UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

"EVALUACIÓN DE RIESGOS INFORMÁTICOS RELACIONADOS A LA GENERACIÓN DE INFORMACIÓN FINANCIERA CONTABLE EN LAS EMPRESAS QUE COMERCIALIZAN EQUIPOS MÉDICOS DEL ÁREA METROPOLITANA DE SAN SALVADOR"

TRABAJO DE INVESTIGACIÓN PRESENTADO POR:

Alvarado Girón, José Jayro

Merino Mercado, Wendy Carolina

Rolin Velásquez, Evelyn Beatriz

PARA OPTAR EL GRADO DE:

LICENCIADO EN CONTADURÍA PÚBLICA

JUNIO, 2019

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES UNIVERSITARIAS

Rector:	Máster Roger Armando Arias Alvarado
Secretario:	Lic. Cristóbal Hernán Ríos Benítez
Decano de la Facultad de Ciencias Económicas:	Lic. Nixon Rogelio Hernández Vázquez
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
Coordinador de Seminario de Procesos de Graduación de la Escuela de Contaduría Pública:	Lic. Daniel Nehemías Reyes López
Docente Director:	Licda. María Margarita de Jesús Martínez de Hernández
Jurado examinador:	Lic. Daniel Nehemías Reyes López Lic. Carlos Ernesto Ramírez

Marzo, 2019

San Salvador, El Salvador, Centroamérica.

AGRADECIMIENTOS

Doy gracias a Dios y nuestra madre la Virgen María por darme la fuerza y fortaleza para seguir adelante a lo largo de estos años. A mis padres que con mucho amor y sacrificio siempre me han apoyado, mis familiares que me ayudaron con sus consejos y cariño. A mis compañeras de tesis por sus incansables esfuerzos para culminar satisfactoriamente esta meta; agradezco además a nuestra docente directora por su guía y el tiempo que nos brindó. A mi novia por su apoyo y finalmente a todos aquellos que me brindaron su apoyo moral y profesional a lo largo de este recorrido.

José Jayro Alvarado Girón

Doy gracias a Dios por ofrecerme la oportunidad de haber concluido con mi educación superior, por su infinito e incondicional apoyo recibido en mi vida. También expreso mi gratitud a mi compañera de tesis Evelyn Rolin por el esfuerzo realizado para poder concluir con este proyecto, a mi mamá, mis hermanos que me motivaron a concluir con mi carrera, mis hijas Keilly y Valeria que a pesar de su corta edad me dieron ánimos para poder concluir con el proceso.

Wendy Carolina Merino Mercado.

Gracias a Dios por su infinito amor y permitirme haber culminado esta etapa de mi carrera, por darme paciencia, sabiduría y fortaleza para luchar por mis sueños. Les agradezco a mis padres Lilian de Rolin, Wilfredo Rolin y mis dos hermanos Oscar Rolin y Carlos Rolin por su apoyo incondicional a lo largo de mi carrera profesional, por siempre darme ánimos para no desmayar y recordarme que no debemos quedarnos estancados sino luchar con todas nuestras fuerzas hasta lograr nuestros objetivos. También agradezco a mis compañeros, con los cuales compartí alegrías y tristeza, pero sin embargo logramos nuestro objetivo.

Evelyn Beatriz Rolin Velásquez

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN EJECUTIVO

Las empresas dependen de la tecnología de la información como una herramienta esencial para el logro de sus objetivos y para el desarrollo de sus actividades operacionales de cada usuario; al mismo tiempo se enfrentan a una amplia gama de amenazas y vulnerabilidades que están asociadas al entorno informático.

Proteger la información, es un problema en el que la solución no es solo la implementación de tecnología como *firewalls, gateways* y antivirus se debe adoptar un enfoque proactivo para identificar y proteger los activos más importantes; con el fin de evaluar y mejorar la eficacia de los procesos en la generación de la información financiera contable. El alcance que esta posee internamente en las empresas es amplio ya que incluye todas las áreas tecnológicas como son el hardware, software, seguridad física, seguridad lógica, redes recursos humanos y procesamiento electrónico de datos.

