas del sector comercio, enfocadas en la venta de productos de la telecomunicación que captan, trasmiten y envían información sensible utilizada para la

realización de sus actividades desde la compra de sus productos hasta la venta de los mismos, implementen o adecuen sus procesos de comercio buscando cumplir lineamientos específicos para salvaguardar la información a través de un tratamiento más completo el cual, se logrará con la adopción de políticas, procedimientos y controles basados en un Estándar Internacional como la ISO/IEC 27001.

Al momento de captar, transmitir y enviar información sensible, es necesario contar con una herramienta que permita realizar esto de forma integrada y para ello, las empresas del sector en estudio han sistematizado sus operaciones haciendo uso de los sistemas contables computarizados los cuales juegan un rol importante en la fluidez de los datos de esta forma, permiten ser analizados, cotejados y resguardados para la toma de decisiones en el nivel gerencial.

En la actualidad este sector no cuenta con una herramienta que se adapte a las actividades específicas que se requiere para el cumplimiento de las mismas, ni tampoco cuenta con políticas y lineamientos que guíen al usuario al hacer uso adecuado del sistema para evitar acceso no autorizados que pongan en riesgo la disponibilidad, integridad y confidencialidad de la información.

El problema identificado en el control interno relacionado a la seguridad de la información para los sistemas contables computarizados presenta las siguientes características:

- Las empresas dedicadas a la comercialización de productos de la telecomunicación no tienen un criterio adecuado para la evaluación de riesgos que gestionen la vulnerabilidad a la que está expuesta la seguridad de la información financiera utilizada para la toma de decisiones gerenciales.

- Limitación en actividades del profesional de la contaduría en el sector en estudio en el área de control interno para la seguridad de la información, por carecer de competencias necesarias para involucrarse en el área.
- En las empresas comercializadoras de productos de la telecomunicación en el área de seguridad de información no constituye prioridad en la revisión de controles internos puesto que, se desconoce el impacto que puede ocasionar un incidente en la seguridad de la información al tener pérdidas de confidencialidad, integridad y disponibilidad de la misma.
- La administración de las entidades en estudio no invierten en el área, por que orientan sus actividades de control en otros rubros más complejos de igual forma, no le dan la relevancia necesaria al incumplimiento en la aplicación de controles para la seguridad de la información

De lo anteriormente expuesto se deriva:

- Clima de incertidumbre sobre la efectividad de control interno que incide en la información financiera utilizada para la toma de decisiones gerenciales, al no salvaguardarla como un activo relevante para las empresas que conforman el sector en estudio.
- Altos costos en servicios de consultoría externa, al contratar profesionales que tengan las competencias suficientes para realizar trabajos sobre control en la seguridad de la información enfocada en las actividades de las empresas en estudio.
- Al no constituir prioridad en la revisión de control interno en el área de seguridad de la información es posible la existencia de pérdidas potenciales de la misma afectando la confidencialidad, integridad y disponibilidad de datos sensible en la tomar de decisiones.

- Sanciones por el ente regulador por exposición de información confidencial a ser divulgada a partes no autorizadas por la entidad del sector en estudio.
- Comprometer las operaciones comerciales, así como también integridad y exactitud de la información, que produzcan altos costos a la entidad.

1.2. Enunciado del problema.

El creciente uso de la tecnología y el aumento en la demanda de los productos de las telecomunicaciones influyen a que la información manejada por estas empresas se haya convertidos en un activo sustancial y por ende se debe enfatizar su importancia en asegurar la confidencialidad, integridad y disponibilidad de la misma, con el propósito de suministrar confianza a la administración de que los datos de clientes, proveedores y de la empresa están protegidos contra pérdidas que se deriven de ataques cibernéticos, robo por parte de terceras personas y procesamiento inadecuados de la misma por parte del personal de la empresa.

Esto conlleva a dotar al personal de una herramienta útil basada en un Estándar Internacional como lo es la ISO/IEC 27001 relacionado con la seguridad de la información y que proporciona una orientación sobre la gestión de riesgos a los que ésta se expone, con el fin de mantener una ventaja competitiva, operativa, rentable y que brinde una buena imagen comercial.

Por todo lo antes mencionado, el enunciado del problema se estructuró de la siguiente forma:

¿En qué medida la falta de procedimientos de control interno relacionado con la ISO/IEC 27001, afecta la seguridad de la información que se maneja a través de los sistemas contables computarizados utilizados en las empresas del sector comercio que se dedican a la venta de productos de telecomunicación del área metropolitana de San Salvador?

1.3. Justificación de la investigación

El control interno es esencial para una administración adecuada, la seguridad de la información es indispensable y disponer con un documento que establezca procedimientos de control interno enfocados a la seguridad es idóneo si se busca el resguardo de ésta.

Por lo anterior, el trabajo de investigación se enfoca en los profesionales de la contaduría pública, que tengan la disposición de implementar controles internos en el área de tecnología de información desde la perspectiva establecida en el Estándar Internacional ISO/IEC 27001 relacionado a la seguridad de la información, para proporcionar una guía o marco de consulta sobre procedimientos adecuados al sector en estudio.

Así mismo, se busca beneficiar a las empresas del sector comercio que se dedican a la venta de productos de telecomunicación, específicamente en el área de control interno para que con esta herramienta puedan fortalecer sus procesos, minimizar sus costos y que esto se refleje en los precios de venta de los productos que ofrecen a beneficio de los consumidores.

Es importante mencionar que el control interno aplicado en las empresas en estudio no integra dentro de sus procedimientos el área de tecnología y de igual forma, carece de éstos para verificar el cumplimiento de aspectos legales aplicables al tema. Por tanto, en esta investigación se considera un análisis de riesgo basado en el marco de referencia aplicable a la seguridad de la información establecido en el Estándar Internacional ISO/IEC 27001.

Existen investigaciones previas sobre esta temática, sin embargo, a diferencia de los estudios anteriores el sector para el cual se enfoca la investigación no posee una herramienta adecuada que proporcione una orientación para analizar y gestionar riesgos para la seguridad de la información, utilizada en la toma de decisiones para las empresas dedicadas a la comercialización de productos de telecomunicación del área metropolitana de San Salvador.

1.4. Objetivos de la investigación

1.4.1. General

Fortalecer las capacidades de las empresas en cuanto a la seguridad de la información a través de procedimientos de control interno adecuados basado en el Estándar Internacional ISO/IEC 27001 para asegurar que la información financiera que se maneja en los sistemas contables computarizados sea confidencial, integral, preservada y disponible en la toma de decisiones del sector comercio en las empresas que se dediquen a la venta de productos de telecomunicación.

1.4.2. Específicos

- Recopilar información sobre los aspectos que se relacionan a la actividad económica de las empresas en estudio e identificar los riesgos que afecten la seguridad de la información.
- Realizar un análisis de los riesgos identificados que afecten la seguridad de la información para disminuir el riesgo de fraude y de flujo de información erróneo o incompleto.
- Fomentar con la investigación una participación del profesional de la contaduría pública para ampliar sus competencias en el área de tecnología de la información.
- Asegurar que el flujo de la información a través de sistema contable computarizado sea lo más confiable, veraz y útil para una buena toma de decisiones gerenciales.

1.5. Hipótesis

1.5.1. Hipótesis

La aplicación de procedimientos de control interno adecuados basados en el Estándar Internacional ISO/IEC 27001, asegura que la información financiera utilizada a través de los sistemas contables computarizados sea preservada, confidencial, integral y disponible.

1.5.2. Determinación de variables

Variable independiente: Procedimientos de control interno adecuados basados en el Estándar Internacional ISO/IEC 27001.

Variable dependiente: Seguridad de la información financiera utilizada a través de los sistemas contables computarizados.

1.5.3. Operacionalización de variables

Variable independiente: Procedimientos de control interno adecuados basados en el Estándar Internacional ISO/IEC 27001.

Indicadores de variable independiente:

- Mayor grado de cumplimiento de objetivos de la entidad.
- Reducción de número de incidentes que se han prevenido riesgos potenciales.
- Evaluaciones internas a las amenazas existentes en el contexto de la seguridad.
- Registros de comunicación de resultados de las evaluaciones para implementar acciones de corrección.
- Imagen comercial sólida ante las partes interesadas.

Variable dependiente: Seguridad de la información financiera utilizada a través de los sistemas contables computarizados.

Indicadores de variable dependiente

- Nivel de satisfacción de los usuarios de la información en la toma de decisiones.
- Definición de políticas contables documentadas en el sistema contable autorizado por la empresa.
- Aplicación de controles que aseguren la información de forma física y lógica en las instalaciones de la empresa.
- Implementación de controles que restrinjan el acceso a los sistemas contables computarizados.

1.6. Limitaciones a la investigación.

La investigación se encontró limitada por las siguientes causas:

- Algunos de los municipios que integran la población y muestra determinada para la investigación son catalogados como zonas inseguras.
- La desconfianza de las empresas encuestadas por tratarse de información susceptible como lo son políticas y sistemas de información.
- Disponibilidad de tiempo que puedan presentar las personas que formarán parte de la muestra determinada.
- Algunas de las empresas seleccionadas de forma aleatoria no fue posible encontrar la unidad de análisis, puesto que se los servicios de contabilidad prestados a las mismas son *outsourcing*.

CAPÍTULO II: MARCO TEÓRICO

2.1. Situación actual de la investigación

Las empresas del sector comercio dedicadas a la venta de productos de telecomunicación están experimentando un período de transición, abordado por el incremento que han tenido en algunos rubros comerciales como lo es la venta de equipos de seguridad dentro de los cuales se puede hacer mención de: cámaras, equipos con tecnología avanzada, equipos de accesos y los sistemas integrados de redes, esto ha conllevado a que la información que manejan tanto de clientes como de proveedores sea de suma importación y haya necesidad de que ésta se resguarde de manera eficaz y eficiente.

Para lograr este fin las empresas deben aplicar medidas de seguridad con un sistema de control interno con base a un Estándar Internacional como lo es la ISO/IEC 27001 la cual, se enfoca en proporcionar procedimientos para resguardar la información de forma segura. Es importante mencionar que muchas empresas actualmente cuentan con procedimientos de control, en la mayoría de casos, estos no están debidamente documentos a su vez que, al momento de implementar una normativa técnica se cubrirá aspectos que por falta de información no se habían logrado cubrir y que pueden llegar a ser una fuente potencial de riesgo.

2.1.1. Control interno.

Con el inicio de transacciones complejas en la gran empresa se comenzó a desarrollar más la importancia que se le daba al control interno ya que, los dueños del negocio se veían imposibilitados a continuar atendiendo personalmente la gestión de los problemas productivos, comerciales y operativos. Por tal razón, el delegar funciones se hizo necesario al igual que establecer procedimientos formales para prevenir riesgos o disminuir errores y fraudes por tanto, se convirtió en un factor sobresaliente para asegurar la continuidad del negocio.

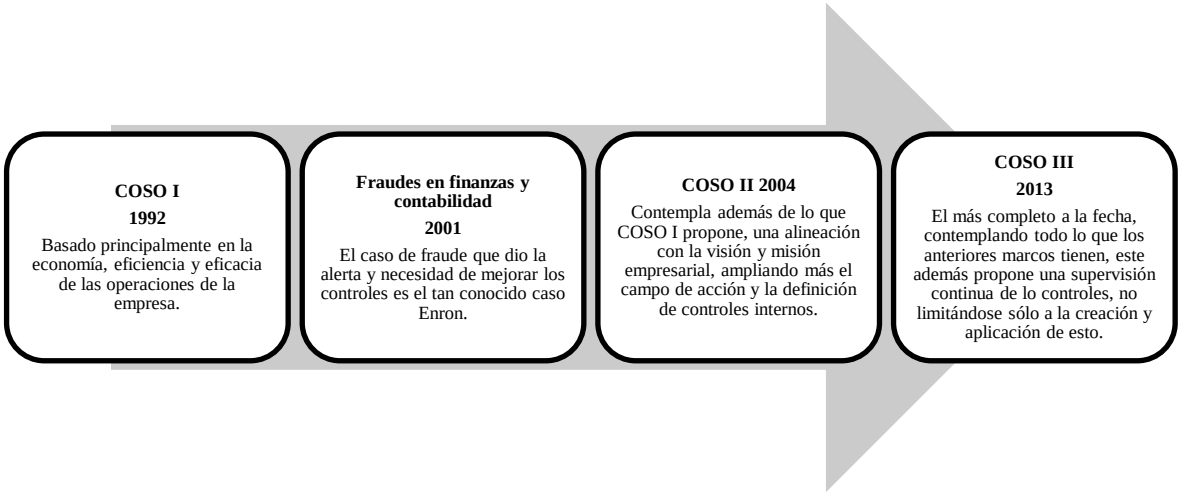


Figura 1, Línea de evolución del sistema de gestión del riesgo COSO

A partir de los grandes fraudes que se desarrollaron en la historia, como lo es uno de los más significativos, el caso Enron, surge la necesidad de un sistema de gestión del riesgo y el más conocido es el enfoque de *Committee of Sponsoring Organizations of the Treadway Commission (*COSO) por sus siglas en inglés, el cual en la figura 1 se muestra como este ha evolucionado partiendo de COSO I hasta el COSO III.

2.1.2. Componentes y principios del control interno

El sistema de control interno tiene como pilar cinco componentes funcionales y diecisiete principios que representan la parte fundamental asociada a cada uno de los componentes. En la tabla 1 se presentan tanto los componentes como los principios que están asociados a cada uno. Mencionar que los cuatro primeros son el eje del diseño y operación del control interno y el último va enfocado en asegurar que continúa operando con efectividad.

Tabla 1
Componentes y principios del control interno.

Componente	Principios relacionados
I. Ambiente de control	1. Entidad comprometida con integridad y valores
	2. Independencia de la supervisión del Control Interno
	3. Estructura organizacional apropiada para objetivos
	4. Competencia profesional
	5. Responsable del Control Interno
II. Evaluación de riesgo	6. Objetivos claros
	7. Gestión de riesgos que afectan los objetivos
	8. Identificación de fraude en la evaluación de riesgos
	9. Monitoreo de cambios que podrían impactar al SC.
III. Actividades de control	10. Definición y desarrollo de actividades de control para mitigar riesgos
	11. Controles para las tecnologías de la información y comunicación para apoyar la consecución de los objetivos institucionales
	12. Despliegue de las actividades de control a través de políticas y procedimientos
IV. Información y comunicación	13. Información de calidad para el Control Interno
	14. Comunicación de la información para apoyar el Control Interno
	15. Comunicación a terceras partes sobre asuntos que afectan el Control Interno
V. Actividades de supervisión	16. Evaluación para comprobar el Control Interno
	17. Comunicación de deficiencias de Control Interno

Nota: Elaborada con información obtenida de COSO III.

2.1.3. Roles, responsabilidades y tipos de controles.

El *Committe of Sponsoring Organizations of the Treadway Commission (*COSO*)* (2004) menciona que: "todo el personal de una entidad tiene alguna responsabilidad en la gestión de riesgos empresariales". El encargado de la unidad de gestión de riesgo es responsable en último lugar y debe asumir su titularidad como tal, apoyado de otros directivos que concuerden con la filosofía de gestión de riesgo implementada, velando por el cumplimiento del riesgo aceptado y gestionando los mismos en el área de responsabilidad de cada uno. La implantación de la gestión

del riesgo debe tener como característica principal la definición clara de los roles y responsabilidad de cada sujeto que participará en este modelo.

Tipos de controles.

Preventivos: para tratar de evitar errores o hechos fraudulentos como por ejemplo: el software de seguridad que evita el acceso a personal no autorizado.

Detección: trata de descubrir a posteriori errores o fraudes que no haya sido posible evitarlos con controles preventivos

Corrección: son un complemento necesario para las actividades de control, ya que tratan de asegurar que se subsanen todos los errores identificados mediante los controles defectivos.

2.1.4. Seguridad de la información

La seguridad de la información y su objetivo

La seguridad de la información involucra una serie de procesos como planificación, implementación, monitoreo y mejora del mismo el cual, se logra al comprender el impacto que ocasiona la falta de medidas de seguridad que inciden en la continuidad de las operaciones. En la actualidad el objetivo de asegurar la información es mantener la confidencialidad, integridad, disponibilidad de la misma, que permita llevar a cabo el desarrollo de la actividad económica anticipándose a los hechos que puedan amenazar a la misma.

Atributos de la seguridad de la información

Confidencialidad: garantiza el resguardo adecuado de la información sensible y tal acceso es limitado al ser almacenada o transmitida a unidades autorizadas.

Integridad: hace referencia a que la información no ha sido alterada con actos de eliminación, duplicidad o cualquier tipo de modificación a la información almacenada, enviada o recibida que evidencien la existencia de incidentes de seguridad.

Disponibilidad: se refiere a acceder de manera oportuna o cuando es requerido a la información lo cual, garantiza la eficiencia de las medidas de seguridad de la información en aspectos de seguridad física y lógica.

Seguridad de la información vs Seguridad informática

La seguridad de la información está más enfocada en riesgos organizacionales, operativos y físicos en el nivel de gestión administrativa de riesgos, en cambio la seguridad informática es más técnica la cual se enfoca en vulnerabilidades y amenazas de las tecnologías de información.

Principales controles para la seguridad de la información

Como parte de las medidas de seguridad que define la gestión de riesgo en las entidades se mencionan algunos controles aplicables al área de seguridad de la información.

- Seguridad de Recursos Humanos
- Gestión de Activos
- Control de accesos
- Seguridad física y ambiental
- Seguimiento

Seguridad física y seguridad lógica.

Es importante mencionar en este apartado lo que implica la seguridad física y lógica de los componentes informáticos que resguardan la información. La seguridad de estos elementos debe ser indiscutible puesto que, así como una tormenta eléctrica puede proporcionar daños

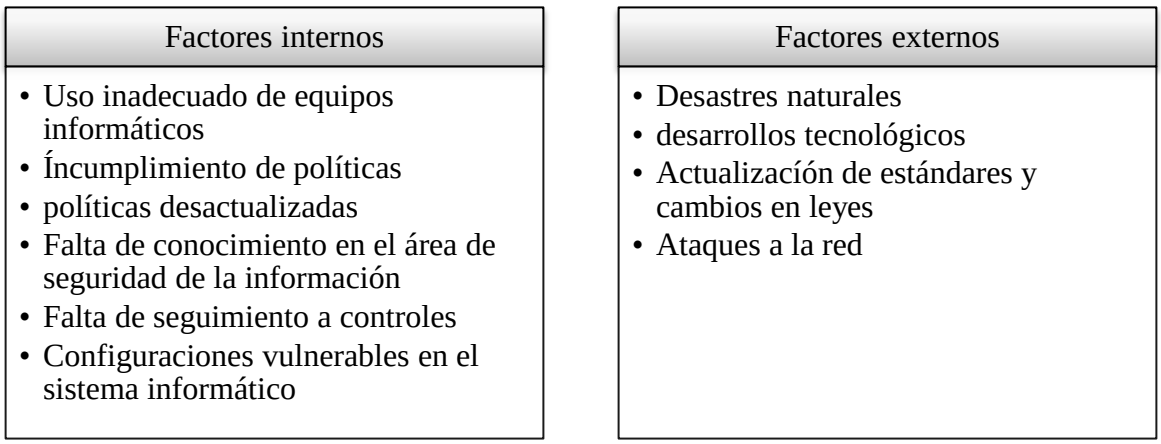


Figura 2, Factores internos y externos que amenazan la seguridad de la información.

Colaterales en un sistema de información dañando el servidor principal, el mismo impacto puede ocasionar un virus que borre datos sensibles e importantes de la entidad que puedan ocasionar retrasos o costos elevados para recuperarlos.

La seguridad física se enfoca en cubrir las amenazas ocasionadas tanto por el ser humano como por la naturaleza del medio físico en que se encuentra ubicado en donde se desarrollan las actividades así como también, las instalaciones del equipo informático que contienen el sistema computarizado.

Las principales amenazas que se prevén son:

- Desastres naturales, incendios accidentales y cualquier daño producido por las condiciones ambientales.
- Amenazas ocasionadas por el ser humano como robos o sabotajes.
- Disturbios internos y externos de forma intencional.

Evaluar y controlar permanentemente la seguridad física del sistema es la base para comenzar a integrar la seguridad como función primordial del mismo. Tener controlado el ambiente y acceso físico permite disminuir siniestros y tener los medios para responder a los

incidentes contra accidentes. El activo más importante de un sistema informático es la información y por tanto, la seguridad lógica se plantea como uno de los objetivos más importantes. La seguridad lógica trata de conseguir los siguientes objetivos:

- Restringir el acceso a los programas y archivos.
- Asegurar que los usuarios puedan trabajar sin supervisión y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos por el procedimiento correcto.
- Verificar que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y que la información recibida sea la misma que la transmitida.
- Disponer de pasos alternativos de emergencia para la transmisión de información.

2.1.5. Sistemas contables computarizados

Contabilidad computarizada.

La contabilidad tiene como propósito proporcionar información financiera sobre una empresa a quienes toman las decisiones administrativas los cuales necesitan de esa información financiera para realizar una buena planeación y control de las actividades de la organización.

Sergio Gonzáles Romero (2013) menciona:

> "Un sistema de información contable está compuesto por los siguientes elementos: los métodos y procedimientos, el *software* de aplicación, las bases de datos, el hardware o e quipos de cómputo y lo más importante, el personal capacitado, los cuales interactúan entre sí de manera coordinada para llevar un control de las actividades financieras y generar información resumiéndolas, en forma, útil para la toma de decisiones".

Componentes de un sistema contable computarizado.

Un Sistema de Información realiza tres actividades básicas: almacenamiento, procesamiento y salida de información. Una actualización del sistema contable a uno computarizado implica contemplar las actividades antes mencionadas y también el ciclo de vida de un sistema de información de esta índole. Las fases mencionadas son:

- Identificación de la necesidad
- Selección del sistema
- Implementación del sistema
- Uso del nuevo sistema

Ventajas de un sistema contable computarizado.

Utilizar sistemas contables computarizados presenta las siguientes ventajas:

- Manejo de gran cantidad de datos de información.
- Gran rapidez del trabajo.
- Reducción del riesgo de error y facilidad en su resolución.
- Integración de la información.
- Reducción de costos.

2.2. Principales definiciones

Los principales conceptos utilizados en el trabajo de investigación debido a la relación y relevancia que tienen con la temática se detallan a continuación:

Tecnologías de la información: se refiere al uso de equipos de telecomunicaciones y computadoras (ordenadores) para la transmisión, el procesamiento y el almacenamiento de datos. La noción abarca cuestiones propias de la informática, la electrónica y las telecomunicaciones.

Activo (Según la ISO/IEC 27001): cualquier cosa que tenga valor para la organización. (ISO27001:2005, pág. 9)

Disponibilidad de la información: propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada. (ISO27001:2005, pág. 9)

Confidencialidad: la propiedad que la información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados. (ISO27001:2005, pág. 10)

Seguridad de la información: es preservar las confidencialidad, integración, disponibilidad, fiabilidad y confianza sobre la información. (ISO27001:2005, pág. 10)

Análisis del riesgo: proceso sistemático que permite identificar las fuentes y calcular el riesgo inherente que puede existir en una transacción. (ISO27001:2005, pág. 11)

Evaluación del riesgo: proceso de comparación estimado, con un criterio específico para determinar el impacto e importancia del riesgo. (ISO27001:2005, pág. 11)

Gestión del riesgo: actividades dirigidas a disminuir o eliminar el riesgo detectado en la evaluación. (ISO27001:2005, pág. 11)

Control interno: es un proceso llevado a cabo por la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías: Eficacia y eficiencia de las operaciones.

Nube informática: Es un modo de transmisión y almacenaje de datos de una red compartida.

Sistema contable computarizado: Un sistema de contabilidad computarizado se vale de computadoras para llevar a cabo los movimientos contables de las cuentas, manejándolas hasta producir las informaciones finales. En los sistemas de contabilidad computarizados, la labor del

contador es prácticamente intelectual. Éste deberá asegurarse de que la configuración y entrada de una transacción estén conectadas, el sistema hará el resto. (Instituto de formación bancaria, pág. s/n)

2.3. Legislación aplicable

A las empresas comercializadoras de productos de telecomunicación les aplican diferentes normativas generales y específicas, pero en esencia, las aplicables tanto en el nivel de sector, como en el ámbito de la seguridad de la información son las que se presentan a continuación:

En la tabla 2 se considera lo que establece la Constitución de La Republica en su Art 2, del cual cabe destacar que “Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen” lo cual, hace inherente el pensar que la información de los clientes recopilada por la empresa no debe ser divulgada pues esto, estaría violando la intimidad personal. Es por esto que resguardar la información es esencial.

En la tabla 3 se presenta lo relacionado al Código de Comercio y la normativa técnica, es importante mencionar que dentro de este marco legal no se obliga al gobierno corporativo a contar con controles de la información digital que manejen, salvo en algunos puntos específicos en los que esta resguardada en formato digital tiene la misma validez del formato físico.

En la tabla 4 se considera lo establecido en el reglamento de la Ley del impuesto sobre la renta, específicamente en su reglamento, en el cual relacionado con el Art 30 de la misma Ley establecen que debe llevarse un control de activos fijos lo cual se hace a través de un cuadro, mismo que puede servir para dar cumplimiento con la cláusula de la ISO/IEC 27001 referente a la administración de los activos relacionados con la seguridad de la información.

Tabla 2
Constitución de la República

Área	Artículo/s de la ley	Descripción
A.5.1. ISO 27001: Orientación de la dirección para la seguridad de la información.	Art 2	Toda persona tiene derecho a la vida, a la integridad física y moral, a la libertad, a la seguridad, al trabajo, a la propiedad y posesión, y a ser protegida en la conservación y defensa de los mismos. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. Se establece la indemnización, conforme a la ley, por daños de carácter moral.

Nota: Se consideró lo que establece la Constitución de la República de El Salvador.

Tabla 3
Código de comercio

Área	**Artículo/s de la ley**	**Descripción**
A.12.3.1. ISO 27001: Respaldo de la información.	Art 455	Los comerciantes podrán hacer uso de microfilm, de discos ópticos o de cualquier otro medio que permita archivar documentos e información, con el objeto de guardar de una manera más eficiente los registros, documentos e informes que le correspondan, una vez transcurridos por lo menos veinticuatro meses desde la fecha de su emisión. Las copias o reproducciones que deriven de microfilm, disco óptico o de cualquier otro medio, tendrán el mismo valor probatorio que los originales siempre que tales copias o reproducciones sean certificadas por notario, previa confrontación con los originales. En caso de falsedad, se estará a lo dispuesto en el código penal.

Nota: Se utilizó el Código de comercio para realizar esta relación.

Tabla 4
Reglamento de la ley del impuesto sobre la renta

Área	**Artículo/s de la ley**	**Descripción**
A.8.1. ISO 27001: Responsabilidad por los activos.	Art 84	Depreciaciones de los bienes dedicados a la producción de ingresos computables se anotarán minuciosamente y detalladamente por medio de registros pormenorizados, debiendo contener, por lo menos, la siguiente información: especificación del bien, valor a depreciar, fecha en que comienza a usarse, periodo de vida útil, mejoras, adiciones, cuota de depreciación, saldo por depreciar, retiro, enajenación, y todos los datos que la naturaleza del bien exija.

Nota: Se elaboró a partir de lo establecido en el Reglamento de la Ley del impuesto sobre la renta

La tabla 5 muestra las implicaciones de la seguridad de la información con respecto al secreto comercial empresarial y como este debe inferir inclusive al momento que se retira una persona de la empresa, con el fin de resguardarla y que no sea utilizada para fines que dañen a la entidad en el mercado.

Tabla 5
Ley de propiedad intelectual

Área	Artículo/s de la ley	Descripción
A.7.3 ISO 2700: Desvinculación y cambio de empleo.	Art 177-181	En estos artículos se establece lo que será considerado como secreto industrial y comercial que guarde una persona y que le permite mantener una ventaja competitiva en el mercado, adoptando medidas necesarias para preservar la confidencialidad que tenga de esta información. Este secreto puede referirse a características de productos, métodos de procesos productivos, recetas o medios y formas de distribución de un producto. También establecen que el secreto industrial o comercial puede transmitirse a una tercera persona, la cual no puede hacer uso de esto sin previa autorización del dueño de la información. En caso de divulgarlo, será responsable de los daños y perjuicios que esto ocasione, todo esto sin perjuicio de las disposiciones penales a las que dieran lugar.

Nota: Información tomada de la ley de propiedad intelectual.

Tabla 6
Ley especial contra los delitos informáticos y conexos

Área	Artículo/s de la ley	Descripción
A.9.2. ISO 27001: Gestión de acceso del usuario.	Art 4	Se refiere a los accesos intencionales y sin autorización o que excedan los derechos concedidos interceptando o utilizando parcial o totalmente un sistema informático será sancionado con prisión de uno a cuatro años
	Art 5	Menciona al que intencionalmente accediera parcial o totalmente a cualquier programa o a los datos almacenados en él, con el propósito de apropiarse de ellos o cometer otro delito con éstos, será sancionado con prisión de dos a cuatro años.
	Art 9	La persona que sin poseer autorización correspondiente burle la seguridad de un sistema informático restringido o protegido con mecanismos de seguridad especifico, será sancionado con prisión de tres a seis años. La inducción de un tercero a realizar actos fraudulentos de esta índole conlleva a la misma sanción
A.9.3. ISO 27001: Responsabilidades del usuario	Art 6	Interferir intencionalmente o altere el funcionamiento de un sistema informático, de forma temporal o permanente, será sancionado con prisión de tres a cinco años. Se considerará agravada la interferencia o alteración, al tratarse de sistemas informáticos públicos o en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión y transporte de energía, de medios de transporte u otros de servicio público, o destinados a la prestación de servicios financieros, la sanción de prisión será de tres a seis años.
	Art 7	Destruir, modificar, ejecutar un programa o realizar cualquier acto destinado a alterar el funcionamiento o inhabilitarlo parcial o totalmente un sistema informático o los componentes de este se sancionará con prisión de tres a cinco años. Si estos daños están destinados a entidades públicas la sanción será de tres a seis años
A.12 ISO 27001: Seguridad de las operaciones	Art 10 - 11	Manipular los datos de un sistema que utilice las Tecnologías de la Información y la Comunicación, mediante cifras falsos o incompletos, el uso indebido de datos o programación, que den como resultado información falsa, incompleta o fraudulenta, con la cuales pretenda obtener beneficios económicos o patrimoniales indebidos para sí o para otro, será sancionado con prisión de dos a cinco años.
	Art 19	Una violación de la seguridad de un sistema informático con la finalidad de destruir, alterar, duplicar, inutilizar o dañar la información, datos o procesos, en cuanto a disponibilidad, integridad y confidencialidad en

	Art 20 - 21	cualquiera de sus etapas (ingreso, procesamiento, transmisión o almacenamiento) será sancionado con prisión de tres a seis años. Interferir, obstruir, interrumpir o interceptar información y que produzca datos nocivos o ineficaces para un tercero será sancionado con tres a seis años de prisión. Si la información interceptada no está disponible al público la sanción será la prisión de siete a diez años.
A.12.4. ISO 27001: Registro y monitoreo	Art 15	Los Administradores del departamento de Tecnológicas de instituciones públicas o privadas, que deshabiliten, alteren, oculten, destruyan, o inutilicen en todo o en parte cualquier información, dato contenido en un registro de acceso, uso de los componentes de éstos, será sancionada con prisión de cinco a ocho años.

Nota: Los artículos tomados de la ley especial contra delitos informáticos y conexos son los más significativos para la investigación.

Tabla 7
Ley de firma electrónica

Área	**Artículo/s de la ley**	**Descripción**
A.5.1. ISO 27001: Orientación de la dirección para la seguridad de la información.	Art 1	En el primer artículo la ley propone equiparar la firma electrónica simple y firma electrónica certificada con la autógrafa, a la vez que reconoce que una firma electrónica es valedera independientemente de su soporte material.
	Art 2	Las regulaciones de la presente Ley serán aplicables a la comunicación electrónica, firma electrónica certificada y firma electrónica simple, o cualquier formato electrónico, independientemente de sus características técnicas o de los desarrollos tecnológicos que se produzcan en el futuro; sus normas serán desarrolladas e interpretadas progresivamente, siempre que se encuentren fundamentadas en la neutralidad tecnológica y equivalencia funcional.
	Art 4	Los principios de la ley son: Autenticidad, integridad, confidencialidad, equivalencia funcional, no repudiación, neutralidad tecnológica y seguridad. Estos principios guardan una relación indiscutible con lo establecido en la norma ISO 27001 con base a la seguridad de la información.
A.12 ISO 27001: Seguridad de las operaciones	Art 14	Los documentos electrónicos deberán conservarse en un medio adecuado con el fin de garantizar su nitidez, integridad, seguridad y fidelidad. Fecha y hora de almacenamiento, existencia de respaldo en caso de error o fallas. Cualquier modificación o alteración del documento hace que este pierda su valor legal.
A.9.3. ISO 27001: Responsabilidades del usuario	Art 15	Es obligación del usuario de almacenamientos de documentos electrónicos para terceros el cumplir con las obligaciones de la ley tanto en la gestión de los documentos como en la solicitud de conversión y almacenamiento de estos, la medida de seguridad física, técnica y de gestión, lista de controles de almacenamiento de documentos, entre otras.
	Art 63	Los usuarios o titulares de firma electrónica están obligados a brindar información veraz y completa, custodiar los mecanismos de seguridad del sistema de certificación que proporcione el prestador y actualizar sus datos en la medida que estos vayan cambiando y solicitar oportunamente la revocación del certificado ante cualquier circunstancia que comprometa la privacidad de los datos

Nota: Información tomada de la ley de firma electrónica

En la tabla 6 se presenta la Ley especial contra los delitos informáticos, de la cual se han recabado los artículos más importantes que tienen relación con las áreas susceptibles de la seguridad de la información y que establecen sanciones por mal uso de la misma que ocasione perjuicios a terceros.

En la tabla 7 se presenta los artículos de la ley de firma electrónica relacionados con la temática y sus áreas pertinentes, cabe destacar que su finalidad es hacer valedera toda aquella información digital a través de una firma de la misma característica, la cual debe velarse que no sea utilizada de manera negligente.

En la tabla 8 presenta los artículos aplicables a la seguridad física de la ley general de prevención de riesgo en los lugares de trabajo, ya que para mantener la información bien resguardada es inherente que el entorno se encuentre en las condiciones idóneas para el fin buscado.

También se toma en consideración una ley que afecta directamente al sector como se observa en la tabla 9 la Ley de contribución especial para la seguridad ciudadana y convivencia la cual únicamente tiene incidencia cuando se venden productos de este rubro económico en específico y que debe considerarse al momento de establecer políticas de seguridad de la información para que sea de conocimiento de los empleados los productos afectos al gravamen.

En la tabla 10 se muestra una de las implicaciones que conlleva el uso inadecuado de información privada o de terceras. Esta es una parte que nuestra legislación penal cubre y que sanciona.

Y para finalizar, también en el Código de trabajo, en el Art 31 numeral 4 se establece que los empleados deben proteger los secretos de la empresa de los que se den cuenta ya sea por su cargo o por caso fortuito.

Tabla 8
Ley general de prevención de riesgos en los lugares de trabajo

Área	Artículo/s de la ley	Descripción
A.11 ISO 27001: Seguridad física y del ambiente	Art 1	Establecer los requisitos que toda entidad debe establecer para asegurar las áreas de trabajo y que garantice un nivel adecuado de protección de la seguridad y salud de los trabajadores.
	Art 8	Es obligación del empleador la formulación y ejecución de programas de gestión de prevención de riesgos ocupacionales de acuerdo con su actividad y la asignación de recursos necesarios para ejecutarlos.
	Art 13	Establece la obligación del empleador de crear comités de seguridad y salud ocupacional en las empresas que laboren quince o más trabajadores. En estos casos dependiendo del número de empleados, así será en número de los delegados de prevención designados.
	Art 22	Dicta las especificaciones que debe contener el edificio en el que se labora en concepto de señalizaciones, los lugares peligrosos entre otros.
	Art 33 - 37	Establecen todas las medidas de prevención que debe considerar el empleador en cuanto a condiciones del lugar de trabajo, señalización de rutas de escape, planes de seguridad, herramientas adecuadas para contrarrestar los casos de emergencia de desastres naturales, fortuitos y los causados por el hombre.

Nota: Información tomada de la ley general de prevención de riesgo en los lugares de trabajo.

Tabla 9
Ley de contribución especial para la seguridad ciudadana y convivencia

Área	Artículo/s de la ley	Descripción
A.5.1. ISO 27001: Orientación de la dirección para la seguridad de la información.	Art 1	La ley establece un gravamen especial para las telecomunicaciones y todos aquellos productos que permitan la utilización de los servicios de telecomunicación.
	Art 3	El hecho generador nace en el momento del pago de servicio de telefonía, televisión, transmisión de datos, transferencia de productos que permitan las telecomunicaciones, retiro de los productos mencionados o el autoconsumo de los mismos
	Art 4	Se establecen quienes serán los sujetos pasivos de la contribución, los cuales son todos aquellos que adquieran los productos que sirvan para generar la trasmisión de las comunicaciones o adquieran un servicio vinculado a esta.
	Art 5	Los agentes de retención serán los proveedores de servicios de telecomunicación y los sujetos pasivos que transfieran dispositivos tecnológicos, aparatos o accesorios de los mismos que permitan la utilización y transmisión de los servicios mencionados.

Nota: Información tomada de la ley de contribución especial para la seguridad ciudadana y convivencia.

Tabla 10
Código penal

Área	Artículo/s de la ley	Descripción
A.9.3. ISO 27001: Responsabilidades del usuario.	Art 184	Se establece que la persona que tenga como finalidad descubrir los secretos o vulnerar la intimidad de otro, se apoderare de comunicación escrita, soporte informático o cualquier otro documento o efecto personal que no le esté dirigido o se apodere de datos reservados de carácter personal o familiar de otro, registrados en ficheros, soportes informáticos o de cualquier otro tipo de archivo o registro público o privado, será sancionado con multa de cincuenta a cien días multa. Si difunde o revelare a terceros los datos reservados que hubieren sido descubierto, la sanción será de cien a doscientos días multa. Y por último a quien se revele el secreto y lo divulgue sabiendo que el origen es ilícito, será sancionado con multa de treinta a cincuenta días multa.

Nota: Información tomada del Código penal de El Salvador.

2.4. Norma técnica aplicable

2.4.1. Estándar Internacional ISO 27001

Reseña histórica ISO/IEC

Los estándares ISO/IEC son elaborados y publicados por *International Organization for Standardization* (ISO) e *Internacional Electrotechnical Commission* (IEC) ambas conocidas por sus siglas en inglés, conformando así el sistema especializado para la normalización mundial creados con el objetivo de brindar herramientas para facilitar las transacciones en el nivel internacional a través de estándares reconocidos. ISO/IEC27001:2013

Con respecto a los temas tratados en estos estándares, por su contenido extenso y por lo complejo que puede llegar a ser la aplicación de los mismos se clasifican por medio de series según el área aplicable como: gestión de calidad, medio ambiente, seguridad de la información, etc.

Estructura serie 27000

ISO/IEC 27001:2013 generalidades

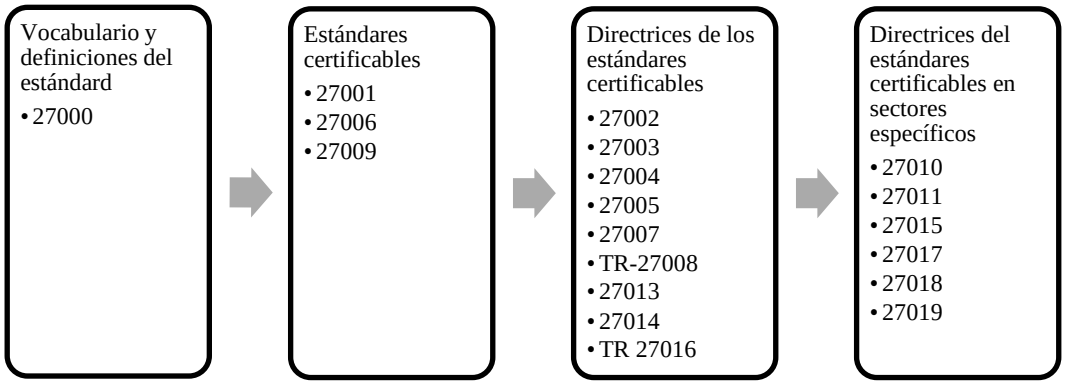


Figura 3, Estándares de la serie 27000

De acuerdo con el alcance de esta investigación se enfocó en la serie 27000 la cual comprende un conjunto de normas relacionadas con la seguridad de la información. Es importante mencionar que la estructura comprende normas certificables las cuales sirven como marco de referencia para poner en prácticas las directrices contenidas en los estándares certificables de una forma más detallada atendiendo el ámbito al cual se quiera aplicar además contiene guías para interpretación las normas en un sector específico, para identificar cuáles de estas normas integran la serie en estudio de acuerdo con su estructura se presenta la figura 3

La norma ISO/IEC 27001 Tecnología de la información- Técnicas de seguridad- Sistemas de gestión de la seguridad de la información- Requisitos en su versión 2013 proporciona las directrices generales aplicables a todas las organizaciones para crear un Sistema de Gestión de Seguridad de la Información el cual se describe a través de un proceso continuo que se basa en establecer, implementar, revisar y mejorar según requerimientos de la norma para mantener la

confidencialidad, integridad y disponibilidad de la información de las partes interesadas internas y externas.

Dentro de su contenido se describe en términos generales el objetivo y dominios de las medidas de seguridad sugeridas por la norma. Para una mejor comprensión del contenido de la ISO/IEC 27001 se presenta la tabla 11.

Estándares relacionados con ISO/IEC 27001

ISO 27000 proporciona un conjunto de definiciones utilizadas en los estándares de esta serie para una mejor interpretación de los mismos.

ISO 27002 contiene directrices para la selección, implementación y administración de controles aplicables a la seguridad de la información de manera más detallada para una mejor comprensión de las medidas de seguridad descritas en el anexo de la ISO/IEC 27001.

ISO 27003 proporciona una guía básica de todos los requisitos establecidos en la ISO/IEC 27001 en las fases del sistema de gestión de la seguridad de la información.

ISO 27004 Es una guía que proporciona lineamientos para evaluar el desempeño de un sistema de gestión de seguridad de la información a través de métricas o técnicas de medición para el cumplimiento de los requisitos de la ISO/IEC 27001.

IS0 27005 Es una guía que proporciona directrices para una implementación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos descritos en la ISO/IEC 27001.

Tabla 11
Estructura ISO/IEC 27001: 2013

Estructura
Preámbulo
Introducción
1. Alcance
2. Referencia normativa
3. Términos y definiciones
4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Apoyo
8. Operación
9. Evaluación de desempeño
10. Mejora
Anexo A Objetivos de control de referencia y controles

Nota: Tomado de la estructura de la ISO/IEC 27001: 2013

Aplicación de la ISO/IEC 27001 en el sector comercial dedicado a la venta de productos de telecomunicación.

La iniciativa de dotar a las entidades del sector comercial dedicado a la venta de productos de telecomunicación con una herramienta para establecer, implementar, mantener y mejorar de manera continua el control interno con base a los lineamientos establecidos en el Estándar Internacional ISO/IEC 27001, nace de la necesidad que estas tienen en las áreas de mayor interés para la administración. Éste recobra su importancia en los últimos tiempos por sugerir controles aplicables a la seguridad de la información de ahí que se tomarán los aspectos para aplicarse al sistema contable computarizado detallando las medidas de control en el área física y lógica que inciden en la información suministrada por el uso de esta herramienta.

Los controles que se proponen están en función de conservar la confidencialidad, integridad y disponibilidad de la información al aplicar un proceso de administración del riesgo, generando confianza en las partes interesadas de que estos se disminuirán de forma efectiva a través de procedimientos específicos para cada área vulnerable.

La base del control interno será el alcance que determine la política de seguridad de la información establecida, la cual debe estar alienada al objetivo de la entidad, incluyendo una mejora continua en el área y en los compromisos aplicables, debe estar disponible a todo el personal y debe ser comunicada pertinentemente por la alta gerencia.

Para que todo esto sea llevado de forma coherente y efectiva debe existir una planificación y determinar en este punto los riesgos y oportunidades que deben ser cubiertos para que el control aplicable a la seguridad de la información pueda lograr los resultados esperados, evitar o disminuir riesgos no deseados y lograr una mejora continua en el personal.

La evaluación y tratamiento del riesgo debe realizarse de forma que brinden resultados consistentes, válidos y comparables de forma continua a través de procesos de evaluación y análisis de los mismos. En caso de que se obtengan resultados que no deseados en el tratamiento de la información, la administración debe considerar revisar los controles adoptados y determinar si no han dejado fuera alguna que sea necesario para obtener los frutos esperados.

Todo lo anterior debe estar relacionado a un objetivo a alcanzar en cada uno de los niveles y funciones relevantes. La administración debe dotar al personal que ejerza esta labor de los recursos necesarios, contar con personas con las competencias adecuadas, divulgar los fines de la política de seguridad de la información establecida y mantener un canal de comunicación activa de cómo se deben realizar las cosas, quien la debe realizar, con quien se deben compartir

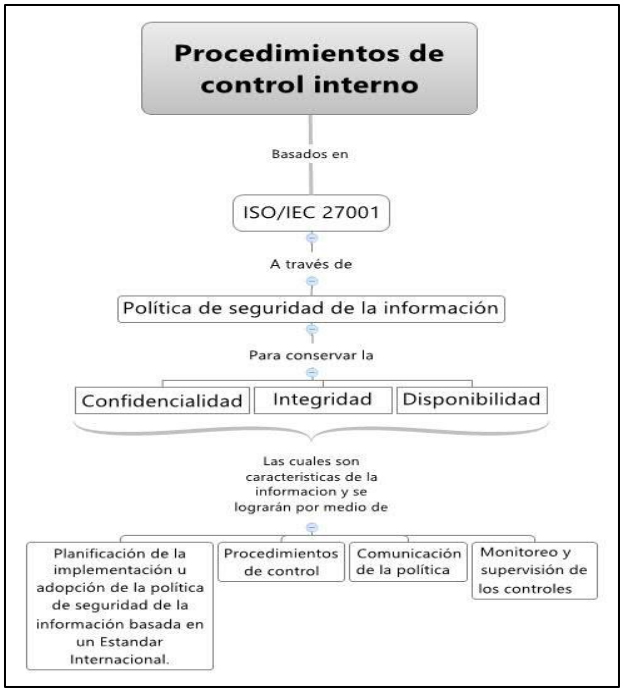


Figura 4, Propuesta táctica de aplicación de la ISO/IEC 27001

La información y los procesos que se verán afectados con la mala gestión de estos procedimientos.

Esta información a su vez debe estar debidamente documentada y actualizada. Además, la administración deberá evaluar el desempeño de la seguridad de la información y la efectividad de los controles a través de métodos que generen resultados comparables y que puedan analizarse adecuadamente. Y por último, la mejora continua es esencial en este aspecto, pues debe evaluarse la conveniencia, suficiencia y efectividad de los procedimientos adoptados. En la figura 4 se muestra a grandes rasgos como se pretende logra la interrelación de la normativo con el sector en estudio.

2.4.2. Aplicación de la normativa ISO 27001 a las áreas de mayor interés

Tabla 12
Aplicación táctica a la seguridad lógica

Área:	Seguridad lógica
1. Alcance y campo de aplicación	Define los requerimientos a considerar para el cumplimiento de la ISO 27001 con respecto a la seguridad lógica la cual implica asegurar el acceso autorizado a los sistemas, además, se define los aspectos a considerar para establecer una política, objetivos y controles que den respuesta a los riesgos asociados para lograr conservar la confidencialidad, integridad y disponibilidad de la información.
2. Referencia normativa	La normativa a la que se hará referencia para abordar esta área es la ISO 27001 de la cual se tomarán los parámetros y directrices que debe adoptar la gerencia al definir el control interno aplicable a la seguridad de la información.
3. Términos y definiciones	Los términos utilizados serán los establecidos en la ISO 27000, los cuales se tomarán de referencia para interpretar la ISO 27001
4. Contexto de la organización	La administración de las empresas dedicadas a la venta de productos de la telecomunicación deberá determinar los asuntos relevantes para la seguridad lógica tanto externos como internos asociados al negocio para lograr los objetivos de resguardar la información, además se debe establecer las necesidades de las partes interesadas para la toma de decisiones en los procesos.
5. Liderazgo	La administración es la encargada de dar el ejemplo en el cumplimiento de la política de seguridad de información que se adecue a los objetivos de la empresa, dotando de los elementos necesarios a las personas que practican esta política además de difundir la misma en el momento oportuno.
6. Planificación	Una adecuada planificación busca lograr los resultados esperados, por tanto, deberá ser coherente con el contexto de la organización y además tendrá que considerar riesgos y oportunidades para disminuir efectos no deseados a la vez que se realizan actividades para mejorar.
7. Apoyo	Una vez adoptado una política y procedimientos, la administración deberá proporcionar los elementos adecuados para asegurar la continuidad de las actividades del negocio a través de medidas de seguridad en el área de seguridad lógica.
8. Operación	La administración debe velar porque los procesos y evaluaciones se documenten adecuadamente, en las etapas de planificación e implementación para cumplir con los objetivos de la seguridad de la información a través de las medidas necesarias para el área de seguridad lógica.
9. Evaluación de desempeño	La evaluación de los procedimientos de seguridad lógica es inherente dado que, a través de monitorear y determinar, como, cuando y quien se debe realizar estas actividades para obtener resultados que representen la cobertura adecuada para el conservar la confidencialidad, integridad y disponibilidad de la información.
10. Mejora	La administración deberá definir un plan si se detectan oportunidades de mejora en los controles asociados al área de seguridad lógica, para llevar a cabo esta etapa la administración debe implementar medidas de seguridad continuas para fortalecer el área y cumplir con las expectativas planteadas.
11. Anexo	La administración de las empresas dedicadas a la venta de productos de telecomunicación deberá establecer procedimientos que resguarden el acceso al sistema de información a través de controles de claves, controles de acceso al sistema, restricción de acceso a información, entre otras.

Nota: Elaborada por el grupo a partir de lo establecido en la normativa técnica.

Tabla 13
Aplicación táctica seguridad física.