El propósito del presente trabajo es proporcionarle a las entidades que se dedican a la comercialización de equipos médicos un modelo de evaluación en la generación de la información financiera contable, ya que es importante que se identifique, analice, valore y se dé un tratamiento a las áreas críticas, así como también los procedimientos en el flujo de esta, según la Norma Técnica Salvadoreña ISO 31000:2018 proporciona las directrices para la gestión del riesgo y su implementación es responsabilidad de la alta dirección.

La recolección de los datos se llevó acabo por medio de cuestionarios con preguntas cerradas y de selección múltiple que se realizó a los encargados de tecnología y los contadores públicos autorizados por el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría (CVPCPA),con el fin de conocer la situación de las empresas comercializadoras de insumos

médicos en relación con la seguridad de la información en el entorno interno y externo; posteriormente se procedió a realizar un diagnóstico de los datos obtenidos, con el fin de identificar los puntos vulnerables al realizar una evaluación de riesgos informáticos.

Según la interpretación de los datos obtenidos en los cuestionarios se confirmó que las empresas que se dedican a la comercialización de insumos médicos, les seria de utilidad un modelo de evaluación de riesgos informáticos en la generación de la información financiera contable.

INTRODUCCIÓN

La evaluación de riesgos informáticos es esencial para salvaguardar los activos en las organizaciones. La aplicación sistemática de políticas, procedimientos y prácticas en relación a los sistemas de información se define en un adecuado proceso de la gestión del riesgo, asegurando la integridad y confidencialidad de los datos según las necesidades de cada sector.

Las deficiencias que se pueden generar como resultado de no implementar lineamientos en la generación de información son de tipo estratégicos, ejecución de programas, administración de datos y operaciones efectivas, por lo cual el compromiso de las organizaciones es asegurar la implementación de controles que contribuyan en cumplir con los objetivos trazados, la misión y visión.

La propuesta del trabajo de investigación es aportar ante la falta de una evaluación de riesgos tecnológicos en el procesamiento electrónico de datos, responsabilidad que es delegada por la alta gerencia hacia los encargados de tecnologías de información y contadores públicos, razón por la que se elaboró un modelo que está basado en la Norma Técnica Salvadoreña ISO 31000:2018, ya que su aplicación conlleva a crear y generar valor en los procesos de la organización.

La investigación se encuentra estructurada en cuatro capítulos con el siguiente contenido sintetizado: En el primer capítulo se presenta el desarrollo de la situación problemática del sector en estudio, la justificación de la investigación, los objetivos planteados, así como las limitaciones que surgieron durante el desarrollo del estudio.

En el segundo capítulo se detalla el estado actual de la seguridad de la información en las empresas que comercializan equipo médico, las principales definiciones y teorías que facilitan la

comprensión del trabajo de investigación, asimismo, en este capítulo se establece la normativa técnica y legal aplicable.

El tercer capítulo contiene el diseño metodológico, definiendo el enfoque y tipo de investigación, la delimitación espacial y temporal, las unidades de análisis, las variables objeto de medición, las técnicas e instrumentos utilizados para recopilar la información, además se presenta el procesamiento, el análisis y posterior interpretación de los datos procesados, finalizando con el diagnóstico de las unidades de análisis sujetas a investigación.

En el cuarto capítulo se desarrolla la propuesta de evaluación de riesgos informáticos, presentando inicialmente un estudio sobre la comprensión de la organización así como su entorno, detallando un análisis del contexto interno y externo de la entidad, sus procesos relevantes incluyendo su cultura organizacional, posteriormente se plantea un diagnóstico de aplicación de la Norma ISO 31000;2018 mediante una serie de cuestionarios de evaluación del control interno informático en las áreas de hardware, software, seguridad física, seguridad lógica, redes, recursos humanos y procesamiento electrónico de datos, dando como resultado una matriz de riesgos así como un diagnóstico de la evaluación de las áreas antes mencionadas.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. SITUACIÓN PROBLEMÁTICA DEL SECTOR VENTA DE EQUIPOS E INSUMOS MÉDICOS