Área:	Seguridad física
1. Alcance y campo de aplicación	Define los requerimientos a considerar para el cumplimiento de la ISO 27001 con respecto a la seguridad física para las empresas dedicadas a la venta de productos de la telecomunicación, la cual implica mantener áreas seguras y protección de equipo, además, especifica los aspectos importantes para establecer política, objetivos y controles para conservar la confidencialidad, integridad y disponibilidad de la información.
2. Referencia normativa	ISO/IEC 27000, ISO 27001
3. Términos y definiciones	• Perímetros de seguridad física • Seguridad física • Política de seguridad de información • Controles de acceso físico
4. Contexto de la organización	La empresa dedicada a la venta de productos de la telecomunicación debe de realizar un análisis previo para definir el objetivo, listar las partes interesadas junto con sus expectativas, factores externos e internos relacionados con aspectos legales y capacidad de la organización para cumplir con las perspectivas planteadas para el área de seguridad física.
5. Liderazgo	La alta dirección debe demostrar compromiso para asegurar la gestión de los aspectos establecidos por la ISO 27001 aplicables al área de seguridad física los cuales se integren a las actividades de la empresa con el fin de lograr los resultados esperados.
6. Planificación	La empresa debe identificar su capacidad organizativa para abordar los riesgos y las oportunidades que necesitan ser cubiertas al momento de planificar y establecer los objetivos en el área de seguridad física. Para tratar riesgos se proporciona el anexo a del Estándar Internacional ISO 27001.
7. Apoyo	La empresa dedicada a la comercialización de productos de la telecomunicación debe dotar de recursos, competencias, conocimiento al personal involucrado en cumplir con los lineamientos establecidos para el área de seguridad física, además, debe determinar y documentar las actividades de comunicación internas y externas.
8. Operación	En esta etapa se debe de implementar lo planificado en relación con las acciones definidas para la evaluación de riesgo, así como también, los planes para el logro de objetivos en el área de seguridad física, con el fin de tener certeza que los procesos se llevan a cabo según lo planeado.
9. Evaluación de desempeño	En relación este apartado, la empresa debe de monitorear, medir y analizar la efectividad de la implementación planificada para el área de seguridad física para lo cual, la entidad debe llevar a cabo actividades de auditoría interna que proporcionen evidencia de su cumplimiento, es importante mencionar que este apartado es opcional, no así para las empresas que se dicten en conformidad con esta normativa.
10. Mejora	En el caso que exista la no conformidad en alguna de las etapas anteriores, las empresas en estudio deben aplicar acciones correctivas para controlar, corregir y evaluar las necesidades en el área de seguridad física con el propósito de garantizar la efectividad de sus actividades de manera continua.
11. Anexo	Las empresas dedicadas a la venta de productos de la telecomunicación para evitar los riesgos asociados al accesos no autorizados y daños que puedan comprometer la seguridad de la información deben de implementar controles adecuados para asegurar el área física en el cual es procesada la información esto incluye controles de acceso físico, perímetros de seguridad, protección contra amenazas externas, gestión de cambios en las instalaciones.

Nota: Elaborada por el grupo a partir de lo establecido en la normativa técnica.

Tabla 14
Aplicación táctica procesamiento electrónico de datos

	Área:	Procesamiento electrónico de datos
1.	**Alcance y campo de aplicación**	Establece los requerimientos según el Estándar Internacional ISO 27001 para establecer, implementar, mantener y mejorar la seguridad de la información atendiendo los objetivos y necesidades en el área de procesamiento electrónico de datos en las empresas dedicadas a la venta de productos de la telecomunicación.
2.	**Referencia normativa**	ISO 27000, ISO 27001
3.	**Términos y definiciones**	• Procesamiento electrónico de datos • Integridad • Confidencialidad • Disponibilidad
4.	**Contexto de la organización**	En el contexto del negocio de venta de productos de la telecomunicación se debe considerar aspectos externos e internos que influyen en las actividades al definir las partes interesadas, el nivel de protección que se brindará al área de procesamiento electrónico de datos y los requisitos solicitados para el cumplimiento de aspectos legales, los cuales deben de ser acorde a los objetivos del área.
5.	**Liderazgo**	La alta dirección debe liderar la gestión de la seguridad en el área de procesamiento electrónico de datos al establecer política, objetivos, asignar responsabilidades y autoridades para comunicar el desempeño sobre las actividades de control que conserven la confidencialidad, integridad y disponibilidad de la información.
6.	**Planificación**	Las empresas deben planificar las acciones adecuadas para abordar los posibles riesgos y oportunidades con respecto al área de procesamiento electrónico de datos entre estas medidas de seguridad incluye: el logro de objetivos, evaluación de riesgos, tratamiento de efectos no deseados que se aborda a través de la implementación adecuada de controles, descritos en el anexo a de la ISO 27001.
7.	**Apoyo**	La alta dirección debe de proporcionar los recursos como el desarrollo de competencias suficientes de los responsables asignados para asegurar la información en el área de procesamiento electrónico de datos además de trasmitir el conocimiento necesario para un desempeño favorable sujeto a mejoras continua, para conservar la confiabilidad, integridad y disponibilidad de la información.
8.	**Operación**	Las empresas dedicadas a la venta de productos de la telecomunicación deben incluir como parte de sus actividades revisar la secuencia de las medidas de control planificadas y controlar los cambios en el tratamiento de riesgos asociados al área de procesamiento electrónico de datos.
9.	**Evaluación de desempeño**	Se debe definir los procesos, intervalos de tiempo para ejecutar actividades que proporcionen evidencia sobre la evaluar del desempeño de las medidas implementadas para asegurar la información, así como también, la efectividad sobre los controles implementados en el área de procesamiento electrónico de datos.
10.	**Mejora**	Una de las etapas importantes es dar seguimiento a la evaluación realizada para implementar acciones correctivas de manera que se logre conservar la confiabilidad, integridad y disponibilidad de la información, en el área de procesamiento electrónico de datos
11.	**Anexo**	Se deben implementar medidas de seguridad que conserven la confiabilidad, integridad y disponibilidad de la información, para lo cual se deben considerar controles para el área de procesamiento electrónico de datos como: clasificación de la información, manejo de la información, manipulación de datos, protección contra pérdida de datos, registro y monitoreo de la información, acuerdos de confidencialidad y no divulgación con las partes interesadas, entre otros.

Nota: Elaborada por el grupo a partir de lo establecido en la normativa técnica.

Tabla 15
Aplicación táctica recursos humanos.

Área:	Recursos humanos
1. Alcance y campo de aplicación	Establece los requerimientos según el Estándar Internacional ISO 27001 para establecer, implementar, mantener y mejorar la seguridad de la información atendiendo los objetivos y necesidades en la gestión de actividades de recursos humanos en las empresas dedicadas a la venta de productos de la telecomunicación, asociados a conservar la confidencialidad, integridad y disponibilidad de la información.
2. Referencia normativa	La normativa a la que se hará referencia para abordar este punto es la ISO 27001 de la cual se tomarán los parámetros y directrices que debe adoptar la gerencia en su control interno para asegurar la información que el recurso humano procesa a través del sistema.
3. Términos y definiciones	Los términos utilizados serán los establecidos en la ISO 27000, los cuales a su vez son considerados en la ISO 27001
4. Contexto de la organización	Las empresas que se dedican a la venta de productos de telecomunicación deberán seleccionar personas las cuales se comprometan con la gestión de la seguridad de la información y que se adapten al control definido por la administración para abordar las amenazas externas y factores que influyan en el cumplimiento de objetivos.
5. Liderazgo	El liderazgo se debe de practicar en el cumplimiento de la política establecida en el área de recursos humanos la cual debe de incluir los roles de cada persona dentro de la entidad, lo cual contribuirá en la ejecución de medidas de seguridad para integridad al personal, en sus responsabilidades y además verificará las autorizaciones a personas con el perfil adecuado.
6. Planificación	Como parte de la planificación en el área de recursos humanos se debe de considerar definir un plan de inducción que proporcione a los nuevos empleados el uso adecuado de los recursos proporcionados para el desempeño de las actividades a realizar, lo cual contribuirá a disminuir los riesgos asociados.
7. Apoyo	La administración deberá dotar de las herramientas necesarias al personal incluyendo: capacitaciones continuas, que contribuyan a las competencias necesarias para cumplir con el objetivo planteado en el área de recursos humanos.
8. Operación	Deberán definirse los niveles organizaciones a los cuales se les proporcionará información con el objetivo de conservar la confidencialidad, integridad y disponibilidad de la información a través de la práctica de medidas de seguridad planificadas para el área de recursos humanos.
9. Evaluación de desempeño	La gerencia deberá verificar que el personal se relacione a las políticas de seguridad de información y por medio de la evaluación de desempeño en el área de recursos humanos se determinen los aspectos en que se puede mejorar controles para que el personal de las empresas que venden productos de la telecomunicación cumpla con los objetivos definidos.
10. Mejora	Deberá plantearse una política que busque el crecimiento personal enfocado a la mejora continua a través identificación de puntos de mejora.
11. Anexo	Deberá establecerse una política en la que el recurso humano comprenda la responsabilidad de la seguridad de la información, que la política se divulgue a todo el personal en las etapas al previo empleo, durante y desvinculación y cambio del mismo.

Nota: Elaborada por el grupo a partir de lo establecido en la normativa técnica.

Tabla 16
Aplicación táctica hardware

	Área:	Hardware
1.	**Alcance y campo de aplicación**	Identificar los requerimientos establecidos por el Estándar Internacional ISO 27001 para establecer, implementar, mantener y mejorar la seguridad de la información atendiendo los objetivos y necesidades con el fin de asegurar la información en el área de hardware de las empresas dedicadas a la venta de productos de la telecomunicación.
2.	**Referencia normativa**	ISO 27000, ISO 27001
3.	**Términos y definiciones**	• Hardware • Activo
4.	**Contexto de la organización**	Para las actividades de control interno aplicable al hardware se debe definir las partes interesadas y los requisitos de éstas, los cuales deben de ser acorde con los aspectos externos e internos que influyen en el logro de objetivo.
5.	**Liderazgo**	Las empresas que venden productos de la telecomunicación deben de liderar la gestión de la seguridad de la información relacionada al área de hardware en el proceso de definir: política, objetivos, asignar responsabilidades y autoridades para comunicar el desempeño de esta área.
6.	**Planificación**	Las empresas deben planificar las acciones adecuadas para abordar los posibles riesgos y oportunidades con respecto al área de hardware entre estas acciones se incluye el logro de objetivos, evaluación de riesgos, tratamiento de efectos no deseados que se aborda a través de la implementación adecuada de controles.
7.	**Apoyo**	La alta dirección debe de proporcionar los recursos adecuados para cumplir con el objetivo del área del hardware, en relación con los recursos se debe considerar las competencias suficientes de los responsables asignadas a su vez deben de trasmitir el conocimiento necesario para un desempeño favorable el cual debe ser comunicado según las necesidades internas y externas para mejorar de manera continua, que aborden actividades que correspondan a conservar la confiabilidad, integridad y disponibilidad de la información.
8.	**Operación**	En la parte de operación se refiere al control que las empresas dedicadas a la venta de productos de la telecomunicación deben considerar al revisar la secuencia de las actividades planificadas y controlar procesos que conlleven a cambios en el tratamiento de riesgos asociados al área de hardware.
9.	**Evaluación de desempeño**	Para cumplir con la evaluación se debe definir los métodos, plazos para evaluar el desempeño de la seguridad de la información y la efectividad sobre los controles planeado en el área de hardware.
10.	**Mejora**	Las empresas a través de la evaluación pueden detectar factores que no están siendo tratados conforme lo planeado para el tratamiento de riesgo en el área de hardware, por tanto, se debe de implementar acciones correctivas de manera que se logre conservar la confiabilidad, integridad y disponibilidad de la información.
11.	**Anexo**	Como parte de asegurar la información se deben implementar medidas para tratar el área de hardware, entre éstas se consideran: inventario de activos y asignar responsable sobre la custodia de los mismos, así como también, aplicar controles en la ubicación y protección del hardware, cláusulas de contrato de servicios de soporte técnico, retiro de equipos y gestionar la capacidad de los elementos materiales utilizado para asegurar la continuidad del negocio, entre otros.

Nota: Elaborada por el grupo a partir de lo establecido en la normativa técnica.

Tabla 17
Aplicación táctica software.

Área:	Software
1. Alcance y campo de aplicación	Identificar los requerimientos establecidos por el Estándar Internacional ISO 27001 para establecer, implementar, mantener y mejorar la seguridad de la información atendiendo los objetivos y necesidades con el fin de asegurar la información en el área de software de las empresas dedicadas a la venta de productos de la telecomunicación.
2. Referencia normativa	La normativa a la que se hará referencia para abordar este punto es la ISO 27001 de la cual se tomarán los parámetros y directrices que debe adoptar la alta gerencia en su control interno para asegurar la información contenida en el software utilizado en sus equipos informáticos.
3. Términos y definiciones	Los términos utilizados serán los establecidos en la ISO 27000, los cuales a su vez son considerados en la ISO 27001
4. Contexto de la organización	Las empresas que se dedican a la venta de productos de telecomunicación deberán determinar aquellos aspectos relevantes asociados al software que debe buscar preservar para mantener la seguridad de la información y como un error o ataque al software puede incidir en la toma de decisiones de la entidad.
5. Liderazgo	Un buen liderazgo a través de una política de seguridad para la información bien cimentada enfocada a mantener la integridad del software, dotarlo de los recursos necesarios y establecer personal que se dedique a velar por el cumplimiento de esto ayudará a crear un entorno seguro.
6. Planificación	Partiendo desde la compra de un software que se adapte a las necesidades de la empresa, hasta determinar si este cuenta con los recursos necesarios y si estos cumplen con los requerimientos para lograr los resultados esperados. Realizar pruebas de vulnerabilidad y determinar que tratamiento se darán a posibles violaciones al software.
7. Apoyo	La organización aparte de contar con un software adecuado debe prepararse con las herramientas de defensa adecuadas, los medios idóneos para que pueda funcionar y además contar con personal capacitado que logre obtener el mayor beneficio del mismo.
8. Operación	Una vez determinado el software deberá planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información, también se deben evaluar los riesgos de la seguridad de la información y como estos serán tratados y minimizados.
9. Evaluación de desempeño	Deberá monitorearse constantemente si el software aún está dentro de los parámetros idóneo para la seguridad de la información para así evaluar la conveniencia, suficiencia y efectividad de los controles establecidos para el área.
10. Mejora	La administración deberá establecer un plan de mejora continua partiendo de las debilidades del software que se detecten con las revisiones efectuadas.
11. Anexo	La encriptación de la información puede ser uno de los objetivos de control a adoptar con el fin de resguardar los datos que contenga el software.

Nota: Elaborada por el grupo a partir de lo establecido en la normativa técnica.

CAPÍTULO III: METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Enfoque y tipo de investigación

Para la investigación sobre la falta de controles internos aplicables a la seguridad de la información, se realizó mediante el enfoque cuantitativo a través de la recolección de datos particulares relacionados a las variables en estudio para probar hipótesis con base en la medición de las mismas.

Además, para analizar de forma sistemática, se aplicó el método hipotético deductivo puesto que, permite determinar un punto de partida sobre las causas que originan el problema y a través del uso de técnica e instrumento para la recolección de datos que permitan realizar un análisis de las hipótesis planteadas para proponer una posible solución al problema.

3.2. Delimitación espacial y temporal

La investigación se realizó en el área metropolitana de San Salvador, porque está compuesta por los municipios en los que se encuentran el mayor número de empresas comerciales que se dedican a la venta de productos de telecomunicación y que cuentan con los recursos y condiciones tecnológicos necesarias para llevar a cabo el trabajo de investigación en el área de control interno.

La investigación se efectuó en el periodo 2017 puesto que, se enfocó en la gestión de riesgos de la seguridad de la información en este lapso. Para esto, se consideró utilizar el marco de referencia el Estándar Internacional emitido por la Organización Internacional de Normalización aplicable a la Seguridad de la Información (ISO 27001), en su versión 2013, con referencia a la parte legal en El Salvador no existe una Ley específica que integre los lineamientos sobre las medidas de seguridad para el resguardo de la información, sin embargo a través de la consulta a las Leyes vigentes se ha relacionado en aspectos específicos que protegen

algunos aspectos a considerar sobre la problemática y el sector en estudio como lo son: Constitución de la República de El Salvador, Código de Comercio, Reglamento de la Ley de impuesto sobre la renta, Ley de propiedad intelectual, Ley especial contra los delitos informáticos y conexos, Ley de firma electrónica, Ley general de prevención de riesgos en los lugares de trabajo, Ley de contribución especial para la seguridad ciudadana y convivencia, Código penal.

3.3. Sujetos y objeto de estudio

El estudio fue dirigido a los Contadores públicos, y el objeto de estudio es el control interno.

3.3.1. Unidades de análisis

Las unidades de análisis a considerar en la investigación son los profesionales de la contaduría que tienen a su cargo la implementación y supervisión del control interno dentro de las entidades del sector comercial que se dedican a la venta de productos de la telecomunicación del área metropolitana de San Salvador.

3.3.2. Población y marco muestral

La población para la investigación lo conforman 66 entidades legalmente constituidas y ubicadas en el área metropolitana de San Salvador clasificadas por la Dirección General de Estadísticas y Censos, en el sector comercio en la actividad de venta al por mayor de equipos de comunicación y venta al por menor de equipo de información y de comunicación en comercios especializados, las cuales están establecidas en el listado del Directorio de Empresas 2015, proporcionados por la Unidad de Clasificadores bajo la Clasificación de Actividades Económicas de El Salvador (CLAESS) en los números 46520 y 47412.

La muestra se determinará con base a la fórmula estadística para poblaciones finitas y la selección de la muestra se realizará por medio del método aleatorio simple, auxiliándose de una tabla de números aleatorios, con aplicabilidad sobre las empresas en estudio.

$$n = \frac{Z^2 P * Q * N}{(N-1)E^2 + Z^2 P * Q}$$

En donde:

n= ? Tamaño de la muestra

Z= 1.96 Nivel de confianza

P= 0.9 Probabilidad de éxito

Q= 0.1 Probabilidad de fracaso

N= 66 Población

E= 0.09 Error máximo admisible en términos de proporción

Sustituyendo:

$$n = \frac{((1.96)^2(0.90 * 0.10 * 66))}{((66-1)(0.09)^2) + ((1.96)^2 0.9 * 0.10)}$$

n= 26 empresas del sector comercio que cumplen con las características en estudio.

3.3.3. Variables e indicadores

Variable independiente: Procedimientos de control interno adecuados basados en el Estándar Internacional ISO/IEC 27001.

Indicadores de variable independiente:

- Mayor grado de cumplimiento de objetivos de la entidad.
- Reducción de número de incidentes que se han prevenido riesgos potenciales.
- Evaluaciones internas a las amenazas existentes en el contexto de la seguridad.
- Registros de comunicación de resultados de las evaluaciones para implementar acciones de corrección.
- Imagen comercial sólida ante las partes interesadas.

Variable dependiente: Seguridad de la información financiera utilizada a través de los sistemas contables computarizados.

Indicadores de variable dependiente

- Nivel de satisfacción de los usuarios de la información en la toma de decisiones.
- Definición de políticas contables documentadas en el sistema contable autorizado por la empresa.
- Aplicación de controles que aseguren la información de forma física y lógica en las instalaciones de la empresa.
- Implementación de controles que restrinjan el acceso a los sistemas contables computarizados.

3.4. Técnicas, materiales e instrumentos

3.4.1. Técnicas y procedimientos para la recopilación de la información

Para efectos de recopilar información sobre la problemática en estudio se realizó una encuesta a los contadores públicos que ejercen en el área de control interno, con la finalidad de profundizar la investigación por otra parte, las personas encuestadas a través de su conocimiento en el sector comercio dedicados a la comercialización de productos de la telecomunicación aportaron su experiencia sobre la investigación.

3.4.2. Instrumentos de medición

El instrumento que se utilizó fue el cuestionario el cual se estructuró con 21 preguntas formuladas de forma cerrada y de opción múltiple, con la finalidad de comprobar la hipótesis planteada en la investigación.

3.5. Procesamiento y análisis de la información

La información recopilada por medio del cuestionario utilizado se trabajará en el programa de Microsoft Excel, se ingresarán los resultados obtenidos, luego se tabulará para presentar de forma gráfica los resultados y finalmente se analizará e interpretará los datos obtenidos en la investigación de campo.

3.6. Cronograma de actividades

N°	ACTIVIDADES	FEB		MARZO					ABRIL				MAYO					JUNIO					JULIO					AGOSTO					SEPTIEMBRE			
		3	4	1	2	3	4	5	1	2	3	4	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4
	ELABORACIÓN DE ANTEPROYECTO																																			
1	Inicio																																			
2	Introducción al trabajo de graduación																																			
3	Entrega de avance 1 (idea) y revisión																																			
4	Marco teórico, conceptual, técnico y legal																																			
5	Entrega avance 2 (Formulación del problema)																																			
6	Revisión de avance 2 y correcciones																																			
7	**Primer avance de anteproyecto (hasta objetivos)**																																			
8	Clases de ortografía asesora metodológica																																			
9	Entrega avance 3																																			
10	Corrección avance 3																																			
11	**Entrega del anteproyecto**																																			
12	Corrección del anteproyecto																																			
13	**Capítulo I: Planteamiento del problema**																																			
14	**Capítulo II: Marco teórico**																																			
15	Elaboración del marco teórico, técnico y legal																																			
16	**Capítulo III: Investigación de campo**																																			
17	Elaboración del cuestionario																																			
18	Recolección y tabulación de la información																																			
19	Corrección de investigación de campo																																			
20	**Capítulo IV: Propuesta de Investigación**																																			
21	Elaboración de la propuesta																																			
22	Entrega de la propuesta																																			
23	**Capítulo V: Conclusiones y recomendaciones**																																			
24	Conclusiones y recomendaciones																																			
25	Entrega de trabajo final																																			
26	Defensa del trabajo																																			

3.7. Presentación de resultados

3.7.1. Tabulación y análisis de resultados

Con la información obtenida de las unidades de análisis a través del instrumento de recopilación de datos, se procedió a ingresar en una hoja de cálculo de Excel y por medio de esta obtener los resultados del proceso de recolección realizado.

Se tabularon las opciones de respuesta a las preguntas realizadas y a partir de esto, se elaboró el análisis y diagnóstico de la situación de la problemática en el campo de estudio.

El análisis se realizó a través de cruce de variables, tablas de frecuencias y análisis de resultados obtenidos los cuales se presentan más adelante.

3.7.1.1. Cruce de preguntas para indicadores de variable independiente.

A continuación se presentan los cruces de variables realizados para el indicador siguiente: evaluaciones internas a las amenazas existentes en el contexto de la seguridad que proporcionan mayor grado de cumplimiento de objetivos de la entidad

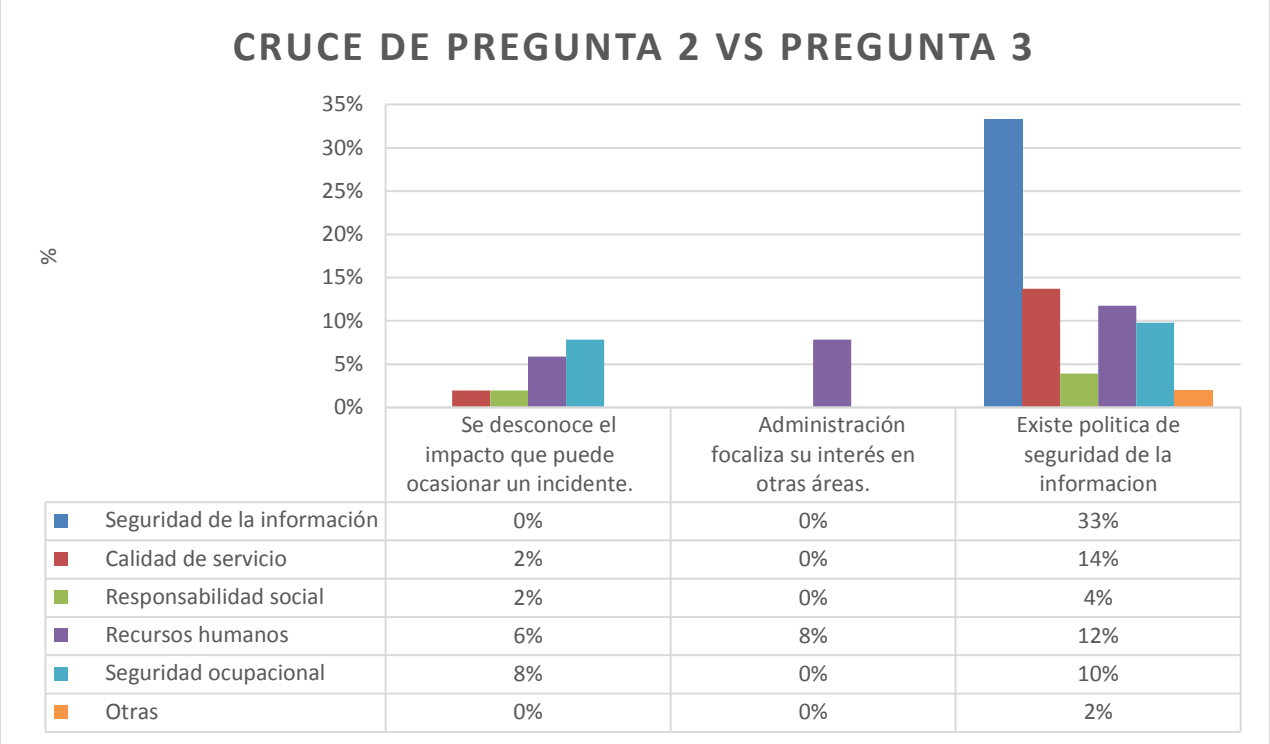
Cruce de pregunta 2 vs pregunta 3

Pregunta 2: Indique ¿Qué otros tipos de políticas posee la empresa distinta a las del área contable?

Pregunta 3: En el caso que no exista política en el área de seguridad de la información ¿cuáles cree que son las razones principales?

Objetivo: Determinar la importancia que tiene la política de seguridad de la información frente a las razones principales por las que en algunas empresas esta no existe.