En El Salvador la medicina presenta grandes cambios, adoptando técnicas de vanguardia, y adquiriendo equipos e insumos de laboratorios avanzados, por lo cual el personal se capacita para estar preparado y ofrecer servicios de primer nivel. La utilización de la tecnología médica radica en las prestaciones que puedan tener el equipo, y la calidad del servicio. Esto se traduce en la seguridad desde que se está diseñando, produciendo y durante su uso en los pacientes, como para el personal médico que lo opera. Otro aspecto importante es la seguridad de la tecnología médica usada para el entorno o medio ambiente en que está expuesto. En nuestro país desde el 2010 está incursionando en el mercado del turismo médico, ahora preparado con tecnología y servicios exportables de alta calidad.

Estas empresas cobran importancia ya que deben suplir las necesidades que el sistema de salud público y privado tiene de equipo e insumo médico para la atención de sus pacientes; además participan en procesos de licitaciones públicas para la suministración de sus productos así como los servicios de mantenimiento que ofrecen , por lo que se valen de procesos de compra que generan ingresos a distintos sectores; la comercialización de mercancías que ofrecen dichas entidades genera en la economía nacional un flujo de efectivo tanto para quien ofrece el equipo, como para quien lo adquiere, dando un poder de compra en la cadena de consumo alimentando así la economía del país.

Las organizaciones con el afán de crecer y optimizar sus recursos están automatizando sus procesos, con el fin que esto les permita mejorar sus controles en la seguridad de la información, aunque en la mayoría no hay una evaluación eficiente que les ayuden a minimizar los riesgos

internos informáticos. Según un informe presentado por la firma de seguridad informática ESET, El Salvador es el segundo país de Centroamérica con la mayor cantidad de casos de ataques por programas malignos, y el tercero con más incidentes de seguridad informática en general (El instrumento fue elaborado en 2016 con una muestra de 4,000 entidades de 13 países latinoamericanos. En El Salvador la muestra consideró 227 empresas de diferentes rubros y tamaños). (grafica, 2017)

El caso Troll Center en El Salvador marcó en el año 2017 un antecedente en cuanto a ciberataques y delitos en contra de distintivos comerciales y violación de derechos de autor, que impactaron en los resultados económicos de la empresa a cargo del periódico de La Prensa Gráfica. Por lo tanto, la generación de la información financiera contable no se encuentra exenta de este tipo de ataques que pueden contribuir al desprestigio de la entidad. (elsalvador.com, 2017)

Uno de los elementos claves de la seguridad en el procesamiento electrónico de datos es el de analizar las amenazas y vulnerabilidades; en dicha actividad se intenta identificar la manipulación, publicación no autorizada, fuga de información, ataques por virus, sabotajes y alteraciones entre otros, estos factores han cobrado visibilidad en distintos ámbitos que potencialmente afectarán a los equipos informáticos de una organización y con base en ello se procede al establecimiento de una serie de acciones orientadas hacia su gestión. Esta estimación se realiza mediante la protección de los activos, del análisis en la magnitud del potencial impacto o pérdida y de la probabilidad que dicho daño ocurra. (Gelbstein, 2014)

El monitoreo y mejora del control interno, también un uso adecuado en tecnologías de la información son relevantes para este tipo de empresas, que deben actualizarse según los cambios tecnológicos en el mercado, con nuevos equipos médicos de diferentes estilos y sofisticados para

mejorar la atención para sus clientes, por lo tanto es necesario que incrementen sus esfuerzos por innovar para estar a la altura de las exigencias del sector y la competencia, así como utilizar en sus sistemas buenas prácticas en seguridad informática, como resultado de una evaluación de riesgos; a medida que avanza la tecnología estas empresas podría ser víctima de un desfase frente a la competencia, logrando obstaculizar el normal funcionamiento como puede ser intrusiones, modificaciones y/o información inexacta, denegación de servicios, entre otros.