Pregunta 2 \ Pregunta 3	Se desconoce el impacto que puede ocasionar un incidente.		Administración focaliza su interés en otras áreas.		Existe política de seguridad de la información		Total	
	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr
Seguridad de la información	0	0%	0	0%	17	33%	17	33%
Calidad de servicio	1	2%	0	0%	7	14%	8	16%
Responsabilidad social	1	2%	0	0%	2	4%	3	6%
Recursos humanos	3	6%	4	8%	6	12%	13	25%
Seguridad ocupacional	4	8%	0	0%	5	10%	9	18%
Otras	0	0%	0	0%	1	2%	1	2%
Totales	**9**	**18%**	**4**	**8%**	**38**	**75%**	**51**	**100%**



Interpretación.

Del total de unidades de análisis encuestadas el 33% cuenta con política de seguridad de la información por lo que la importancia que se le brinda a esta área es significativa. También existe un 14% de empresas que cuentan con políticas de calidad de servicio y un 12% con las de recursos humanos. De las entidades que no tienen política de seguridad de la información, un 8% asegura que la administración focaliza su interés en otras áreas y en estos casos particulares es en el área de recursos humanos.

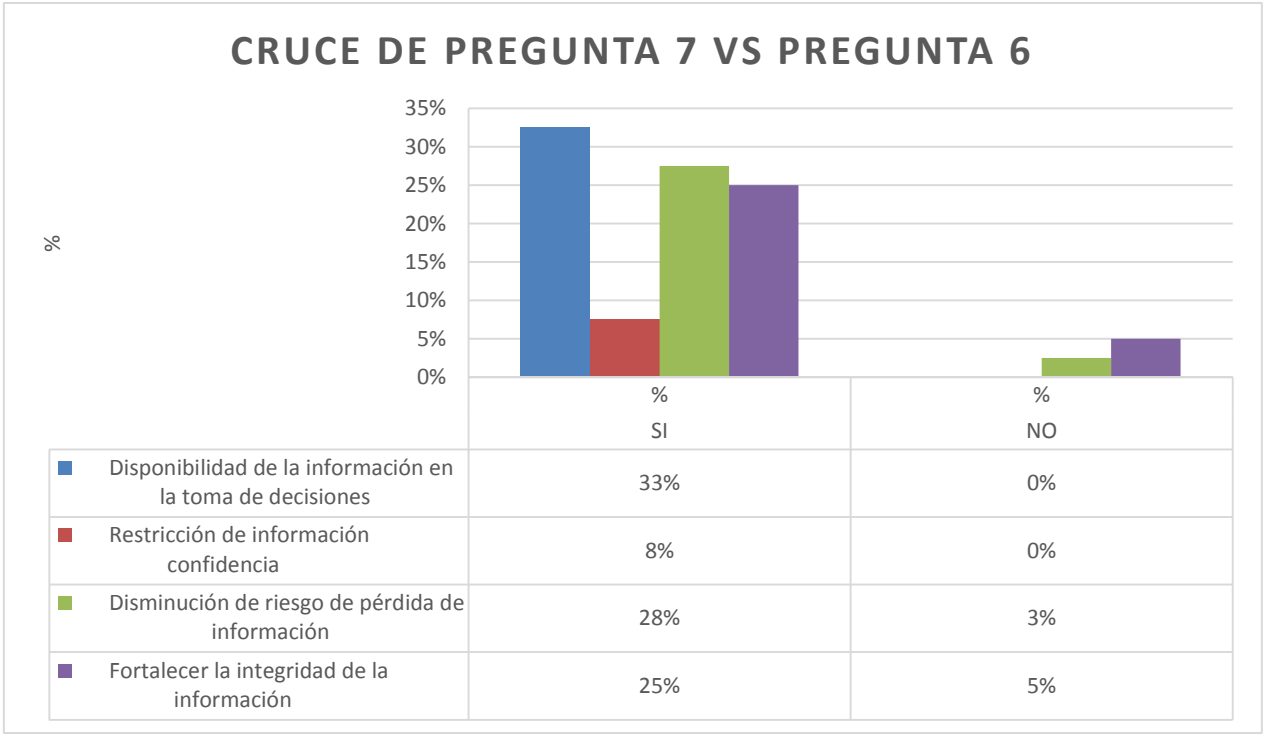
Cruce de pregunta 6 vs pregunta 7

Pregunta 6: ¿Existen controles aplicables al uso del sistema contable computarizado en el lugar en que labora?

Pregunta 7: ¿Cuál considera que es el beneficio de aplicar procedimientos de control interno para asegurar la información que se maneja en el sistema contable computarizado?

Objetivo: Identificar la existencia de controles aplicables al sistema contable computarizado y el beneficio de asegurar la información con estos.

Pregunta 7 \ Pregunta 6	SI		NO		Total	
	Fa	Fr	Fa	Fr	Fa	Fr
Disponibilidad de la información en la toma de decisiones	13	33%	0	0%	13	33%
Restricción de información confidencia	3	8%	0	0%	3	8%
Disminución de riesgo de pérdida de información	11	28%	1	3%	12	30%
Fortalecer la integridad de la información	10	25%	2	5%	12	30%
Totales	**37**	**93%**	**3**	**8%**	**40**	**100%**



Interpretación.

Del total de unidades encuestadas y considerando el cruce efectuado se puede mencionar que el 33% cuenta con controles aplicables al sistema contable computarizado y que el beneficio que buscan a través de esto es contar con la disponibilidad de la información para la toma de decisiones. También de forma representativa con un 28% se afirma que contar con esto controles ayuda a la disminución de riesgo de pérdida de la información.

Un 25% considera que al contar con controles también se fortalece la integridad de esta, la cual es una de las características principales que siempre debe conservar.

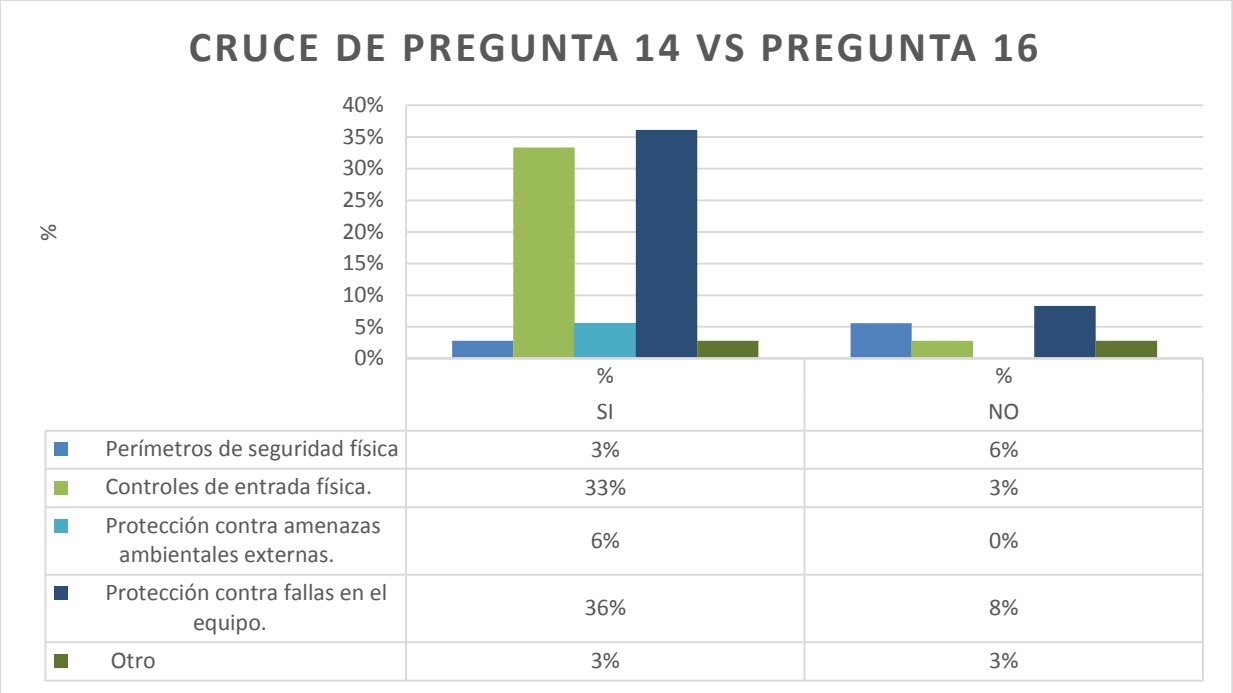
Cruce de pregunta 14 vs pregunta 16

Pregunta 14: En el área de seguridad física, ¿cuáles de los siguientes controles se practican en su lugar de trabajo?

Pregunta 16: ¿Existe en su empresa una unidad que dé seguimiento a los procesos relacionados a la seguridad de la información?

Objetivo: Comprobar la existencia de una unidad de seguimiento a los procesos de seguridad de la información a través de la práctica de controles de seguridad física.

Pregunta 14 \ Pregunta 16	SI		NO		Total	
	Fa	Fr	Fa	Fr	Fa	Fr
Perímetros de seguridad física	1	3%	2	6%	3	8%
Controles de entrada física.	12	33%	1	3%	13	36%
Protección contra amenazas ambientales externas.	2	6%	0	0%	2	6%
Protección contra fallas en el equipo.	13	36%	3	8%	16	44%
Otro	1	3%	1	3%	2	6%
Totales	**29**	**81%**	**7**	**19%**	**36**	**100%**



	% SI	% NO
Perímetros de seguridad física	3%	6%
Controles de entrada física.	33%	3%
Protección contra amenazas ambientales externas.	6%	0%
Protección contra fallas en el equipo.	36%	8%
Otro	3%	3%

Interpretación.

La existencia de una unidad de seguimiento de procesos relacionados a la seguridad de la información se puede ver a través de la existencia de controles implementados. Por esto se puede observar que, del total de unidades de análisis encuestadas, un 36% afirma tener unidad de seguimiento y cuenta con controles de protección de fallas de equipos, además, un 33% también cuenta con controles de entrada física.

Resulta interesante el considerar que el 19% no cuenta con una unidad de seguimiento, pero que a pesar de esto cuentan con controles de protección de fallas de equipos con un 8%.

A continuación se presentan los cruces de variables realizados para el indicador siguiente: Plan de mitigación del número de incidentes que prevén riesgos potenciales a través de los registros de comunicación de resultados de las evaluaciones para implementar acciones de corrección.

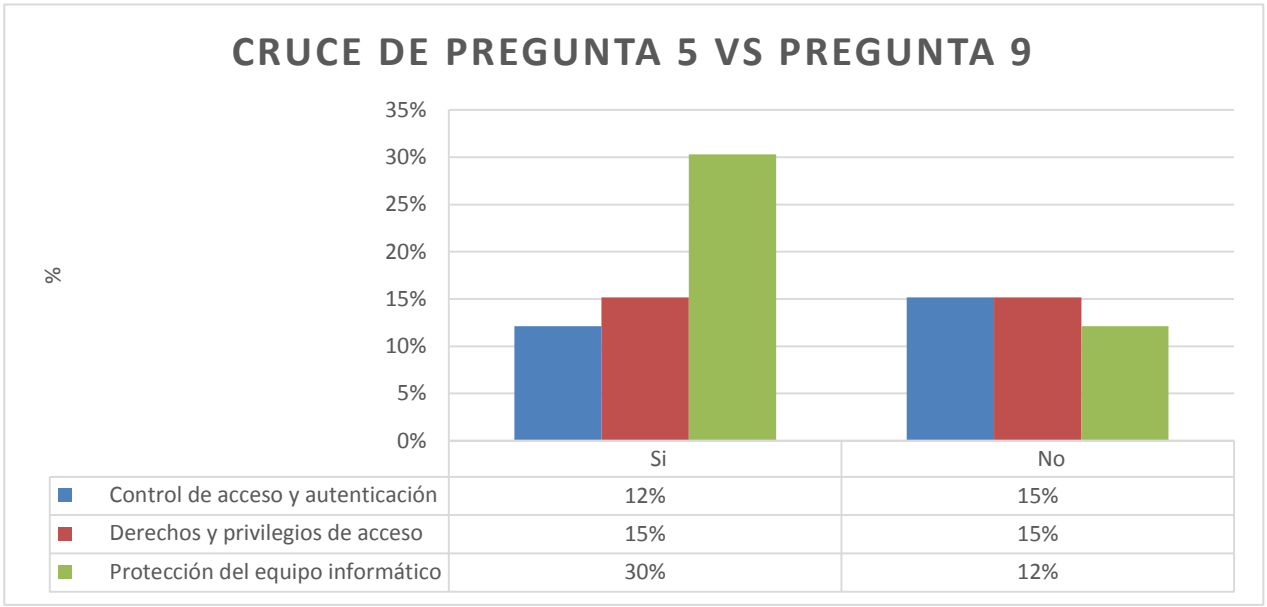
Cruce de pregunta 5 vs pregunta 9

Pregunta 5: ¿Cuál es el área más sensible y que requiere política de seguridad de la información dada su incidencia en la preparación de estados financieros?

Pregunta 9: ¿Existe un plan de trabajo establecido por la gerencia general que brinde un adecuado tratamiento para asegurar la información contable?

Objetivo: Determinar el área más sensible que requiere política de seguridad de la información para lograr subsanar el riesgo a través de la existencia de un plan de tratamiento adecuado de la información.

Pregunta 5 \ Pregunta 9	SI		NO		Total	
	Fa	Fr	Fa	Fr	Fa	Fr
Control de acceso y autenticación	4	13%	5	15%	9	28%
Derechos y privilegios de acceso	5	15%	5	15%	10	30%
Protección del equipo informático	10	30%	4	12%	14	42%
Totales	**19**	**58%**	**14**	**42%**	**33**	**100%**



Interpretación.

La determinación de áreas sensibles que requieran atención adicional por su importancia en los estados financieros es inherente cuando existe un plan de trabajo que busque resguardar la información. Esto se ve reflejado en los resultados obtenidos en los que un 58% cuenta con un plan de trabajo establecido y dentro de esta el área considerada más sensible es la protección del equipo informático con in 30%. Este valor considerado en conjunto con los que no cuentan con un plan de trabajo, representan el 42% del total de empresas encuestadas que consideran esta área la más sensible y que afecta directamente los Estados Financieros en caso de suceder un siniestro.

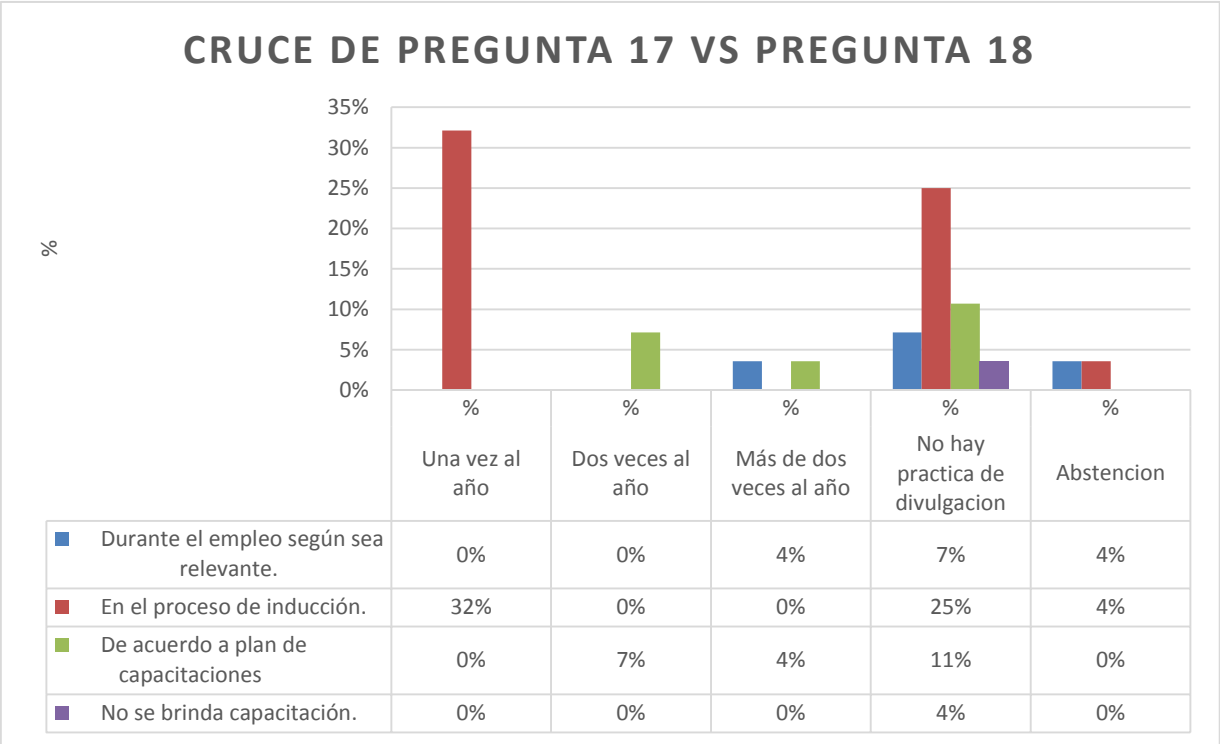
Cruce de pregunta 17 vs pregunta 18

Pregunta 17: ¿En qué momento se brinda capacitación a los usuarios del sistema contable computarizado?

Pregunta 18: ¿Con qué frecuencia se efectúa la divulgación de la política de seguridad de la información a los empleados dentro de la empresa en que labora?

Objetivo: Conocer los momentos en los que se capacita al personal nuevo y determinar la coincidencia de este suceso con la divulgación de la política de seguridad de la información.

Pregunta 17 \ Pregunta 18	Una vez al año		Dos veces al año		Más de dos veces al año		No hay practica de divulgación		Abstenciones		Total	
	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr
Durante el empleo según sea relevante	0	0%	0	0%	1	4%	2	7%	1	4%	4	14%
En el proceso de inducción	9	32%	0	0%	0	0%	7	25%	1	4%	17	61%
De acuerdo a plan de capacitaciones	0	0%	2	7%	1	4%	3	11%	0	0%	6	21%
No se brinda capacitación	0	0%	0	0%	0	0%	1	4%	0	0%	1	4%
Totales	9	32%	2	7%	2	7%	13	46%	2	7%	28	100%



	% Una vez al año	% Dos veces al año	% Más de dos veces al año	% No hay practica de divulgacion	% Abstencion
Durante el empleo según sea relevante.	0%	0%	4%	7%	4%
En el proceso de inducción.	32%	0%	0%	25%	4%
De acuerdo a plan de capacitaciones	0%	7%	4%	11%	0%
No se brinda capacitación.	0%	0%	0%	4%	0%

Interpretación.

Del total de unidades de análisis, el 46% determino que no existe una divulgación de política de seguridad de la información o que en su defecto no existe esta. El 32% de las unidades de análisis comenta que reciben capacitaciones al menos una vez al año y en contraposición también afirman que no existe la divulgación de política de seguridad de la información.

3.7.1.2. Cruce de preguntas para indicadores de variable dependiente.

A continuación se presentan los cruces de variables realizados para el indicador siguiente: definición de políticas contables documentadas en el sistema contable autorizado por la empresa que permita la implementación de controles que restrinjan el acceso a los sistemas contables computarizados.

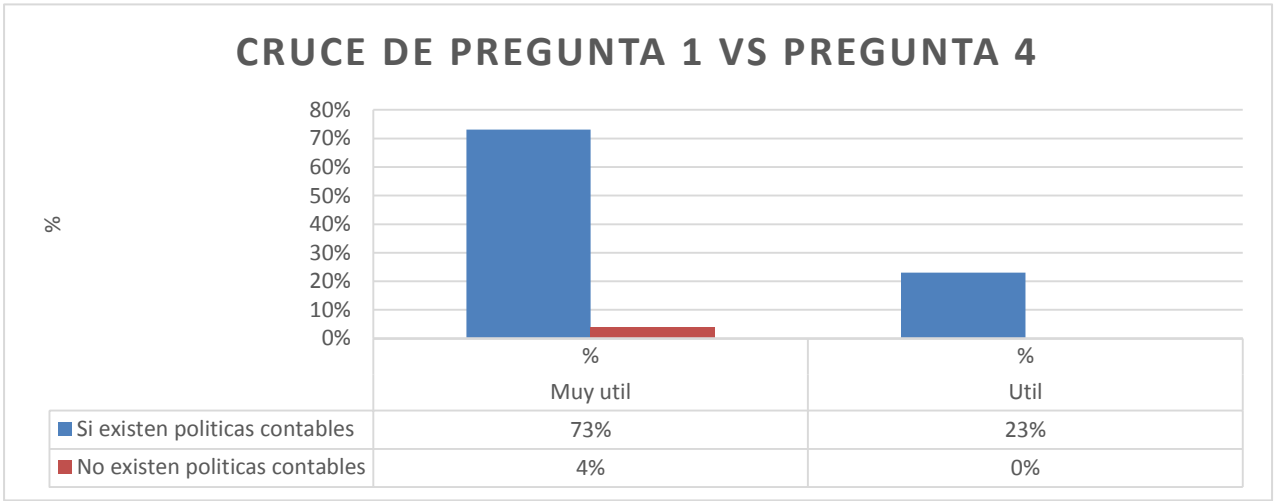
Cruce de pregunta 1 vs pregunta 4

Pregunta 1: En la empresa en la que labora ¿Existen políticas contables que indiquen el tratamiento de las transacciones económicas en el reconocimiento, medición, revelación y presentación?

Pregunta 4: Según su experiencia, ¿qué grado de utilidad posee la política de seguridad de la información en la determinación de las cifras contables presentadas en los Estados Financieros?

Objetivo: Identificar la existencia de políticas contables y la utilidad que representaría complementar estas con una política de seguridad de la información.

Pregunta 1 \ Pregunta 4	Muy útil		Útil		Total	
	Fa	Fr	Fa	Fr	Fa	Fr
Si existen políticas contables	19	73%	6	23%	25	96%
No existen políticas contables	1	4%	0	0%	1	4%
Totales	**20**	**77%**	**6**	**23%**	**26**	**100%**



Interpretación.

Del total de datos recopilados, el 73% cuenta con políticas contables y además considera que sería muy útil contar con políticas de seguridad de la información, lo que representa la importancia que día a día toma este activo en las entidades privadas. En total un 96% de los encuestados consideran según su experiencia laboral que es útil o muy útil contar con política de seguridad de la información. En contraposición, el 4% de los encuestados no cuenta con políticas contables pero a pesar de esto considera muy útil el contar con una de seguridad de la información.

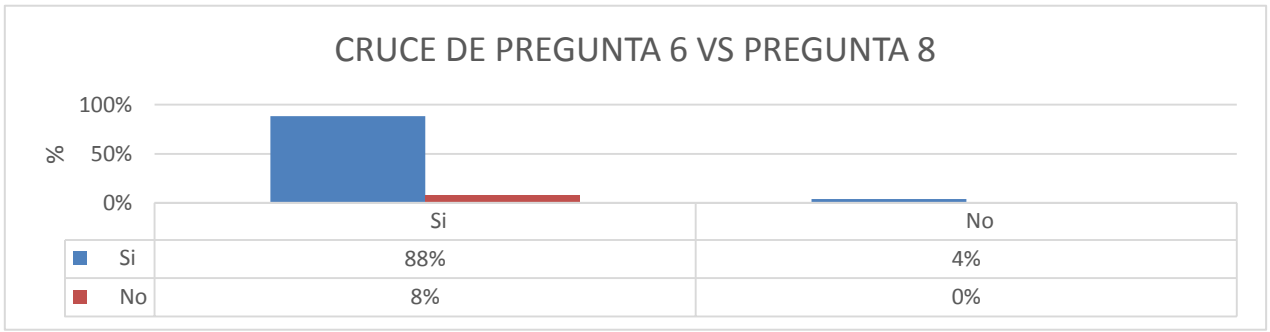
Cruce de pregunta 6 vs pregunta 8

Pregunta 6: ¿Existen controles aplicables al uso del sistema contable computarizado en el lugar en que labora?

Pregunta 8: ¿Considera que es necesario fortalecer la seguridad de la información, a través de una política específica?

Objetivo: Indagar a ceca de la necesidad de fortalecer la seguridad de la información a pesar de la existencia de controles del sistema contable computarizado.

Pregunta 6 \ Pregunta 8	**Si**		**No**		**Total**	
	Fa	**Fr**	**Fa**	**Fr**	**Fa**	**Fr**
Si	23	88%	1	4%	24	92%
No	2	8%	0	0%	2	8%
Totales	**25**	**96%**	**1**	**4%**	**26**	**100%**



Interpretación.

Del total de unidades de análisis, el 88% de los encuestados considera que es necesario fortalecer la seguridad de la información a través de una política específica, además, en este grupo de empresas cuentan con controles internos aplicables al sistema contable computarizado. Esto indica que a pesar de que exista un buen control interno, la seguridad de la información como activo invaluable que es necesita un cuido especifico.

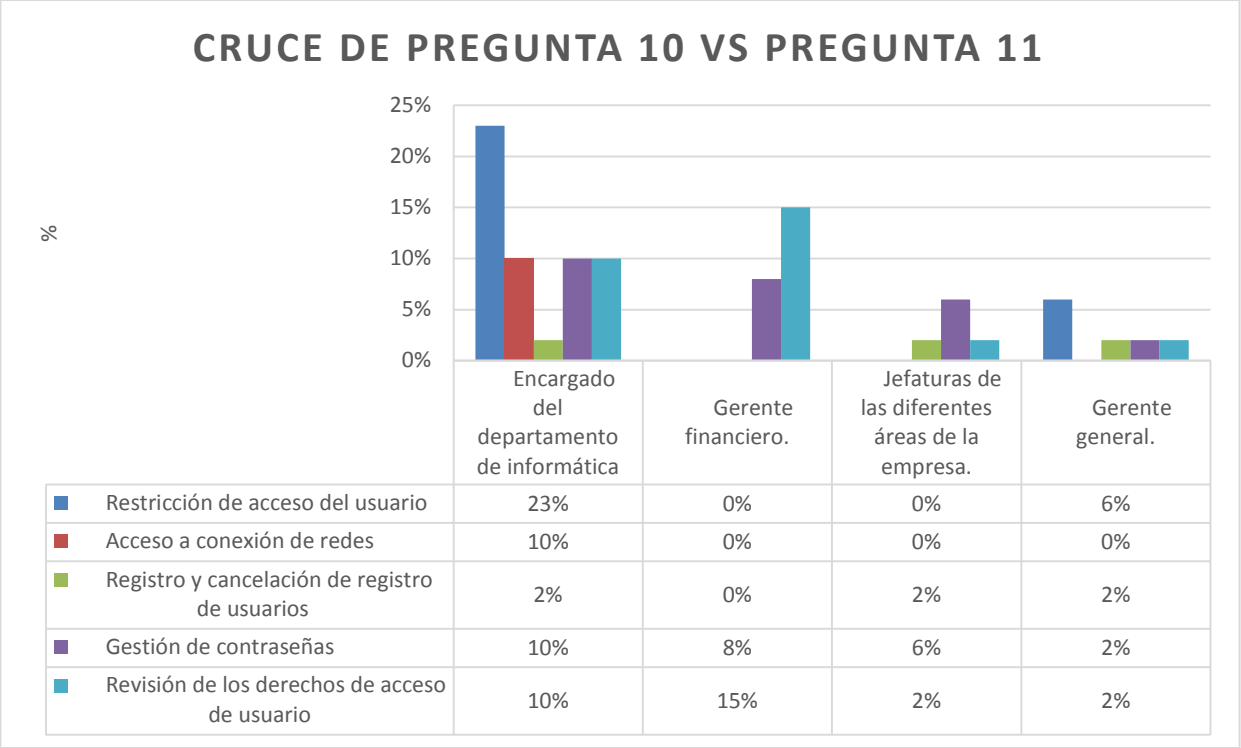
Cruce de pregunta 10 vs pregunta 11

Pregunta 10: Para el área de seguridad lógica, ¿cuál de los siguientes controles de acceso al sistema contable computarizado considera más importante?

Pregunta 11: ¿Quién autoriza los privilegios de acceso a los usuarios del sistema contable computarizado?

Objetivo: Conocer quien autoriza los privilegios de acceso y si realmente los controles de acceso al sistema son importantes para la entidad.

Pregunta 10 \ Pregunta 11	Encargado del departamento de informática		Gerente financiero		Jefaturas de las diferentes áreas de la empresa		Gerente general		Total	
	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr
Restricción de acceso del usuario	9	23%	0	0%	0	0%	2	6%	11	29%
Acceso a conexión de redes	4	10%	0	0%	0	0%	0	0%	4	10%
Registro y cancelación de registro de usuarios	1	2%	0	0%	1	2%	1	2%	3	6%
Gestión de contraseñas	4	10%	3	8%	2	6%	1	2%	10	26%
Revisión de los derechos de acceso de usuario	4	10%	6	15%	1	2%	1	2%	12	29%
Totales	**22**	**55%**	**9**	**23%**	**4**	**10%**	**5**	**12%**	**40**	**100%**



	Encargado del departamento de informática	Gerente financiero.	Jefaturas de las diferentes áreas de la empresa.	Gerente general.
Restricción de acceso del usuario	23%	0%	0%	6%
Acceso a conexión de redes	10%	0%	0%	0%
Registro y cancelación de registro de usuarios	2%	0%	2%	2%
Gestión de contraseñas	10%	8%	6%	2%
Revisión de los derechos de acceso de usuario	10%	15%	2%	2%

Interpretación.

Del total de unidades de análisis se puede determinar que para el 23% de los encuestados la restricción del acceso del usuario es la más importante en la seguridad lógica, a la vez que los accesos son definidos en su mayoría por el encargado de informática con un 55% del total de encuestados.

La revisión de los derechos de acceso representado por el 15% de los encuestados en los que el gerente financiero es quien autoriza los accesos es la segunda más importante. A nivel global esta representa un 29% del total de los encuestados. De esto se puede deducir que la revisión continua de los derechos de acceso permite verificar si estos son suficientes o inadecuados para la persona que los tenga.

A continuación se presentan los cruces de variables realizados para el siguiente indicador: aplicación de controles que aseguren la información de forma física y lógica en las instalaciones de la empresa de tal forma que los usuarios de la información puedan tener seguridad de esta en la toma de decisiones.

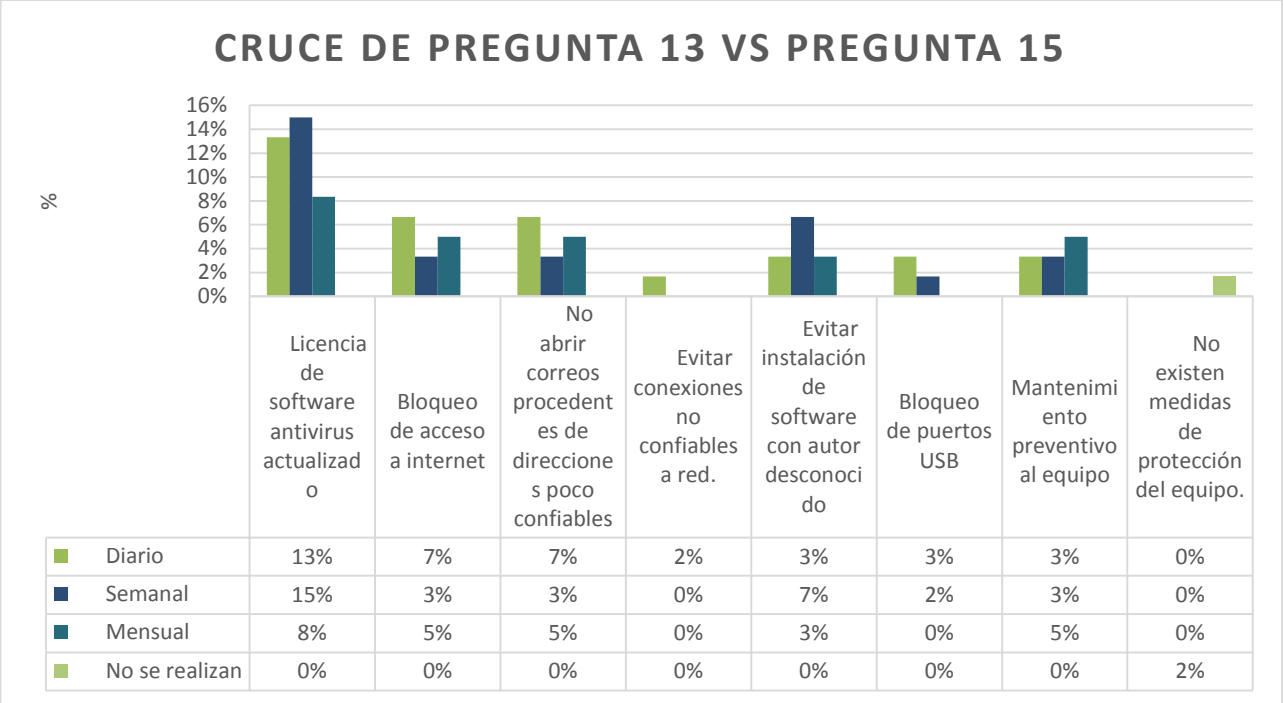
Cruce de pregunta 13 vs pregunta 15

Pregunta 13: ¿Con qué frecuencia se realizan respaldos de la información financiera y contable?

Pregunta 15: Señale las medidas de protección del equipo contra software malicioso que se aplican en la empresa.

Objetivo: Determinar cómo influye la realización de respaldos dependiendo de las medidas de protección del software.

Pregunta 15 \ Pregunta 13	**Diario**		**Semanal**		**Mensual**		**No se realiza**		**Total**	
	Fa	**Fr**	**Fa**	**Fr**	**Fa**	**Fr**	**Fa**	**Fr**	**Fa**	**Fr**
Licencia de software antivirus actualizado	8	13%	9	15%	5	8%	0	0%	22	37%
Bloqueo de acceso a internet	4	7%	2	3%	3	5%	0	0%	9	15%
No abrir correos procedentes de direcciones poco confiables	4	7%	2	3%	3	5%	0	0%	9	15%
Evitar conexiones no confiables a red.	1	2%	0	0%	0	0%	0	0%	1	2%
Evitar instalación de software con autor desconocido	2	3%	4	7%	2	3%	0	0%	8	13%
Bloqueo de puertos USB	2	3%	1	2%	0	0%	0	0%	3	5%
Mantenimiento preventivo al equipo	2	3%	2	3%	3	5%	0	0%	7	12%
No existen medidas de protección del equipo.	0	0%	0	0%	0	0%	1	2%	1	2%
Totales	23	38%	20	33%	16	27%	1	2%	60	100%



	Licencia de software antivirus actualizado	Bloqueo de acceso a internet	No abrir correos procedentes de direcciones poco confiables	Evitar conexiones no confiables a red.	Evitar instalación de software con autor desconocido	Bloqueo de puertos USB	Mantenimiento preventivo al equipo	No existen medidas de protección del equipo.
Diario	13%	7%	7%	2%	3%	3%	3%	0%
Semanal	15%	3%	3%	0%	7%	2%	3%	0%
Mensual	8%	5%	5%	0%	3%	0%	5%	0%
No se realizan	0%	0%	0%	0%	0%	0%	0%	2%

Interpretación.

Del total de encuestados, el 13% elabora respaldos diarios y cuentan únicamente con licencia de antivirus. A pesar de esto también cuentan con otras medidas de protección como los bloqueos a internet con un 7% y no abrir correos de direcciones desconocidas también con un 7%.

La medida de protección más utilizada es la licencia de software antivirus indiferentemente del periodo escogido para realizar los respaldos de la información, representada esta opción con un 36% en total.

3.7.2. Diagnóstico

En las empresas encuestadas se detectó la existencia de políticas diferentes a las contables, siendo la más significativa la existencia de políticas de seguridad de la información, la cual a pesar de que no se le da mucha importancia debido a que las empresas focalizan su atención en otras áreas, la política como tal está presente en las entidades.

A raíz de esto surgen procedimientos de control que las entidades siguen y las jefaturas de las empresas se encargar de hacer valer estos en el sistema contable computarizado pues genera beneficios relacionados a las características de la información, específicamente en la disponibilidad de esta para la toma de decisiones.

También las entidades cuentan con controles de acceso físico a las instalaciones que ayudan a disminuir el riesgo de pérdidas de equipos con información importante de la entidad. Se cuenta con planes de mantenimiento preventivo que ayudan a la duración a nivel de vida útil de los equipos.

En la seguridad lógica la restricción de acceso al usuario es el procedimiento considerado más importante y por el que se debe velar que se le dé el debido cumplimiento y seguimiento a través de la revisión de los derechos de acceso al usuario.

Para enfrentar amenazas que puedan ocasionar daños a la información dentro del software las entidades utilizan como medida de prevención el uso de licencias de software antivirus, el respaldo de la información continuo, bloqueos de acceso a internet, entre otros lo que les permite mantenerse en un margen de seguridad ante amenazas externas que se encuentren en la red o se transmitan a través de dispositivos móviles (USB).

Importante en este ámbito es la capacitación al capital humano desde el momento de su ingreso a la entidad como en el transcurso del tiempo. En este punto atañe el hecho de que solamente se capacita al personal en un curso de inducción inicial, en el cual también se le da a conocer la política de seguridad de la información, la cual solamente se hace en esa ocasión especial.

Las entidades con las respuestas brindadas en las encuestas que se les realizaron consideran que establecer una política para el área de seguridad de la información con sus respectivos controles que integren todos los aspectos relacionados que fortalezcan la continuidad del negocio, la disponibilidad de la información para la toma de decisiones, la integridad de las cifras financieras generadas a través del sistema contable y la confidencialidad de la misma es indispensable.

La importancia de plasmar estas características a través de una herramienta útil y necesaria, basada en un Estándar Internacional como lo es la ISO 27001 es grande y a la vez todo un reto, punto en el cual la referencia la debe hacer el gobierno corporativo de las entidades, puesto que ya existe el control interno dentro de la organización basado en buenos principios y criterios, los cuales verán un salto de la calidad al adoptar un nuevo planteamiento de cómo se deben hacer las cosas de manera adecuada.

CAPÍTULO IV: PROPUESTA

4.1. Planteamiento del caso

Las empresas del sector comercio que se dedican a la venta de productos de telecomunicación demuestran darle importancia a la seguridad de la información a través de controles internos aplicables a esta área. Sin embargo, no se enfoca el esfuerzo requerido debido a que sus controles no están estructurados de manera uniforme para lo que puede significar la pérdida de información sensible de la empresa.

Se identificó que las empresas cuentan con políticas en el área de seguridad de la información, lo cual representa un punto favorable puesto que la alta gerencia tiene presente su importancia para conservar la confiabilidad, integridad y disponibilidad de la información sin embargo el contar con estas políticas de seguridad no garantiza conservar la calidad de la misma, ya que para lograr ésta característica se debe de efectuar un análisis de los aspectos que conllevan el definir controles para el uso del sistema contable computarizado.

Las empresas en estudio determinaron que uno de los beneficios que pueden proporcionar la aplicación de procedimientos de control interno para asegurar la información manejada en el sistema contable computarizado es abordar las amenazas en el contexto de la seguridad de la información a través de medidas de seguridad para evaluar estas condiciones y de esta forma establecer las medidas correctivas que prevén riesgos potenciales.

A través de las evaluaciones internas sobre las amenazas existentes en el contexto de la seguridad de la información, es importante que la gerencia establezca una unidad que dé seguimiento a estas condiciones poco favorables, con el objetivo de proporcionar un mayor grado de cumplimiento de objetivos dentro de la entidad.

Para los controles implementados en asegurar el acceso al sistema contable computarizado se deben de realizar una evaluación para prever riesgos potenciales y conforme se establezcan resultados implementar acciones correctivas.

Esta importancia de las seguridad de la información también retomada por los profesionales de la contabilidad que reconocen y consideren esencial y útil la política de seguridad de la información para obtener cifras contables adecuadas para la toma de decisiones y por ello, según su experiencia laboral, determinaron que disponer de una política de seguridad de la información proporciona una mayor confiabilidad en las cifras de los estados financieros y la necesidad de fortalecer la seguridad de la información, a través de la política específica que aborde controles internos en las áreas que se procesa información para conservar la confidencialidad, integridad y disponibilidad de la información es inherente.

Conocer un modelo de gestión de la seguridad de la información es esencial si se quiere acoplar esto al control interno. Puede servir de guía el tener una noción de lo que se quiere conseguir y como se va conseguir. Punto a favor es que con la investigación de campo realizada, se determinó que la mayoría de los profesionales de la contabilidad encuestados conocen el Estándar Internacional ISO/IEC 27001 y no les sería extraño tomar en consideración un documento basado en este estándar que proporcione una guía adecuada para el resguardo de la información manejada a través del sistema contable computarizado.

4.2. Estructura del plan de solución

El plan de solución se propone una manual de procedimientos de control interno aplicable a la seguridad de la información para sistemas contables computarizados según ISO 27001 en las empresas comercializadoras de productos de telecomunicación en el área Metropolitana de San Salvador, para lo cual se determinaron a través de la estructura organizativa de la empresa AJTecnología, S.A. de C.V., las áreas de mayor interés las cuales son: Seguridad lógica, seguridad física, procesamiento electrónico de datos, recursos humanos, hardware y software. Atendiendo a las necesidades de esta entidad se ha definido procedimientos de control interno los cuales están clasificados por el tipo de control que proporcionan como de: prevención, detección y corrección.

Además para cada procedimiento conforme los roles realizados por los empleados de la entidad se ha descrito la responsabilidad del personal encargado de la seguridad de la información y qué actividades realizará en su cargo, para cada procedimiento se requiere cumplir requisitos formales los cuales se sugieren de manera ilustrativa en los anexos.

4.3. Beneficios y limitantes

4.3.1. Beneficios

La propuesta que se presenta de la investigación pretende abordar el área de seguridad de la información a través de los procedimientos planteados con el fin de dotar a las entidades y a su personal de una herramienta idónea para fortalecer los controles aplicables a la información y su seguridad en el sistema contable computarizado, dándole así la importancia que este activo necesita.

Otro beneficio de la propuesta es asegurar que la información cumpla con sus características principales como lo es la confidencialidad, integridad y disponibilidad de esta al momento de la toma de decisiones. Así como también brindar una guía basada en un Estándar Internacional como lo es la ISO/IEC 27001 con el fin de sustentar los procedimientos propuestos en un documento de gran aceptación en el mundo empresarial.

4.3.2. Limitaciones.

El presente documento solo está enfocado a la adopción de un control interno basado en la ISO/IEC 27001 y solo está dirigido para aquellas personas naturales o jurídicas que busquen una forma de mejorar sus controles de manera adecuada. A pesar de que la ISO/IEC 27001 tiene como premisa la adopción de un Sistema de Gestión de Seguridad de la información, en esta investigación, no se abordó por completo este proceso debido a que iba dirigido a un sector que si bien es cierto ha crecido con el paso del tiempo, la capacidad instalada de las empresas estudiadas no era suficiente para la implementación de un trabajo tan amplio.

Atendiendo a las necesidades que se observaron en la investigación realizada, se vio que un manual de controles internos enfocado a la seguridad de la información era sustancial y necesario en las empresas del sector comercio dedicadas a la venta de productos de telecomunicación. Debido a esto se tomó como referencia la empresa AJTecnologia, S.A. de C.V.

La herramienta que se propone se titula: “El control interno aplicable a seguridad de la información para sistemas contables computarizados según ISO 27001 en empresas comercializadoras de productos de telecomunicación en el área metropolitana de San Salvador” y el desarrollo de los procedimientos se presentan contenidos en el manual siguiente:

4.4. Desarrollo de caso práctico

MANUAL DE PROCEDIMIENTO DE CONTROL INTERNO APLICABLE A LA SEGURIDAD DE LA INFORMACIÓN PARA SISTEMAS CONTABLES COMPUTARIZADOS SEGÚN ISO 27001 EN EMPRESAS COMERCIALIZADORAS DE PRODUCTOS DE TELECOMUNICACIÓN EN EL ÁREA METROPOLITANA DE SAN SALVADOR

Índice

Alcance:

AJTecnología, S.A. de C.V. considera que la información es el activo más valioso, razón por la cual éste manual en que se desarrolla las directrices establecidas para la política de seguridad de la información tomando como referencia lo establecido en el Estándar Internacional ISO 27001 está dirigido para el conocimiento y cumplimiento de las medidas de para las área de mayor interés que incluye: la seguridad física, lógica, hardware, software, recursos humanos y datos, que requieren llevar a cabo por el personal de la entidad para conservar la confidencialidad, integridad de la información que se maneja tanto en el sistema contable computarizado así como también la información almacenada, transferida o procesada de una manera adecuada.

Objetivo:

Establecer los aspectos que integran la política de seguridad de la información en las áreas de mayor interés para asegurar que la información financiera que se maneja en los sistemas contables computarizados sea confidencial, integra y esté disponible en la toma de decisiones de la empresa.

Generalidades de la empresa

La empresa AJTecnología, S.A. de C.V. es una empresa con más de 50 años en el mercado nacional, la cual se desarrolla en el sector comercial dedicado a la venta de productos de la telecomunicación en el interior de El Salvador. Dentro de la gama de productos que ofrece al mercado se encuentran: cámaras de vigilancia, audífonos, teléfonos, alarmas, micrófonos profesionales, accesorios de cámara, cables y fibras óptica, cableado estructurado, protectores para voltaje, entre otros.

Organización interna

La empresa tiene establecido las jerarquías para la toma de decisiones, como máxima autoridad se define el gerente general el cual aprueba todas las transacciones y actividades del entorno del negocio, posteriormente se encuentran integrados los departamentos de:

- **Gerencia financiera:** integrada por el contador general y auxiliar.
- **Gerencia de ventas:** el cual la integran el gerente de ventas, asistente de ventas, vendedores.
- **Departamento de soporte técnico:** el cual está integrado por el personal que proporciona la asistencia técnica a los clientes.
- **Departamento de informática:** el cual está integrado por el jefe de TI, y dos asistentes de informática.
- **Departamento de recursos humanos:** el cual forma parte el jefe de recursos humanos y dos personas encargados de planilla.
- **Departamento de compras:** conformado por una persona encargada.
- **Departamento de créditos**: integrado por una persona encargada de cobros.

Liderazgo y compromiso de la dirección

Uno de los principios definidos dentro de la empresa es el compromiso de la dirección para liderar las buenas prácticas en cuento al cumplimiento de las políticas internas establecidas, así como también apoyar al personal dotándolos de las herramientas necesarias como: capacitaciones y asignación de recursos técnicos para que desarrollen sus actividades de manera que agreguen valor a la entidad en todos sus aspectos y en todas sus áreas de importancia.

Procedimientos de control

Área: Seguridad lógica

Alcance y campo de aplicación: Definir los requerimientos a considerar con respecto a la seguridad lógica la cual implica asegurar el acceso autorizado a los sistemas a través de la implementación de una política, objetivos y controles que den respuesta a los riesgos asociados

Objetivo de la política: Limitar el acceso a la información para lograr conservar la confidencialidad, integridad y disponibilidad de la información, que permitan proporcionar un nivel de confianza para la toma de decisiones.

Procedimiento	Control	Tipo de control	Formato a usar
Gestión de control de acceso	El gerente general debe de reunirse con el contador general, y los jefes de departamentos para clasificar la información que se maneja en cada área y posteriormente asignarle el nivel de seguridad que se debe de proporcionar a través de medidas de seguridad a considerar.	Preventivo	-
	Para el análisis de clasificar la información con respecto al manejo, procesamiento y almacenamiento de la misma tanto de forma física como digital, se realizará a nivel de jerarquía, en segundo lugar se tomará como base las áreas según el organigrama y posteriormente se considerará el cargo y roles desempeñados por los usuarios.	Preventivo	-
	El gerente general debe de convocar al contador público y el departamento de informática para limitar los accesos a los datos que se manejan en el sistema, según la clasificación de la misma.	Preventivo	-
	La clave del administrador del sistema estará bajo la custodia del jefe de informática, el cual asignará el acceso al sistema contable computarizado siempre y cuando se haya completado el procedimiento de solicitud de acceso, establecido en los procedimientos de administración de acceso.	Preventivo	Anexo N°1
Acceso a redes y servicios de red	El jefe de informática debe de tener identificadas la red segura a través de un listado de las redes existentes y que dispositivos se conectan con cada red.	Preventivo	-

Procedimiento	Control	Tipo de control	Formato a usar
Acceso a redes y servicios de red	El encargado de realizar la supervisión de los equipos debe de configurar los equipos de manera que se bloque el acceso a redes desconocidas, así como también los dispositivos deben de estar configurados de tal manera que se alerte al área de informática cuando exista alguna anomalía.	Preventivo	-
	Para el bloqueo de redes desconocidas, se deben de utilizar protocolos de cifrado de datos para los estándares *Wi-fi* como el WEP y el WPA, como medida de seguridad a la red.	Preventivo	-
	Para detectar anomalías en la red se deberá contar con mecanismos como sistema de detección de intrusiones internos y externos o tener habilitado el firewall, así como también se deberá de verificar la configuración de software antivirus para la detección de redes no autorizadas, así como también sitios web desconocidos y bloquear accesos a redes sociales.	Preventivo	-
Administración de acceso a los usuarios	Monitorear el uso de servicios de red por lo menos una vez al mes para detectar la conexión de elementos no autorizados y que los mismos usuarios no se conecten a otra red que no sea segura.	Detección	-
	El gerente general debe de aprobar el registro y cancelación de usuarios a través de solicitudes de acceso al sistema solicitados por los jefes inmediatos.	Preventivo	Anexo N°1
	Para cada usuario gerencia general, el contador general y el jefe de informática deben de definir las acciones particulares a las que accederá cada usuario en lectura, escritura, eliminación y ejecución, así como también limitar la información contenida en el sistema.	Preventivo	-
	Al realizar algún cambio interno de ascenso, descenso o cese de empleo se debe de comunicar a gerencia general, al contador y el jefe de informática para revisar los derechos de acceso de los usuarios.	Preventivo	Anexo N°1

Procedimiento	Control	Tipo de control	Formato a usar
Administración de acceso a los usuarios	Gerencia general debe de solicitar el cambio de contraseñas a los usuarios por lo menos una vez cada dos meses, para conservar la calidad de las contraseñas o en casos particulares que sea necesario. Esta solicitud se realizará a través de correo electrónico.	Preventivo	-
	El encargado de monitorear los accesos otorgados deberá de revisar los derechos de acceso de los usuarios,	Detección	-
	Se deberá de programar una rutina mensual de supervisión de actividades realizadas por los usuarios, para detectar irregularidades y/o errores.	Detección	-
	En dado caso se encuentren irregularidades y/o errores, se deberá de comunicar con gerencia general para que gire instrucciones en el bloqueo de accesos no autorizados, amonestando de forma verbal al empleado	Correctivo	-
	En el contrato de los empleados debe de incluir los términos y las condiciones de empleo según el área, el rol que el nuevo empleado realizará, la responsabilidad de sus acciones y las sanciones a tomar en caso de incumplimiento del contrato laboral. Así como también deben de comprometerse al cumplimiento del contrato de confidencialidad.	Preventivo	-
	El contrato con los proveedores de internet o servicios externos, así como también con los clientes debe de contener cláusulas de confidencialidad.	Preventivo	
	En el proceso de inducción los empleados se les deben de definir los requerimientos de autenticidad de los usuarios para hacer uso del sistema.	Preventivo	-
	Cuando se otorgue los derechos de acceso a un usuario al sistema con contraseña provisional, debe de cambiar la contraseña inmediatamente.	Preventivo	-

Procedimiento	Control	Tipo de control	Formato a usar
Administración de acceso a los usuarios	El jefe de informática debe de solicitar que la nueva contraseña sea fácil de recordar, no sea vulnerable en el número de caracteres y que se la contraseña seleccionada contenta una longitud mínima.	Preventivo	-
	Se deberá llevar una bitácora de registro de los usuarios que accedan al sistema contable computarizado, la cual contenta: usuario, fecha de acceso, hora, acción a realizar, número de visitas realizadas, errores de sistema.	Preventivo	
	El jefe inmediato de cada área debe de comunicar a través de correo electrónico al departamento de informática con copia a gerencia general solicitando que se deshabilite o elimine el usuario que abandone su puesto de trabajo, así como también se debe de indicar al resto de empleados que no compartan información con la persona que se retira.	Preventivo	-
	Comunicar a los empleados la restricción en el envío de información a correos electrónicos no protegidos.	Preventivo	-
	Informar al personal que la administración del usuario en el sistema es individual y que debe de ser responsable de su uso.	Preventivo	-
	Los usuarios que tengan acceso a puntos claves de la información se proporcionarán una autenticación adicional con claves criptográficas.	Preventivo	-
	Se tendrá un acceso de dominio en los equipos de la empresa, lo que implica que los archivo elaborados en las computadoras de la entidad solo podrán ser utilizados en las maquinas del domino.	Preventivo	-
	La gerencia debe de asignar a un responsable para que realice actividades de revisar los derechos de acceso de los usuarios una vez al mes.	Detección	-

Procedimiento	Control	Tipo de control	Formato a usar
Despidos o Cambios de responsabilidad en el empleo	Cuando se realice cese de empleo el jefe inmediato del personal debe de comunicar al departamento de recursos humanos y a gerencia general para notificar la desvinculación labora, a través de una acción de personal el cual contendrá la fecha de cese de labores, cargo y razón o comentario del porqué se realiza el despido. Además, el jefe de informática deberá de recibir el equipo utilizado por el empleado, y verificar las condiciones del mismo por medio de una *lista de chequeo*, para determinar si existen daños a los equipos asignados. Si existiera algún daño se cuantificará el daño y será descontado en la liquidación laboral.	Preventivo	Anexo N°9
	Cuando exista un ascenso laboral, éste debe de ser autorizado por gerencia general, posteriormente se definirá junto con el jefe de informática y el contador general la asignación de privilegios a realizar en el sistema contable computarizado, auxiliándose del manual de puestos definido por recursos humanos.	Preventivo	
	Para la asignación de recursos o herramientas a los empleados que se ha ascendido o descendido, se deberá de llenar un formato en donde se enliste el equipo asignado, definiendo las responsabilidades de conservar la confidencialidad, integridad y disponibilidad de la información.	Preventivo	
	El encargado de TI debe de verificar que los accesos solicitados para los usuarios sean adecuados para el rol a desempeñar, para el caso que se otorguen accesos privilegiados a los usuarios se deberá definir los requisitos para mantener dichos privilegios y fecha de vencimiento de los mismos.	Preventivo	Anexo N°1
	En el proceso de monitoreo de los accesos otorgados se debe de evaluar las competencias de los usuarios con derechos de acceso privilegiado para verificar el cumplimiento de los requisitos solicitados al momento de otorgarlos.	Detección	-

Procedimiento	Control	Tipo de control	Formato a usar
Responsabilidad de los usuarios	Comunicar al usuario las responsabilidades asignadas para mantener la información de autenticación secreta.	Preventivo	-
	Realizar una divulgación de política de control de acceso por lo menos una vez al mes por medio de correos electrónicos recordando dichas responsabilidades.	Preventivo	-
Control de acceso al sistema	En los requisitos de acceso al sistema debe de solicitar la verificación de autenticidad de usuario antes de proporcionar información.	Preventivo	-
	En caso de incumplimiento a lo establecido en los procedimientos de control de acceso primeramente se hará un llamado de atención de forma verbal se conversará con el empleado para que conozca las consecuencias de sus actos, si vuelve a incumplir se redactará una acción de personal de forma escrita, y la tercera vez se dará de baja al empleado	Correctivo	-
Respaldo	Se realizan respaldos de manera sistemática y automática a través de un software gratuito que proporciona las herramientas idóneas para salva guardar información sensible en caso de pérdida o falla del sistema.	Preventivo	-
	El jefe de informática se encargará de revisar la capacidad de los dispositivos de almacenamiento por equipo de manera que se asegure un adecuado resguardo de la información digital. Para el caso de información física el encargado de resguardar la información será cada jefe inmediato por departamento.	Preventivo	-
	El jefe de informática se asegurará que los respaldos realizados por los usuarios, sean útiles y estén disponibles para consultas.	Detección	-
	Todas las copias de información se resguardarán en un área adecuada que conserve la calidad de la misma y proporcionar un control de acceso únicamente por el jefe de informática.	Preventivo	-
	En caso de que exista restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información.	Preventivo	-

Procedimiento	Control	Tipo de control	Formato a usar
	Cada usuario del sistema contable computarizad es responsable de realizar los respaldos, en caso de presentarse inconvenientes en este proceso, se debe solicitar el apoyo del encargado de informática para verificar que se realice de forma adecuada.	Preventivo	-
	El jefe de informática verificará que se mantenga un archivo actualizado de las copias de respaldo de la información sensible.	Preventivo	-
	El jefe de informática verificará la correcta ejecución de los respaldos de la información realizando una revisión de las mismas para confirmar que estén disponibles.	Detección	-
	El lapso para realizar respaldo está determinado por las áreas que utilizan el sistema, para usuarios gerenciales se ejecutan automáticamente cada dos días y para el resto de usuarios cada semana.	Preventivo	-
	Del sistema contable en general se realizan respaldos semanales y mensuales los cuales se almacenan en discos duros adecuados que responden contra fallas.	Preventivo	-
	Se dispondrá de una bitácora de control en la que se verifique si realmente los respaldos han sido realizados según las programaciones parametrizadas.	Detección	
	El acceso físico a los respaldos se debe limitar. De manera que el resguardo únicamente acceda el encargado de informática y gerencia general.	Preventivo	
	Periódicamente se realizarán actividades para probar que realmente los respaldos estarán disponibles y serán funcionales al momento de una emergencia. Este punto será ejecutado por el jefe de informática.	Detección	
Transferencia y manejo de la información	El servidor de correo está configurado de tal manera que no permita la transferencia de archivos de distintas extensiones a direcciones de correo que no estén bajo el dominio de la empresa.	Preventivo	-
	El sistema de información provee un logs de actividades en el cual se puede verificar el historial de las actividades realizadas por los usuarios y determinar la existencia de anomalías y accesos no autorizados	Preventivo	-

Área: Software

Alcance y campo de aplicación: Identificar los requerimientos establecidos por el Estándar Internacional ISO 27001 para establecer, implementar, mantener y mejorar la seguridad de la información atendiendo los objetivos y necesidades con el fin de asegurar la información en el área de software de las empresas dedicadas a la venta de productos de la telecomunicación.

Objetivo de la política: Lograr el uso adecuado del software proporcionado a los usuarios que permita conservar la confidencialidad, integridad y disponibilidad de la información que se maneta a través del software utilizado por la empresa.

Procedimiento	Control	Tipo de control	Formato a usar
Adquisición de licencia de Software	El gerente general autorizará la adquisición de licencia de software, la cual será gestionada por el personal de compras para proponer a gerencia general la mejor opción de software según las necesidades de la entidad.	Preventivo	-
	Para la selección del software se deberá de considerar las condiciones y capacidad del hardware y la compatibilidad de los mismos para la instalación de este en los equipos informáticos.	Preventivo	-
	Cuando se seleccione al proveedor del software, se realizará un contrato en el cual se debe de establecer las condiciones de servicio incluyendo cláusulas de mantenimiento, consultoría, capacitación de los usuarios, pruebas del mismo, responsabilidades del proveedor y de la empresa.	Preventivo	-
	Toda adquisición de software que deba ser conectado a la red de la empresa, deberá de gestionarse con el jefe de informática y posteriormente ser aprobado por gerencia general.	Preventivo	-
	El jefe de informática deberá de gestionar que se guarde una copia del software adquirido como medida de seguridad del servicio, además se deberá de solicitar al proveedor un manual de usuario del software adquirido.	Preventivo	-

Procedimiento	Control	Tipo de control	Formato a usar
Pruebas de software	El jefe de informática deberá de velar porque se realicen las pruebas necesarias del software antes de difundir el mismo por los equipos de la empresa.	Preventivo	-
	Las pruebas realizadas al software deberán de registrarse a través de archivos físicos o digitales, desarrollando una breve descripción de las condiciones encontradas al realizar las pruebas del software.	Detección	-
	Para la verificación de los procesos, el jefe de informática deberá de verificar los mismos junto con los usuarios asignados para cada módulo del software.	Preventivo	-
	El jefe de informática será el encargado de instalar el software en los dispositivos requeridos y será el responsable las licencias obtenidas estén actualizadas para hacer uso del software.	Preventivo	-
	El jefe de informática deberá configurar el equipo informático de manera que él sea el único usuario administrador que tenga la autorización de instalar o desinstalar software a los equipos	Preventivo	-
	En el caso que se cambie de software, se deberán disponer de las versiones del software por el que se sustituirá, para consultar la información.	Preventivo	-
Inicio de sesión seguro	La configuración del sistema debe de estar parametrizado para no mostrar identificadores del sistema hasta que haya finalizado el inicio de sesión, no proporcionar ayuda durante el proceso de inicio de sesión.	Preventivo	-
	En el caso que los usuarios coloquen datos incorrectos la iniciar sesión no se debería de mostrar una pista de los elementos correctos.	Preventivo	-
	El software deberá de limitar a tres los intentos permitidos como máximo de errores en inicio de sesión.	Preventivo	-
	Si se intenta ingresar a un usuario con claves incorrectas inmediatamente se deberá de bloquear el acceso y alertar al departamento de informática.	Detección	-
	Si el departamento de informática identifica el intento forzoso de accesos no autorizados deberá comunicar al gerente general para que éste autorice el desbloqueo del usuario.	Detección	-

Procedimiento	Control	Tipo de control	Formato a usar
Inicio de sesión seguro	El jefe del departamento de informática se encargará de llevar una bitácora de registro de accesos no autorizados en donde se establezca: Fecha, hora del inicio de sesión correcto anteriormente, detalle de intentos fallidos, usuario bloqueado, fecha de autorización de desbloqueo de usuario.	Preventivo	Anexo N°2
Actualizaciones	Para realizar una actualización se deberá de identificar a detalle las modificaciones que se tendrán al actualizar.	Preventivo	-
	Contactarse con el proveedor del software para fines de soporte técnico para realizar las consultas necesarias.	Preventivo	-
	Solicitar a gerencia general la autorización para ejecutar las actualizaciones requeridas por el software	Preventivo	-
	Se realizan actualizaciones continuas del sistema de información utilizando una nube para salvaguardar la información según las necesidades requeridas.	Preventivo	-
	Se debería de disponer de bitácoras que detallen las actualizaciones realizadas, así mismo se deberá de tener el registro de las modificaciones realizadas al software.	Preventivo	Anexo N°3
	El encargado de TI deberá realizar mantener archivos sobre las versiones anteriores del software.	Preventivo	-
	Se deberá de disponer de un manual físico y/o en línea de los módulos existentes del software que detallen las opciones contenidas en el menú con sus especificaciones necesarias.	Preventivo	-
Software de protección	El mantenimiento que se les dará a los equipos deberá de incluir la revisión de software antivirus, como tipo de mantenimiento, verificando la fecha de activación, fecha de caducidad, Vigencia de licencia del producto, y configurar para que éste no sea desactivado por los usuarios.	Detección	Anexo N°4

Área: Seguridad física

Alcance y campo de aplicación: Definir requerimientos a considerar para el cumplimiento de la ISO 27001 con respecto a la seguridad física los cuales implica mantener áreas seguras y protección de equipo además, especifica los aspectos importantes para establecer política, objetivos y controles para conservar la confidencialidad, integridad y disponibilidad de la información.

Objetivos de la política: Determinar las directrices adecuadas para el correcto control de aseguramiento de los equipos en los que se procesa la información de la empresa.

Procedimiento	Control	Tipo de control	Formato a usar
Seguridad de los dispositivos móviles de la entidad.	Inventario de dispositivos móviles el cual debe llevar el auxiliar del departamento de informática.	Preventivo	Anexo N°5
	Brindar los utensilios adecuados para la protección física del equipo, esto lo tendrá que gestionar el jefe de informática junto al área de compras.	Preventivo	Anexo N°6
	Restringir la instalación de software no autorizado. El departamento de informática debe contar con un listado de programas que pueden utilizarse según las necesidades de cada área de la empresa.	Preventivo	-
	Controlar el acceso a los diferentes dispositivos móviles a través de una contraseña segura.	Preventivo	-
	Cifrado de la información contenida en los dispositivos. El acceso remoto debe supervisarse en el momento que se realiza.	Detección	-
	Realizar respaldos de la información de forma continua en caso de falla o error de los equipos.	Preventivo	-

Procedimiento	Control	Tipo de control	Formato a usar
Establecer responsables de la administración de los activos y su protección.	De forma anual, el jefe del departamento de informática deberá realizar un inventario físico de los activos relacionados a la información de la empresa.	Preventivo	Anexo N°7
	Este inventario se debe comparar con los activos fijos reconocidos por el área de contabilidad y establecer la existencia de diferencias entre ambas partes.	Detección	
	El auxiliar del departamento de informática llevará un control sobre la propiedad de los activos. Determinando el estado en que este se encuentra en cada una de las revisiones o inventarios realizadas.	Detección	
	El jefe del departamento de informática establecerá las directrices de uso adecuado de los activos, esto implica si estos pueden retirarse de la entidad y el procedimiento a seguir para autorizar esto.	Preventivo	
	Al finalizar la relación laboral, el empleado deberá devolver los insumos prestados para realizar su trabajo. El auxiliar de informática en conjunto con el jefe de recursos humanos, deberá recibir y hacer constar que el equipo devuelto está en buenas condiciones y que su deterioro ha sido sólo por el uso continuo.	Detección	
Clasificar y resguardar adecuadamente la información dentro de la entidad.	La información impresa se clasificará en términos de requisitos legales, técnicos, valor comercial y sensibilidad de la misma. Esto lo realizará el auxiliar contable encargado de archivar la información. La clasificación deberá basarse en cuatro puntos: a) información accesible para todos, b) información resguardada para el área comercial, c) información accesible sólo para el departamento de contabilidad y por último d) información accesible solamente con autorización de gerencia general.	Preventivo	
	El auxiliar contable encargado de archivar la información etiquetará oportunamente la misma, con el fin de que sea fácil la obtención de documentos en específico en un momento determinado. En caso de que la información sea digital, el auxiliar de informática deberá etiquetar las carpetas en las que se guarden de forma que sea entendible y fácil de localizar.	Detección	

Procedimiento	Control	Tipo de control	Formato a usar
Determinar el correcto uso y manejo de los activos de la entidad.	La documentación se debe resguardar en un lugar seguro con acceso limitado, acceso que primordialmente solo tendrá el departamento de contabilidad, y dependiendo de la información solicitada se le dará acceso. Dicho acceso lo deberá autorizar la gerencia financiera o el contador general.	Preventivo	
Adecuado manejo de los medios de resguardo de la información.	La información utilizada en medios como dispositivos móviles, deberá estar encriptada. Esta acción la deberá realizar el jefe del departamento de informática.	Preventivo	
	La información importante se almacenará en discos duros. A su vez, deberá mantenerse un respaldo adicional en caso de pérdida de la información en uno de los discos principales. Esta acción debe ser monitoreada por el jefe del departamento de informática.	Preventivo	
	En caso de que sea necesario extraer información de los respaldos o medios de la empresa, se deberá hacer única y exclusivamente en medios que sean proporcionados por la entidad los cuales, estén debidamente identificados. Este control será llevado por el auxiliar del departamento de informática.	Preventivo	
	La extracción de información de las bases de datos de la empresa deberá realizarse previa autorización. Si es información a disponibilidad de la persona, previa autorización del departamento de informática siempre y cuando justifiquen el fin. Si es información sensible, la autorización será difundida por gerencia financiera y si la información es confidencial o sumamente importante, única y exclusivamente será autorizada por gerencia general.	Preventivo	
Perímetros de seguridad.	El encargado de servicios verificará la existencia de perímetros establecidos en los cuales las instalaciones se mantengan en buen estado a fin de alertar un desastre natural. Esto se realizará a través de una inspección física en el área de procesamiento de información y en la que esta resguardado el servidor.	Detección	

Procedimiento	Control	Tipo de control	Formato a usar
Perímetros de seguridad.	Las visititas deberán ser atendidas en el área de recepción en la cual, no se les dará acceso a las estaciones salvo autorización de gerencia general. El personal de la entidad tendrá su acceso a las instalaciones en el área de bodega y este será permitido por el vigilante de turno verificando que el empleado este haciendo uso de su carnet de identificación de la entidad.	Preventivo	
	Deberá existir un control de acceso en el cual solo pueda acceder el personal empleado de la empresa. Este control de acceso, deberá ser actualizado por recursos humanos cada vez que ingrese o se retire personal de la entidad.	Preventivo	
	Existencia de un sistema de alarmas, señalización de rutas de evacuación y alarmas de incendio, extintores en lugares adecuados y de importancia. Son parámetros de seguridad por las que el encargado de servicios generales deberá velar con el fin de resguardar la información de las áreas importantes en caso de que sucediera un siniestro.	Preventivo	
Controles de entrada físicos.	Existencia de bitácora de registros de entradas y salidas de visitas a las instalaciones. Se identificará a la persona solicitando un documento de identidad con foto. La bitácora al final del día será enviada a gerencia general para su revisión.	Detección	Anexo N°8
	Se protegerá el acceso a áreas importantes de la entidad a través de tarjetas de acceso y en casos especiales como: el acceso a bodegas o salas de reunión privadas, sólo se accederá con la tarjeta de acceso y la huella dactilar de la persona autorizada. Esta autorización será establecida por recursos humanos dependiendo al área en la que se desarrolle el empleado.	Preventivo	
	El departamento de informática será el encargado de verificar los accesos de personas ajenas a la empresa y de llevar una bitácora de estos. Esta será trasladada a gerencia general al final del día.	Detección	
	Todo el personal de la empresa ya sea empleado o subcontrata deberá portar el gafete que lo acredita como miembro de la empresa de forma visible. Recursos humanos deberá velar por el cumplimiento de esta directriz y en caso contrario se sancionará con acciones de personal.	Preventivo	

Procedimiento	Control	Tipo de control	Formato a usar
Protección de oficinas, salas de reuniones e instalaciones en general.	Los accesos a lugares restringidos estarán resguardados por controles de acceso dactilares y con tarjeta de acceso. Estos accesos serán determinados por recursos humanos.	Preventivo	
	Los contactos internos como externos de la empresa sólo estarán a disposición del personal empresarial. En ningún caso, esta información deberá salir de las instalaciones de la entidad. Recursos humanos proporcionará información actualizada y velará porque ésta información se mantenga dentro de la entidad.	Preventivo	
Seguridad en las áreas de entrega y carga	Restricción de acceso a las áreas de entrega y carga de personal no autorizado y ajeno a la empresa. Esto lo velará el personal de vigilancia.	Preventivo	

Área: Hardware

Alcance y campo de aplicación: Identificación de los requerimientos establecidos por el Estándar Internacional ISO 27001 para establecer, implementar, mantener y mejorar la seguridad de la información atendiendo los objetivos y necesidades con el fin de asegurar la información en el área de hardware.

Objetivos de la política: Implementar la protección adecuada contra fallas o errores en el hardware de los equipos que almacenan información sensible de la entidad.

Procedimiento	Control	Tipo de control	Formato a usar
Adquisición de hardware	Los equipos que se adquieran para uso informático y como política interna de compra marca HP.	Preventivo	-
	El jefe de informática a través de la *lista de chequeo* de equipos se determina la necesidad de comprar nuevo hardware.	Preventivo	-
	El jefe de informática solicita que el jefe inmediato del departamento realice una solicitud de compra, para poder gestionar la compra del mismo a través del departamento de compra, posteriormente se solicita la autorización del gerente general para su aprobación.	Preventivo	-
	Cuando se recibe el hardware, el jefe de informática recibe lo solicitado y revisa la calidad del hardware, garantía del mismo, procede a codificar el equipo, asignar responsable, y gestionar los controles para la entrega del mismo. En caso de que exista inconformidades en la compra se solicita el cambio con el proveedor.	Preventivo	-
Protección de equipos informáticos.	Los equipos de procesamiento de información deberán estar ubicados en zonas resguardadas del acceso no autorizado de personas externas de la entidad. La ubicación del equipo deberá estar supervisada por el departamento de informática.	Preventivo	
	El servidor deberá estar ubicado en un lugar en el que pueda ser monitoreado el acceso. El personal de informática es el único que tiene acceso libre y la potestad para brindar acceso a personas externas del área.	Preventivo	

Procedimiento	Control	Tipo de control	Formato a usar
Protección de equipos informáticos.	El servidor deberá estar con las protecciones pertinentes. Se deberá mantener una temperatura adecuada y cerca de la misma deberá ubicarse un extintor en caso de siniestro y con el fin de no perder información sensible para la empresa. El departamento de informática velará por el cumplimiento de estas directrices.	Preventivo	
	Comer, beber o fumar cerca de los equipos de procesamiento de información estará prohibido. Esta directriz velará por que se cumpla el departamento de recursos humanos.	Detección	
Servicios básicos de apoyo y mantenimiento del equipo.	Existirá una planta eléctrica provisional la cual permitirá el resguardo de la información en caso de fallas en los servicios eléctricos. El encargado de servicios generales velará que esta planta esté en buen funcionamiento y documentará esta supervisión.	Preventivo	
Seguridad del cableado del equipo informático y de telecomunicación.	Los cables de electricidad y de comunicaciones deberán estar enterrados o debidamente cubiertos con canaletas con el fin de que no sean de fácil acceso.	Preventivo	
	Evitar interferencias en la comunicación separando los cables eléctricos de los cables de telefonía.	Preventivo	
Mantenimiento preventivo y correctivo de los equipos	Los equipos en los que se procesa información deberán estar debidamente conservados, de esto se debe encargar el auxiliar de informática de la revisión de que los equipos funciones acorde a las necesidades.	Preventivo	
	Las reparaciones y mantenimiento de los equipos sólo lo podrán realizar el personal del departamento de informática o algún experto que sea autorizado por los mismos para realizar alguna revisión preventiva o correctiva de los equipos.	Preventivo	
	El auxiliar de informática, tendrá una bitácora en la que resguardará los incidentes por fallas o errores en los equipos en la cual consigne: fecha del incidente, descripción del incidente, gravedad, departamento, persona que tiene asignado el equipo y la recomendación respectiva. Esta bitácora será trasladada a final de semana al jefe del departamento de informática.	Detección	

Procedimiento	Control	Tipo de control	Formato a usar
Mantenimiento preventivo y correctivo de los equipos	Deberá existir una calendarización de los mantenimientos a realizar y quien los ejecutará. Esta calendarización deberá enviarse de forma oportuna a todo el personal involucrado. Esta acción será realizada por el auxiliar de informática.	Preventivo	
	Una vez ejecutado el mantenimiento de los equipos, la persona que realice el mismo deberá asegurarse que el equipo funciona correctamente y no presenta fallas.	Detección	
Seguridad de los equipos fuera de las instalaciones de la empresa.	Los equipos que gerencia general autorice utilizarlo fuera de las instalaciones. En la autorización deberá establecerse el código del equipo, modelo, marca, número de serie y tiempo que se tendrá afuera de la empresa, encargado del mismo, firma del responsable.	Detección	
	Fuera de las instalaciones la persona encargada del equipo no deberá dejar estos sin supervisión en lugares públicos.	Preventivo	
	En caso de que se ceda la posesión del equipo fuera de las instalaciones, se deberá documentar el traspaso de la cesión de la responsabilidad. Este traspaso deberá ser informado oportunamente a la jefa de recursos humanos.	Preventivo	
Retiro de activos	Para retirar los equipos informáticos del sitio en el que se encuentra ubicados, se realizará con previa autorización de gerencia general y del jefe de informática.	Preventivo	
	El jefe de informática verificará que se dé cumplimiento al tiempo establecido para el retiro de los activos y el retorno de los equipos a su lugar.	Detección	
	Se deberá de documentar el retiro de los activos identificando, la persona responsable del activo, fecha de retiro y retorno del mismo, así como también el lugar de donde se retira y donde ingresa.	Preventivo	
Eliminación o reutilización de equipos	El jefe de informática es responsable de verificar todos los equipos que contengan información almacenada sea extraída y salvaguardada, antes de eliminar o reutilizar los equipos.	Preventivo	
	En el caso que los equipos sean reasignados, el jefe de informática extraerá y realizará un resguardo de la información extraída y verificará que el software con licencia se haya extraído o se haya sobrescrito de manera segura.	Preventivo	

Procedimiento	Control	Tipo de control	Formato a usar
Eliminación o reutilización de equipos	Para los equipos que almacenan información confidencial, éstos se destruirán físicamente o la información contenida en los mismos se deberá de destruir, eliminar o sobrescribir de manera que no se pueda recuperar a través del software *Eraser*, el cual el único autorizado para realizar estas actividades es el jefe de informática con previa autorización de gerencia general y el usuario del mismo.	Preventivo	
Escritorios y pantallas despejadas	El personal responsable de las computadoras deberá bloquear la pantalla de su computador cuando no estén utilizando el equipo o cuando se retiren de su lugar trabajo.	Preventivo	
	El personal deberá ser responsable de mantener su escritorio libre de documentos confidenciales que se encuentren sin custodia.	Preventivo	
Chatarra electrónica	Para los equipos que almacenen información confidencial serán destruidos físicamente, en el caso de discos duros se utiliza utensilios pesados para la destrucción definitiva.	Preventivo	
	Dentro de las chatarras electrónicas clasificadas por la empresa se enlista: refrigeradores, aires acondicionados, electrodomésticos en general, equipos de informática y telecomunicaciones, aparatos de alumbrado, herramientas eléctricas.	Preventivo	
	Antes de clasificar los activos como chatarra electrónica, previamente se realiza una inspección con especialistas si es viable la reparación de los mismos.	Preventivo	
	La empresa como parte de su política de responsabilidad social, ha establecido un sistema de reciclaje de sus propios productos y cada tres meses, son entregados a empresas encargadas de recibir desechos electrónicos.	Preventivo	

Área: Recursos humanos

Alcance y campo de aplicación: Establece los requerimientos según el Estándar Internacional ISO 27001 para establecer, implementar, mantener y mejorar la seguridad de la información atendiendo los objetivos y necesidades en el área de recursos humanos en las empresas dedicadas a la venta de productos de la telecomunicación, asociados a conservar la confidencialidad, integridad y disponibilidad de la información

Objetivo de la política: Garantizar que los procedimientos para la selección de los empleados, los términos y condiciones del empleo sea cumplan durante el empleo.

Procedimiento	Control	Tipo de control	Formato a usar
Selección	Gerencia general debe de definir las plazas que se ofertarán considerando el puesto, las competencias requeridas.	Preventivo	-
	Se debe de definir las áreas a las que tendrá acceso el postulante.	Preventivo	-
	El jefe del departamento de recursos humanos debe de verificar la información citada en el curriculum vitae de los postulantes, a través de confirmaciones de las referencias laborales y familiares del mismo. Así como también la identificación según el Documentos de identidad, antecedentes penales y la verificar el grado académico según títulos o calificaciones académicas, para puestos claves.	Preventivo	-
	La empresa debe de cumplir con la legislación necesaria para realizar la selección de los empleados.	Preventivo	-
	Se realiza una entrevista con los postulantes para realizar una prueba diagnóstica de los conocimientos.	Preventivo	-
	El gerente general es el encargado de seleccionar según el perfil solicitado, en relación con las competencias de cada postulante.	Preventivo	-

Procedimiento	Control	Tipo de control	Formato a usar
Términos y condiciones de empleo	Cuando se contrate al personal para puestos relacionados a la seguridad de la información el candidato debe de poseer competencias necesarias para desempeñar el rol.	Preventivo	-
	Al momento de realizar la contratación, los contratos deberían de indicar las responsabilidades del empleado, así como también las de la empresa Ajtecnología.	Preventivo	-
	Los contratos laborales deberían de incluir la cláusula de mantener la confidencialidad y la no divulgación de información, así como también las medidas a tomar si se incumple los requisitos de seguridad de la información.	Preventivo	-
	En el proceso de inducción se deberá aclarar a los empleados los roles y responsabilidades de seguridad de la información	Preventivo	-
	El jefe de recursos humanos deberá de enviar copia de los contratos laborales firmados a gerencia general para asegurarse que todos los empleados están de acuerdo con los términos y condiciones de los mismos.	Preventivo	-
	El jefe de recursos humanos deberá de compartir el manual de control interno para la seguridad de la información a los empleados.	Preventivo	-
Responsabilidades de la dirección	El gerente general debe de delegar al encargado de TI y al jefe inmediato para que comunique y proporcione las instrucciones preliminares para llevar a cabo el rol asignado y responsabilidades al empleado.	Preventivo	-
	El gerente general proporcionará un buzón para que se realicen las denuncias de forma anónima sobre las políticas transgredidas a la seguridad de la información.	Detección	-
	El gerente general delegará al encargado de informática para que realice las investigaciones pertinentes sobre las denuncias realizadas por transgresiones a la política y procedimientos de seguridad de información	Correctivo	-
	Gerencia general debe de incentivar a sus empleados para dar cumplimiento a las políticas establecidas, a través de reconocimientos de empleado del año, otorgando un bono.	Preventivo	-

Procedimiento	Control	Tipo de control	Formato a usar
Responsabilidades de la dirección	El gerente general debe de definir el plan de capacitación, educación y concientización relacionado a las políticas y procedimientos de la organización determinando su frecuencia de acuerdo las áreas del negocio.	Preventivo	-
	La jefatura de recursos humanos establecerá planes de capacitación en los cuales se aborden las diferentes áreas de la empresa, desde el personal técnico, hasta el personal administrativo. Este plan de capacitaciones deberá ser avalado por gerencia general.	Preventivo	-
	La jefatura de recursos humanos será la encargada de elaborar una evaluación sorpresa posterior a las capacitaciones recibidas con el fin de verificar la retención del conocimiento adquirido.	Detección	
	Como parte del plan de capacitación y concientización se entregarán panfletos o boletines informativos en donde se recuerden las medidas de seguridad requeridas por la empresa.	Preventivo	-
Capacitación	En las capacitaciones se abordarán aspectos como: el compromiso de la dirección de con la seguridad de la información; recordatorio de políticas, procedimientos, leyes; responsabilidad del personal; procedimientos básicos de seguridad; puntos de contactos y recursos para recibir información adicional.	Preventivo	-
	Conforme se realicen traslados, nuevos ingresos o modificación en requisitos de seguridad se impartirán las capacitaciones de dos horas por área.	Preventivo	-
	El jefe de recursos humanos verificará que las capacitaciones recibidas hayan sido aprovechadas, caso contrario, se descontará lo cancelado en la capacitación al empleado que demuestre que no dedico intereses en la temática tocada.	Preventivo	-

Procedimiento	Control	Tipo de control	Formato a usar
Proceso disciplinario	Gerencia general debe de clasificar los incidentes de seguridad según su naturaleza, gravedad de la transgresión y su impacto en la empresa	Preventivo	-
	En caso de incumplimiento a lo establecido en la política de seguridad de la información primeramente se hará un llamado de atención de forma verbal se conversará con el empleado para que reconozca las consecuencias de sus actos, si vuelve a incumplir se redactará una - acción de personal de forma escrita, y la tercera vez se dará de baja al empleado	Correctivo	-

Área: Procesamiento electrónico de datos

Alcance y campo de aplicación: Determinación de los requerimientos según el Estándar Internacional ISO 27001 para establecer, implementar, mantener y mejorar la seguridad de la información atendiendo los objetivos y necesidades en el área de procesamiento electrónico de datos en la empresa.

Objetivos de la política: Brindar la protección adecuada contra la pérdida de datos.

Procedimiento	Control	Tipo de control	Formato a usar
Configuración del sistema contable computarizado	El jefe del departamento de informática es quien tiene el acceso de administrador del sistema contable computarizado, y se tiene asignado la configuración del mismo con previa autorización del gerente general.	Preventivo	
	Para configurar la creación de usuarios, modificaciones o solicitudes de accesos, el jefe de informática ingresará como administrador del sistema y realizará las configuraciones aprobadas y autorizadas, posteriormente verificará que el sistema esté parametrizado según lo establecido en la configuración.	Preventivo	
	Periódicamente se deberá montar una prueba de control la cual estará diseñada para probar que realmente los respaldos estarán disponibles y serán funcionales al momento de una emergencia. Este punto deberá abordarlo el jefe del departamento de informática.	Preventivo	
	Además de la revisión de la parametrización del sistema realizada por el jefe de informática, se solicita al contador general que realice las revisiones pertinentes para validar que los datos que ingresan al sistema contable computarizado están siendo procesados de manera adecuada.	Preventivo	
	El contador general es responsable de la revisión de la información que se maneja en el sistema contable computarizado, de igual forma deberá de comunicar al jefe de informática y gerencia general si se detecta alguna deficiencia en el procesamiento de datos.	Preventivo	

Procedimiento	Control	Tipo de control	Formato a usar
Configuración del sistema contable computarizado	El contador y el jefe de informática velarán por que el sistema contable computarizado esté parametrizado de manera que las transacciones realizadas no se evadan acciones que complementan la información, y no permita continuar una acción sin completar los procesos.	Preventivo	
	Al registrar la información en el sistema contable computarizado, se configurará de manera que exista la opción de validar la información, de forma que el usuario se asegure que los datos ingresados son correctos.	Preventivo	
	La información ingresada al sistema debe de estar protegida mientras se espera la validación de registros confidenciales.	Preventivo	
	El jefe de informática solicitará al contador general que revise que la información generada en los distintos módulos, y usuarios del sistema se integren al procesar los datos ingresados al sistema.	Preventivo	
	El jefe informático junto con el contador general serán los encargados de verificar que la información contenida en el sistema contable computarizado esté disponible por medio de consultas en cualquier momento y que ésta se muestre únicamente a los usuarios autorizados.	Preventivo	
	Las transacciones realizadas en el sistema contable computarizado, deberán de estar referenciadas de manera que se pueda identificarse la fecha, hora, usuario, correlativo de transacción, tipo de transacción, módulo de origen, así mismo se deberá de verificar que no exista la duplicidad de transacciones.	Preventivo	
	El sistema contable computarizado estará parametrizado de manera que limite las transacciones de crear, modificar, aprobar y la eliminación de transacciones realizadas por los usuarios se bloqueará de forma que no sea permitida dicha acción. En caso que se deba corregir algún dato aprobado se realizará la corrección con una reversión de registros contables, con el objeto que se mantenga integra la información y se pueda identificar las transacciones realizadas.	Preventivo	

Procedimiento	Control	Tipo de control	Formato a usar
Configuración del sistema contable computarizado	El sistema contable computarizado estará parametrizado de manera que evite la pérdida de datos, en caso de que existan fallos técnicos que intervengan en la finalización de procesamiento de los mismos.	Preventivo	
	Cada vez que se efectúen actualizaciones en el sistema contable computarizado, el contador general y el encargado de informática realizarán una revisión de saldos, transacciones, de manera que al comparar la información con el respaldo realizado previamente se pueda determinar diferencias.	Detección	
	El sistema será configurado por el jefe de informática previa autorización de gerencia general y conocimiento del contador general de manera que el agregar, modificar, reemplazar o realizar cambios de datos sea únicamente con la clave del administrador, y que éstas acciones estén justificadas, aprobadas y autorizadas por el gerente general.	Corrección	-
Registro de eventos	Se deberán producir, mantener y revisar de forma periódica los registros de eventos de los usuarios, las exenciones, fallas y todo lo relacionado a la seguridad de la información.	Detección	
	Estos registros de eventos se identificará: ID del usuario, actividad realizada, fecha, hora, detalle del evento clave, accesos al sistema exitosos y rechazados, cambios de configuración del sistema, uso de privilegios, uso de las aplicaciones, activación de alarmas y desactivación y los registros realizados en el sistema por el personal de cada área.	Detección	

CONCLUSIONES.

- Se identificó que las empresas cuentan con controles internos sin embargo, los encargados de ejecutarlo carecen de un criterio adecuado para realizar actividades de evaluaciones internas debido a que la alta gerencia focaliza sus actividades de capacitación al personal en otras áreas de interés distintas a las relacionadas con la seguridad de la información.

- Las empresas a pesar de contar con medidas preventivas de riesgos hacia la seguridad de la información, enfatizan que es necesario contar con procedimientos de control internos aplicable a la seguridad de la información de los sistemas contables computarizados con respecto al área de seguridad lógica y además fortalecer la seguridad física conforme se realicen monitoreo a los riesgos potenciales y que estos sean comunicados adecuadamente al personal.

- Las empresas tienen definidas políticas contables documentadas en un sistema contable computarizado sin embargo, según la experiencia laboral los usuarios del sistema reconocen la necesidad de fortalecer la seguridad de la información contable a través de una política específica que restrinja el acceso al mismo puesto que, se reconoce que al conservar la confidencialidad, integridad y disponibilidad de la información proporciona un nivel de confianza a la administración para la toma de decisiones.

- Las empresas no cuentan con las medidas de seguridad adecuadas con respecto a las áreas de accesos físicos y lógicos, las cuales permitan proporcionen certeza que las áreas restringidas e información confidencial no puedan ser manipulada por personas no autorizadas.

- Los profesionales que ejercen la contaduría pública conocen el Estándar Internacional ISO/IEC 27001 sin embargo no cuentan con controles internos basados en los lineamientos relacionados a éste para conservar la confidencialidad, integridad y disponibilidad de la información contenida en los sistemas contables que ayude a disminuir los riesgos de pérdidas de calidad de la misma.

RECOMENDACIONES.

- La alta gerencia debe de liderar y apoyar al personal encargado de control interno a través de capacitaciones para que estos adquiera las competencias necesarias para desarrollar un criterio adecuado que le permita realizar una evaluación interna a las amenazas existentes y determinar las medidas adecuadas en el contexto de la seguridad de la información financiera.

- Implementar controles internos aplicables a la seguridad de la información a través de un manual basado en el Estándar Internacional ISO 27001 que enfatice una cultura de riesgo y con el objetivo que la información manejada en el sistema contable computarizado conserve la confidencialidad, integridad y disponibilidad para la toma de decisiones a través de acciones de corrección para mitigar amenazas.

- Determinar procedimientos de control interno para las áreas de seguridad lógica y seguridad física que ayuden a disminuir los riesgos inherentes de pérdida de la información del sistema contable computarizado y que garanticen la confidencialidad, integridad y disponibilidad de ésta para la toma de decisiones

- Actualizar la política existente adoptando los requerimientos establecidos en el Estándar Internacional ISO/IEC 27001 de manera que se integren los controles adecuados conforme la estructura de la norma para lograr un mayor grado de cumplimiento de objetivos para asegurar la información financiera.

BIBLIOGRAFÍA

Aspel coi (2016), recuperado de

xhttp://www.aspel.com.mx/productos/coi/presentacion.html

Carmen Bauset Carbonell (2016), *La evolución de las TI*.

Contpaq (2016), obtenido de

https://www.contpaqi.com/CONTPAQi/index.aspx

IBM Pymes México (2016), obtenido de

https://www.ibm.com/us-en/?lnk=m

Francisco Fernández Izquierdo (2000), *La historia moderna y nuevas tecnologías de la información y comunicación*.

ISO 27001/IEC 27001:2005 *Tecnología de la Información- Técnicas de seguridad- Sistemas de gestión de seguridad de la información*- Requerimientos-primera Edición 2005.

Roberto Sampieri *Metodología de la investigación* –sexta edición.

Oracle Latinoamérica (2016), recuperado de

http://www.oracle.com/lad/index.html.

Lorena Alexandra Nuñez (2010), Tesis de grado "*Implementación de un sistema contable computarizado en la fábrica alfarera ubicada en el valle de Tumbaco provincia de pichincha para el periodo del 01 al 31 de enero del 2008*".

Lic. Mae. Mario Cornejo (2015), Diapositivas de clase *"Necesidad de control en informática"*

Committee of Sponsoring Organizatios of the Treadway Commission (COSO) (2004), *Gestión de riesgos corporativos – Marco integrado*

ANEXOS

1. En la empresa en la que labora ¿Existen políticas contables que indiquen el tratamiento de las transacciones económicas en el reconocimiento, medición, revelación y presentación?

   Objetivo: Identificar si la empresa posee políticas contables documentadas y disponibles para el personal encargado del registro de transacciones que contribuyen a la elaboración de Estados Financieros.

Alternativa	Frecuencia absoluta	Frecuencia relativa
a) Si	25	96%
b) No	1	4%
Total	**26**	**100%**

Análisis: La existencia de políticas contables que indiquen el tratamiento de las transacciones económicas de una forma adecuada y dando cumplimiento a las necesidades de la entidad son importantes puesto que al definir las medidas a seguir se proporcionará información contable integra, fiable y se tendrá disponible para la toma de decisiones de las partes interesadas.

Dados los resultados obtenidos el 96% posee políticas contables que indiquen los lineamientos para el tratamiento de la información contable lo cual, representa un porcentaje muy favorable puesto que la mayoría de los encuestados confirmaron que cuentan con lineamientos uniforme para propósitos contables. Sin embargo, el 4% indicó no contar con instrucciones específicas para el tratamiento de las transacciones económicas lo cual representa una debilidad en el control interno y una condición desfavorable en la toma de decisiones debido a que las transacciones pueden incidir en la integridad, fiabilidad y disponibilidad de la información.

2. Indique ¿Qué otros tipos de políticas posee la empresa distinta a las del área contable?

Objetivo: Determinar si la empresa posee políticas diferentes a las contables documentadas y disponibles para el personal encargado de cada área.

Alternativa	Frecuencia absoluta	Frecuencia relativa
a) Seguridad de la información	17	65%
b) Calidad de servicio	8	31%
c) Responsabilidad social	3	12%
d) Recursos humanos	13	50%
e) Seguridad ocupacional	9	35%
f) Otras (especifique)	1	4%

Análisis: La definición de políticas en áreas específicas fortalecen el control interno de la entidad, de acuerdo con el contexto del negocio, sin embargo, la seguridad de la información es una de las áreas importantes que debe de adoptar en toda entidad puesto que, su aplicación se percibe de forma íntegra en el funcionamiento del negocio.

Según los resultados, el 65% identificó contar con políticas en el área de seguridad de la información, lo cual representa un porcentaje favorable debido a que la alta gerencia tiene presente su importancia para conservar la confiabilidad, integridad y disponibilidad de la información.

El 31% indicó que una de las políticas específicas a parte de las contables se desarrolla en el área de calidad de servicio, para efectos de control interno y continuidad del negocio es relevante ya que refleja el cuidado que se tiene al conservar su presencia en el mercado.

El 12% confirmó tener establecidas políticas que contribuyan a desarrollar mejoras para la sociedad. Por otra parte, el 50% señaló que existen políticas relacionadas a recursos humanos indicando ser favorable al proporcionar los lineamientos de inducción al personal.

El 35% manifestó que existen políticas sobre la seguridad ocupacional, lo cual es favorable para cubrir los riesgos existentes en el área de seguridad física, punto clave para

salvaguardar la información contra amenazas que pongan en juicio la integridad y disponibilidad de la información.

El 4% confirmó que poseen otras políticas como la ética profesional en el área de contabilidad lo cual representa ser un indicador favorable para conservar la confidencialidad de la información.

3. En el caso que no exista política en el área de seguridad de la información ¿cuáles cree que son las razones principales?

   Objetivo: Indagar las dos razones principales por las cuales no existen políticas para el área de seguridad de la información.

Alternativa	Frecuencia absoluta	Frecuencia relativa
a) Se desconoce el impacto que puede ocasionar un incidente.	5	56%
b) Administración focaliza su interés en otras áreas.	4	44%
c) Falta de personal capacitado.	0	0%
d) No le es aplicable al entorno en el que labora	0	0%
e) Otra (especifique)	0	0%

Análisis: La existencia de política en el área de seguridad de la información es importante para conservar la confiabilidad, integridad y disponibilidad de la información.

La mayoría de los encuestados afirmaron contar con política en el área de seguridad según los resultados de la pregunta número dos, no obstante el 56% que confirmaron no tener definidas políticas para este rubro, debido a que se desconoce el impacto que puede ocasionar un

incidente que ponga en riesgo la conservación de la confiabilidad, integridad y disponibilidad de la información, lo cual representa un porcentaje desfavorable, puesto que si no se cubre el riesgo a través de la implementación de medidas de seguridad queda en juicio la calidad de la información para la toma de decisiones de la alta gerencia y de las partes interesadas en general.

Así mismo, el 44% indicó que la administración focaliza su interés en otras áreas, lo cual resulta ser desfavorable, puesto que no se cuentan con medidas de seguridad que proporcionen certeza que se aborden los riesgos inherentes a la seguridad de la información de una manera adecuada en la cual se analice los parámetros claves para conservar la información.

4. Según su experiencia, ¿qué grado de utilidad posee la política de seguridad de la información en la determinación de las cifras contables presentadas en los estados financieros?

   Objetivo: Conocer si para el profesional resultaría útil disponer con política de seguridad de la información que influya en la fiabilidad de las cifras contables presentadas en los estados financieros.

Alternativa	Frecuencia absoluta	Frecuencia relativa
a) Muy útil	20	77%
b) Útil	6	23%
c) Poco útil	0	0%
d) Nada útil	0	0%
Total	**26**	**100%**

Análisis: Que los profesionales de la contabilidad conozcan y consideren importante y útil la política de seguridad de la información para obtener cifras contables adecuadas para la toma de decisiones es importante.

Esto se ve reflejado en los resultados obtenidos en los que el 77% de los encuestados considera según su experiencia laboral que disponer de una política de seguridad de la información proporciona una mayor confiabilidad en las cifras de los estados financieros.

Un 23% considera que es útil contar con esta política, lo que lleva a determinar que el 100% de los encuestados brinda una aceptación positiva a la política de seguridad de la información para la obtención de cifras contables presentadas en los estados financieros.

De lo anterior se puede concluir que, según la experiencia de los encuestados, contar con esta herramienta de apoyo para mejorar el control interno referente a la información es esencial y necesario para asegurar la integridad y confiabilidad de los datos contables.

5. ¿Cuál es el área más sensible y que requiere política de seguridad de la información dada su incidencia en la preparación de estados financieros?

   Objetivo: Determinar en qué área el profesional considera la existencia de mayor riesgo de afectación en las cifras contables.

Alternativa	Frecuencia absoluta	Frecuencia relativa
a) Control de acceso y autenticación	9	35%
b) Derechos y privilegios de acceso	10	38%
c) Protección del equipo informático	14	54%

Análisis:

La información presentada en los estados financieros es útil en la toma de decisiones cuando cumple las características necesarias para informar a los usuarios interesados la actividad

económica de la entidad, y es por ello que se deben de cubrir las áreas sensibles a través de políticas específicas que puedan abordar la seguridad física y lógica que inciden en la seguridad de la información.

Según los resultados obtenidos el 54% de los encuestados afirmaron que la protección del equipo informático es el área más sensible que requiere política de seguridad de la información dada su incidencia en la preparación de estados financieros, debido a que través de la implementación una política adecuada se cubren los riesgos asociados al área física, proporcionando de esta forma un parámetro importante para conservar la disponibilidad de la información.

El 38% indicó el derecho y privilegios de acceso puesto que consideran el conservar la confidencialidad e integridad de la información ser más importante.

El 35% manifestó que el control de acceso y autenticación de los usuarios es el área más sensible, debido a su incidencia en la preparación de estados financieros, debido a que si se cuenta con una política que regule este riesgo se estaría fortaleciendo la confidencialidad, integridad y disponibilidad de la información que se maneja en el sistema contable computarizado.

Lo anterior demuestra que dada su incidencia el 73% confirma que el área de seguridad lógica incide den una mayor proporción en la preparación de estados financieros que el área de seguridad física representada con el 54%, se requiere abordar estas deficiencias y fortalecerlas a través de medidas de seguridad adecuadas para abordar estas áreas.

6. ¿Existen controles aplicables al uso del sistema contable computarizado en el lugar en que labora?

Objetivo: Conocer la existencia de controles aplicables al uso del sistema contable computarizado que afecta en la presentación de información integra, disponible, confidencial y preservada.

Alternativa	Frecuencia absoluta	Frecuencia relativa
a) Si	24	92%
b) No	2	8%
Total	**26**	**100%**

Análisis: Es importante la aplicación de controles para el uso del sistema contable computarizado puesto que éste es una herramienta tecnológica útil para salvaguardar la información confidencial, la cual debe de estar restringida para conservar la confidencialidad, integridad y disponibilidad de la información en la presentación de información.

El 92% manifestó contar con controles aplicables al uso del sistema contable computarizado, no obstante, el contar con estas medidas de seguridad no garantiza conservar la calidad de la información, puesto que para lograr esta característica se debe de efectuar un análisis de los aspectos que conllevan el definir controles para el uso del sistema contable computarizado.

Por otra parte, el 8% de los encuestados manifestó no tener definidos para el uso del sistema contable computarizado, esto representa un porcentaje mínimo, pero proporciona un indicador importante para identificar que la entidad necesita se definan e implemente medidas de seguridad adecuadas que estén acorde a los objetivos de la entidad.

7. ¿Cuál considera que es el beneficio de aplicar procedimientos de control interno para asegurar la información que se maneja en el sistema contable computarizado?

Objetivo: Determinar los beneficios que se obtendrán de aplicar procedimientos de control interno en la seguridad de la información.

Alternativa	Frecuencia absoluta	Frecuencia relativa
a) Disponibilidad de la información en la toma de decisiones	13	50%
b) Restricción de información confidencia	3	12%
c) Disminución de riesgo de pérdida de información	12	46%
d) Fortalecer la integridad de la información	12	46%
e) Otro (especifique)	0	0%

Análisis: El control interno bien aplicado genera beneficios palpables en el ambienten empresarial. La aplicación correcta de procedimientos de control enfocados a la seguridad de la información que se maneja en el sistema contable computarizado proporcionará disponibilidad, resguardo, ambiente de seguridad y disminución de riesgos.

Según los resultados obtenidos en la investigación de campo, el 50% consideró que la disponibilidad de la información en la toma de decisiones es el beneficio con mayor representación debido a que es una de las características de la misma que se debe de abordar para que ésta sea de calidad.

El disminuir los riesgos de perder información, así como también el fortalecer la integridad de la información están representados por el 46% indicando que ambos beneficios se obtienen a través de aplicar procedimientos de control interno para conservar la disponibilidad e integridad de la información.

El 12% confirmó que el restringir la información confidencial es considerado un beneficio al practicar medidas de seguridad.

De lo anterior se demuestra que los encuestados reconocen los beneficios que se obtienen al ejercer controles acordes a las necesidades de la empresa para que la información proporcionada a la alta dirección cumpla con la confiabilidad, integridad y disponibilidad de la misma.

8. ¿Considera que es necesario fortalecer la seguridad de la información, a través de una política específica?

   Objetivo: Indagar si es necesario contar con política de seguridad de la información en la empresa para el profesional.

Alternativa	Frecuencia absoluta	Relación porcentual
a) Si	25	96%
b) No	1	4%
Total	**26**	**100%**

Análisis: Como parte del alcance de establecer una política aplicable a la seguridad de la información se deben considerar factores externos e internos en el contexto de la entidad además de las actividades a considerar partiendo del compromiso de la alta gerencia en planificar, apoyar, implementar, evaluar y mejorar las medidas de seguridad que integrarán la política, con el fin de asegurar la información.

Dados los resultados obtenidos en la investigación de campo los profesionales de la contaduría pública que ejercen en el área de control interno en las empresas que se dedican a la venta de productos de la telecomunicación el 96% confirma la necesidad de fortalecer la seguridad de la información, a través de la política específica que aborde controles internos en

las áreas que se procesa información para conservar la confidencialidad, integridad y disponibilidad de la información

El 4% de los encuestados opinó que no es necesario establecer lineamientos específicos en las áreas que procesan información confidencial debido a que cuentan con una política definida para el resguardo de la misma.

9. ¿Existe un plan de trabajo establecido por la gerencia general que brinde un adecuado tratamiento para asegurar la información contable?

   Objetivo: Determinar si la alta gerencia cuenta con un plan de trabajo enfocado a la seguridad de la información de la empresa.

Alternativa	Frecuencia absoluta	Relación porcentual
a) Si	15	58%
b) No	11	42%
Total	**26**	**100%**

Análisis: Un plan de trabajo que aborde aspectos claves para cubrir las áreas sensibles que proporcionan información contable es importante que se defina en el mismo la responsabilidad que le compete a la alta gerencia sobre evaluar la efectividad del mismo, a través de actividades de monitoreo para verificar que las actividades y aspectos contenidos en el plan de trabajo se realicen conforme se ha establecido. De esta forma se dará seguimiento a lo panificado y de haber una no conformidad con el mismo se analizarán las medidas de control correctivas para conservar la confiabilidad, integridad y disponibilidad de la información.

Según los resultados obtenidos a través de la encuesta realizada a los contadores públicos que laboran en el área de control interno el 58% indicó que cuenta con un plan de trabajo

enfocado que aborda controles internos aplicable a las áreas que procesan información, lo cual indica la existencia del mismo, sin embargo no se puede definir su efectividad sin efectuar medidas de seguimiento al mismo como parte de las medidas de seguridad adecuadas.

El 42% de los encuestados confirma que no se cuenta con un plan de trabajo que brinde un adecuado tratamiento para asegurar la información contable como parte de los aspectos a considerar en el control interno aplicable en la entidad, esto indica la necesidad de definir e implementar un plan de trabajo que cubra los elementos que puede incidir en la calidad de la información.

10. Para el área de seguridad lógica, ¿cuál de los siguientes controles de acceso al sistema contable computarizado considera más importante?

    Objetivo: Identificar qué tipo de control de acceso considera más importante para el uso del sistema contable computarizado.

Alternativa	Frecuencia absoluta	Relación porcentual
a) Restricción de acceso del usuario	11	42%
b) Acceso a conexión de redes	4	15%
c) Registro y cancelación de registro de usuarios	3	12%
d) Gestión de contraseñas	10	38%
e) Revisión de los derechos de acceso de usuario	12	46%
f) Otro (Especifique)	0	0%

Análisis: Para el área de seguridad lógica se consideran controles de acceso a la información restringida e instalaciones de procesamiento de información contable, esto marca un parámetro para definir las medidas de seguridad a definir e implementar en las partes que hacen uso del sistema contable computarizado.

De los resultados obtenidos en las encuestas el mayor porcentaje está representado por el 46% que afirmó como el control más importante la revisión de los derechos de acceso de usuarios puesto que se descartar la existencia de aspectos que vulneren las acciones establecidas al asignar los privilegios. Así mismo, el 42% de los profesionales consideró que la restricción de acceso del usuario es el control más importante para considerar como parte de las medidas de seguridad que deben ser reguladas.

El 38% de los encuestados optó por el control para la gestión de contraseñas dado que en el proceso de asignar contraseñas la calidad de las mismas al iniciar sesión de una forma segura representa un resultado favorable para proteger la confidencialidad, autenticidad e integridad de la información.

No obstante, el 15% de los encuestados indicó que el acceso a conexión de redes contribuye a proteger la información en el sistema contable computarizado es uno de los controles más importantes a considerar en el área de seguridad lógica. El 12% confirmó que el registro y cancelación de es más importante para salvaguardad la información contable en el sistema contable computarizado.

11. ¿Quién autoriza los privilegios de acceso a los usuarios del sistema contable computarizado?

Objetivo: Determinar quién es el encargado de autorizar los accesos al sistema contable computarizado.

Alternativa	Frecuencia absoluta	Relación porcentual
a) Gerente general.	5	19%
b) Gerente financiero.	9	35%

c) Encargado del departamento de informática	11	42%
d) Jefaturas de las diferentes áreas de la empresa.	2	8%
e) Otro (especifique)	0	0%

Análisis: Para asegurar el acceso al sistema contable computarizado uno de los aspectos a definir por la alta gerencia es el personal especializado para la asignación de usuarios y sus respectivos privilegios acorde a las funciones desarrolladas, para restringir el uso de información confidencial.

Dados los resultados el porcentaje más alto lo representa el 42% que aseguró la responsabilidad del encargado del departamento de informática en establecer los privilegios a los usuarios para el uso del sistema contable computarizado, lo cual representa un riesgo si éste carece del conocimiento suficiente para asignar las funciones a realizar que incidan en conservar la integridad y disponibilidad de la información contable.

El 35% de los encuestados afirmaron como parte de los procedimientos de control interno en asignar privilegios a los usuarios lo efectúa el gerente financiero lo cual representa un porcentaje favorable debido a que el encargado posee el conocimiento adecuada para el tratamiento de la seguridad de la información contable.

Según lo indicó el 19% de los encuestados es el gerente general quien realiza este procedimiento de control interno en definir las acciones que puede llevar a cabo los usuarios del sistema, lo cual indica un porcentaje poco favorable puesto que se requiere de un análisis de las actividades a realizar por los usuarios para la asignación de los privilegios como parte de las medidas de seguridad para abordar los riesgos existentes en este proceso.

Sin embargo, representando la minoría con el 8% identificó a las jefaturas de las diferentes áreas de las empresas como encargados de gestionar los privilegios asignados a los usuarios y posteriormente se comunicaba a informática para habilitar dichas funciones.

12. ¿Con qué frecuencia se realizan actualizaciones al sistema contable computarizado para subsanar deficiencias del mismo?

    Objetivo: Cuantificar la frecuencia con la que se realizan actualizaciones en el sistema contable computarizado de la empresa.

Alternativa	Frecuencia absoluta	Relación porcentual
a) Mensual	8	31%
b) Trimestral	6	23%
c) Anual	5	19%
d) Otra frecuencia (especifique)	4	15%
e) No se realizan actualizaciones.	3	12%
Total	**26**	**100%**

Análisis: Uno de los aspectos a considerar en el mantenimiento del sistema contable computarizado son las actualizaciones para mejorar el funcionamiento del mismo.

Los resultados obtenidos de los encuestados el 31% confirmaron que se realizan actualizaciones de forma mensual, lo cual indica para efectos de control interno se busca mejorar constantemente como parte de proporcionar de forma favorable una herramienta útil para los usuarios de la información.

El 23% de la muestra manifestaron que las actualizaciones para mejorar el sistema se realizan trimestralmente, esto representa un porcentaje favorable al proporcionar mejoras al mismo con el fin de abordar los aspectos de seguridad de la información.

El 19% indicó como medida de seguridad realizar actualizaciones año lo cual representa una limitante para efectos de seguridad puesto que deben ser tratados en un lapso menor al establecido.

El 15% especificaron que se realizan actualizaciones conforme se soliciten según los aspectos a mejorar lo cual representa un control adecuado para conservar la confiabilidad, integridad y disponibilidad de la información.

Por otra parte, el 12% confirmó que no se realizan actualizaciones lo cual indica que se deben de considerar lo más pronto posible para superar esa condición desfavorable.

13. ¿Con qué frecuencia se realizan respaldos de la información financiera y contable?

Objetivo: Determinar si en la empresa se realizan respaldos de la información financiera y contable para mantener la integridad y disponibilidad de esta y la frecuencia con la que esta se realiza.

Alternativa	Frecuencia absoluta	Relación porcentual
a) Diario	11	42%
b) Semanal	9	35%
c) Mensual	5	19%
d) Otra frecuencia (especifique)	0	0%
e) No se realizan	1	4%
Total	**26**	**100%**

Análisis: Una de las medidas de seguridad parar proteger contra la pérdida de información en general es realizar respaldos los cuales se debe establecer la frecuencia con que estos se efectúen según la necesidad.

Según los resultados obtenidos el 42% confirmó realizar diariamente como actividades de control interno respaldos de la información financiera y contable lo cual es ideal para proteger el activo contra pérdida potencial y conservar su calidad.

Así mismo, 35% afirmó efectuar respaldos cada semana como medida de seguridad favorable en términos de tiempo ya que existe un mejor control de calidad sobre la información resguardada y cubrir riesgos que incidan en la integridad y disponibilidad de la información.

El 19% manifestó practicar esta medida de seguridad cada mes lo cual indica ser poco favorable puesto que existe un mayor riesgo de pérdida de información ante algún evento de seguridad que incida en conservación de la misma.

Por otra parte, el 4% indicó no realizar respaldos lo cual representa un porcentaje mínimo desfavorable que requiere definir, implementar medidas de control interno correctivas para conservar la información financiera y contable de forma urgente.

14. En el área de seguridad física, ¿cuáles de los siguientes controles se practican en su lugar de trabajo?

    Objetivo: Conocer el mantenimiento adecuado que se les brinda a los equipos para el uso del sistema contable computarizado para la prevención de pérdidas, daños, robo o compromiso de activos y la interrupción de actividades que pongan en riesgo la disponibilidad de la información

Alternativa	Frecuencia absoluta	Relación porcentual
a) Perímetros de seguridad física	3	12%
b) Controles de entrada física.	13	50%

c) Protección contra amenazas ambientales externas.	2	8%
d) Protección contra fallas en el equipo.	16	62%
e) Otro (especifique)	2	8%

Análisis: Dentro de los aspectos a considerar en el área de seguridad física es brindar a los equipos utilizados por la empresa el mantenimiento adecuado para proporcionar las condiciones óptimas para realizar las actividades del negocio de forma continua.

Como parte del control interno relacionado con la seguridad de la información en el área de seguridad física el 62% afirmaron brindar una protección contra fallas en el equipo, por tanto, es muy favorable debido a que se proporciona un adecuado mantenimiento a las herramientas utilizadas para asegurar la información y la continuidad del negocio.

El 50% de los encuestados estableció como parte de las medidas de seguridad practicadas es mantener controles de entrada física, por consiguiente, es favorable para restringir el acceso no autorizado a las áreas en donde se procesa información confidencial.

El 12% representa la práctica de controles internos al utilizar perímetros de seguridad física para controlar, proteger y monitorear las áreas sensibles en las que se procesa información confidencial. El 8% de los encuestados indicó practicar el control de protección contra amenazas ambientales externas, lo cual es una de las medidas de seguridad muy favorables a considerar como parte de los procedimientos aplicables al área de seguridad física.

Por otra parte 8% manifestó no practicar ningún control interno aplicable al área de seguridad física, representando un porcentaje mínimo que se deben de implementar medidas de seguridad lo más pronto posible.

15. Señale las medidas de protección del equipo contra software malicioso que se aplican en la empresa.

Objetivo: Conocer el mantenimiento adecuado que se les brinda a los equipos para el uso del sistema contable computarizado para la prevención de pérdidas, daños, robo o compromiso de activos y la interrupción de actividades que pongan en riesgo la disponibilidad de la información.

Alternativa	Frecuencia absoluta	Relación porcentual
a) Licencia de software antivirus actualizado	22	85%
b) Bloqueo de acceso a internet	9	35%
c) No abrir correos procedentes de direcciones poco confiables	9	35%
d) Evitar conexiones no confiables a red	1	4%
e) Evitar instalación de software con autor desconocido	8	31%
f) Bloqueo de puertos USB	3	12%
g) Mantenimiento preventivo al equipo	7	27%
h) Otra (Especifique)	0	0%
i) No existen medidas de protección del equipo	1	4%
j) No tiene conocimiento en el área	0	0%

Análisis: Dentro de los objetivos de control de la ISO 27001 en el apartado de control de acceso establece que como un punto esencial el resguardo de la información a través de la gestión de accesos y la responsabilidad del usuario de seguir una política de seguridad de la información.

Del total de unidades de análisis, se pudo observar que el 85% tiene como medida de protección la licencia de software antivirus actualizado, el 35% bloqueo de acceso a internet y no abrir correos procedentes de direcciones poco confiables, el 31% evitar instalaciones de software con autor desconocido, el 27% mantenimiento preventivo del equipo, 12% bloqueo de puertos USB y el 4% evita conexiones no confiables o no cuentan con medidas de protección del equipo.

Lo antes expuesto nos muestra que las empresas encuestadas del sector si cuentan con medidas de protección del equipo contra software maliciosos en el que el más común es la actualización de licencias antivirus, pero a su vez es la única medida en muchos casos, siendo solamente nueve unidades de análisis las que cuentan con otra medida diferente lo cual implica un riesgo asegurado, además es importante mencionar que una de las empresas no cuenta con medidas de protección de equipos.

16. ¿Existe en su empresa una unidad que dé seguimiento a los procesos relacionados a la seguridad de la información?

Objetivo: Indagar si existen procedimientos de seguimientos a controles para detectar deficiencias.

Alternativa	Frecuencia absoluta	Relación porcentual
a) Si	20	77%
b) No	6	23%
Total	**26**	**100%**

Análisis: Es importante para un control interno darles seguimiento a los procedimientos establecidos, esta actividad es fortalecida con una unidad de seguimiento de estos, lo cual ayudará a que sea más fácil detectar las deficiencias que en su momento no se consideraron.

De total de unidades de análisis, el 77% se puede interpretar que si cuentan con una unidad de seguimiento de los procesos relacionados a la seguridad de la información, se asume que son empresas que buscan darle la importancia necesaria a la información por otra parte un 23% no cuenta con alguna unidad que busque darle el seguimiento adecuado este activo tan importante.

17. ¿En qué momento se brinda capacitación a los usuarios del sistema contable computarizado?

Objetivo: Conocer si se brinda a los usuarios del sistema contable computarizado capacitación para reduciendo el riesgo de error humano

Alternativa	Frecuencia absoluta	Relación porcentual
a) Durante el empleo según sea relevante	4	15%
b) En el proceso de inducción	17	65%
c) De acuerdo con plan de capacitaciones	6	23%
d) No se brinda capacitación	1	4%

Análisis: La inducción inicial al personal de nuevo ingreso o al momento de cambio en un sistema contable computarizado es esencial para asegurar el correcto funcionamiento de los procesos asociados al sistema de información. La ISO 27001 en sus objetivos establece la importancia de infundir un ambiente de seguridad de información.

De total de unidades de análisis el 65% capacita a los usuarios del sistema contable computarizado en la inducción, el 23% lo hace de acuerdo con un plan de capacitaciones, un 15% durante el empleo según sea relevante y solo un 4% no brinda capacitaciones.

Lo anterior afirma que las empresas encuestadas le dan importancia al correcto uso del sistema contable computarizado pues conocen que a través del uso adecuado del mismo es una herramienta para procesar información para la toma de decisiones de la alta gerencia.

18. ¿Con qué frecuencia se efectúa la divulgación de la política de seguridad de la información a los empleados dentro de la empresa en que labora?

Objetivo: Conocer si se brinda a los usuarios del sistema contable computarizado capacitación para reduciendo el riesgo de error humano

Alternativa	Frecuencia absoluta	Relación porcentual
a) Una vez al año	9	35%
b) Dos veces al año	2	8%
c) Más de dos veces al año	2	8%
d) Otra frecuencia (especifique)	12	45%
e) Abstenciones	1	4%
Total	**26**	**100%**

Análisis: La comunicación es un factor importante al momento de practicar las medidas establecidas en el control interno, para obtener resultados favorables se requiere la divulgación de los lineamientos adoptados de manera eficiente y eficaz al personal responsable de salvaguardar la información.

De total de unidades de análisis el 45% confirmó que poseen otras frecuencias a las alternativas sugeridas, demostrando de forma unánime que no existe una divulgación de una política de seguridad de la información, al momento de la contratación ni durante el empleo lo cual es desfavorable puesto que si no se transmite la importancia de aplicar los lineamientos establecidos no se lograrán los resultados esperados de las partes interesadas, por otra parte,35% manifestó realizar la divulgación una vez al año, un 8% practica esta medida dos veces al año o más y el 4% se abstuvo de contestar la pregunta.

Es importante recalcar que del 45% identificó la existencia de una política pero que la misma no se divulga al personal lo que indica que no transmiten el compromiso adquirido por el personal encargado de la supervisión del control interno.

19. En el caso que conozca un modelo que gestione la seguridad de la información, ¿cuál marco de referencia considera que es más apropiado adoptar según las necesidades del lugar en que labora?

Objetivo: Conocer si el profesional identifica algún marco de referencia para la gestión de seguridad de la información.

Alternativa	Frecuencia absoluta	Relación porcentual
a) Estándar Internacional ISO27001	21	81%
b) Biblioteca de Infraestructura de Tecnologías de Información (ITIL, por sus siglas en inglés)	1	4%
c) Objetivos de Control para Información y Tecnologías Relacionadas (COBIT, por sus siglas en inglés)	1	4%
d) Otro (especifique)	2	8%
e) Abstenciones	1	4%
Total	**26**	**100%**

Análisis: Conocer un modelo de gestión de la seguridad de la información es esencial si se quiere acoplar esto al control interno. Puede servir de guía el tener una noción de lo que se quiere conseguir y como se va conseguir.

Del total de unidades de análisis, el 81% conoce el estándar ISO 27001, un 8% otro tipo de estándar y el 4% conoce lo que es ITIL, COBIT o simplemente se abstuvo de contestar.

Conforme los resultados obtenidos es importante mencionar que la mayoría conoce la ISO 27001 y la aplicación de un modelo de gestión de información asociado al control interno.

20. ¿Cómo considera que afectaría en su empresa la implementación de controles internos aplicables a la seguridad de la seguridad de la información para sistemas contables computarizados?

Objetivo: Conocer la opinión del profesional sobre la propuesta de trabajo de investigación a realizar.

Alternativa	Frecuencia absoluta	Relación porcentual
a) Muy favorable	23	88%
b) Favorable	3	12%
c) Poco favorable	0	0%
d) Desfavorable	0	0%
Total	**26**	**100%**

Análisis: Conocer la opinión de las unidades de análisis es imperante al momento de querer desarrollar una herramienta que ayude a fortalecer los controles internos referidos a la seguridad de la información, pues si se considera que en el medio no es necesario, no hay razón alguna para destinar tiempo a dicha labor.

Del total de unidades de análisis, el 88% considera muy favorable la implementación de controles internos aplicables a la seguridad de la información para los sistemas contables computarizados, un 12% confirma que es favorable.

Esto demuestra que, a pesar de contar con controles o políticas de seguridad de la información, reforzar estos aspectos con los requerimientos de un Estándar Internacional es aceptable por los profesionales de la contaduría pública encargados del control interno en las diferentes áreas de la empresa.

21. ¿Qué grado de utilidad le asignaría a un documento que proporcione una guía sobre el control interno aplicable a la seguridad de la información para sistemas contables computarizados?

Objetivo: Conocer la opinión del profesional sobre la propuesta de trabajo de investigación a realizar.

Alternativa	Frecuencia absoluta	Relación porcentual
a) Muy útil	22	85%
b) Útil	4	15%
c) Poco útil	0	0%
d) Nada útil	0	0%
Total	**26**	**100%**

Análisis: Conocer la utilidad que supone una herramienta de control para la seguridad de la información para sistemas contables computarizados para las unidades de análisis es necesario ya que demuestra un preámbulo de la aceptación que esto tendría en el ámbito laboral, por tanto, se estará realizando un aporte significativo para la profesión de la contaduría pública.

Del total de unidades de análisis, el 85% considera que sería muy útil una guía sobre control interno aplicable a la seguridad de la información para sistemas contables computarizados, un 15% que sería útil y un 0% considera que sería poco útil o nada útil este tipo de guía.

De lo anterior se puede mencionar que el 100% de las unidades de análisis considera muy útil o útil la elaboración de una guía de control interno. Esto implica que una herramienta de esta índole podría ser aceptada y aplicada con el fin de fortalecer el control en las entidades del sector en estudio para el área de seguridad de la información contable y financiera.

Anexo N° 1

Empresa: AJTECNOLOGÍA, S.A. DE C.V.				
Solicitud de acceso al sistema				
		fecha de solicitud:		
Departamento:		*fecha de autorización:*		
Jefe inmediato:		*fecha de entrega de usuario:*		
Solicitante:				
Cargo:				
Código de equipo asignado:				
Módulos solicitados:		*Privilegios de acceso solicitados:*		
Vigencia de los privilegios solicitados:				
Comentario:				
Firmas:	_____ *Solicitante*	_____ *Jefe inmediato*	_____ *Gerente general*	_____ *Dto de TI*

Anexo N° 2

Empresa: AJTECNOLOGÍA, S.A. DE C.V.				
Bitácora de registro de accesos no autorizados				
del:		al:		
Usuario	Fecha, hora del inicio de sesión correcto anteriormente	# intentos fallidos	Usuario bloqueado	Fecha de bloqueo de usuario

Anexo N° 3

Empresa: AJTECNOLOGÍA, S.A. DE C.V.
Bitácora de actualización del software

Encargado: fecha de solicitud de actualización:
Proveedor del software: fecha de autorización:
Soporte técnico solicitado:
Áreas a actualizar:

Detalle de actualización	Aplicaciones/módulos a actualizar	Fecha/hora de última actualización	Fecha/ de actualización	Versión anterior

Firmas: _____ Gerente general _____ Departamento de TI

Anexo N° 4

Empresa: AJTECNOLOGÍA, S.A. DE C.V.
Bitácora de mantenimiento de activos

Encargado del equipo:_____
Código de activo:_____
Tipo de activo:_____
Jefe inmediato:_____
Área de trabajo:_____

Observaciones:_____

Tipo de mantenimiento	Fecha de mantenimiento	Fecha de último mantenimiento	Fecha programada del próximo mantenimiento	Comentario

_____ Responsable del equipo
_____ Encargado de mantenimiento
_____ Gerente general
_____ Depto de TI

Anexo N° 5

AJTECNOLOGIA, S.A. DE C.V.
Control de dispositivos móviles de la entidad

N°	Fecha de adquisición	Descripción	Modelo		Marca		Responsable	Departamento

Firmas **Elaborado** **Revisado** **Autorizado**

Anexo N° 6

AJTECNOLOGIA, S.A. DE C.V.
Formato de orden de compra de utensilios

Orden de compra **N°**

N° de ítems a solicitar	Descripción	Costo	Total

Departamento que solicita

Firmas **Solicitado** **Revisado** **Autorizado**

Anexo N° 7

AJTECNOLOGIA, S.A. DE C.V.
Inventario de activos

N°	Ítems encontrados	Descripción	Modelo		Marca		Responsable	Departamento	Ítems según control de activos	diferencias encontradas

Firmas **Elaborado** **Revisado** **Autorizado**

Anexo N° 8

AJTECNOLOGIA, S.A. DE C.V.
Bitácora de ingresos a las instalaciones

Hora de ingreso	Motivo de la visita	Documento de identificación	Nombre de la persona	Hora de retiro de las instalaciones	Firma del visitante

Firmas _____ Elaborado _____ Revisado

Anexo N° 9

Empresa: AJTECNOLOGÍA, S.A. DE C.V.

Lista de chequeo de equipos

Fecha:_____

Encargado del equipo:_____
Código de activo:_____
Tipo de activo:_____
Jefe inmediato:_____
Área de trabajo:_____

Observaciones:_____

Hardware		Software	
Equipo	Estado		Estado
Monitor		Respaldos de información	
CPU		Accesos autorizados	
Memoria *Ram*		Puertos USB	
Disco duro		Privilegios asignados	
Mouse		Activación de antivirus	
Teclado		Acceso a redes	
Teléfono celular			
Escritorio			
Otras_____			
Otras_____			

Comentarios:

_____ _____ _____
Responsable del equipo Gerente general Depto de TI