El propósito de los controles internos informáticos es verificar que los recursos, información, energía, dinero, equipo, recursos humanos, sistemas informáticos y materiales son adecuadamente coordinados por el gobierno de la entidad o por quien ellos designen.

Es importante realizar una evaluación en cuanto a los controles informáticos de los activos tangibles como intangibles en los que se guarda la información financiera contable, principalmente a los servidores, esto con el fin de mitigar los riesgos que se generan debido al uso inadecuado por parte de los usuarios. Algunas de las causas pueden ser:

- El personal tiene permisos de accesos que no están autorizados por los jefes inmediatos, los cuales pueden tener como resultado la pérdida de información o el ingreso de datos indebidos.

- Falta de conocimiento sobre los procedimientos a seguir para identificar los riesgos en el ingreso de la información, que contribuya a detectar los errores y el mal funcionamiento en el sistema contable.

- No existe un método para cerciorarse de que los datos ingresados, recibidos para su valoración están completos, exactos y autorizados por los encargados de cada área en la organización
- Control interno deficiente ya que permite a los usuarios tener permisos de acceso más allá de los necesarios para realizar sus actividades en la empresa, dejando así de funcionar los procedimientos para la segregación de sus obligaciones.
- Falta de procedimientos para el resguardo de los archivos y la información confidencial.
- No se realizan cambios necesarios en los sistemas contables o programas en los equipos informáticos, para minimizar el ingreso de datos al sistema de forma manual.

Los datos que generan la información financiera contable, cada día tienen un mayor valor, por esta razón surge la necesidad de mejorar los controles internos y externos, para identificar las amenazas y vulnerabilidades que enfrentan las empresas para garantizar la confiabilidad en los procesos sistematizados.

Por tanto para las entidades que se dedican a la comercialización de equipos médicos existe los riesgos informáticos, en el procesamiento de la información en el sistema, esto debido a que no se realiza una evaluación suficiente y adecuada ni existen controles y políticas relacionadas con el mantenimiento de los software o hardware; una parte de los datos se procesan de forma no automatizada y esto puede provocar que la información sea inexacta e incongruente, además al no seguir los procedimientos establecidos para el mejor funcionamiento de los sistemas podría provocar que personal no autorizado tanto interno como externo puedan realizar operaciones que puedan poner en peligro la confiablidad e integridad de los datos procesados en los sistemas informáticos.

1.2. ENUNCIADO DEL PROBLEMA

Con la realización de los cuestionarios para la evaluación de riesgos informáticos en la generación de la información financiera contable, se pretende orientar a los profesionales en contaduría pública y a los encargados de las tecnologías de la información para puedan identificar y valorar los riesgos de incorrección material para dar una respuesta oportuna según la NIA 315 y la Norma Técnica Salvadoreña ISO 31000:2018 que brindan las directrices necesarias que conlleven a la integridad y confiabilidad de la información. Lo anterior descrito permite plantear la siguiente interrogante:

¿Cómo afecta la falta de una evaluación de riesgos informáticos en la generación de información financiera contable en la captura, procesamiento, almacenamiento y salida de la información en las empresas que comercializan equipos médicos del área metropolitana de San Salvador?

1.3. JUSTIFICACIÓN DE LA INVESTIGACIÓN

1.3.1. Novedoso

El desarrollo de la investigación se considera novedoso, ya que las empresas que se dedican a la comercialización de equipos médicos no cuentan con un modelo de evaluación idóneo y suficiente para la prevención y control de riesgos informáticos relacionados a la generación de información financiera contable. Debido al acelerado crecimiento tecnológico de estos negocios; han tenido la necesidad de adquirir software para procesar los datos y así agilizar sus procesos.

Además, se considera innovador porque para su implementación se debe de tener en cuenta la aplicación de estándares internacionales y buenas prácticas para el buen uso de las tecnologías de la información, que favorezca la identificación de las áreas vulnerables y las amenazas tanto

internas como externas para cumplir con lo establecido en las normas técnicas. Este sector está interesado en resguardar sus activos de manera íntegra y confidencial con la aplicación de controles y procedimientos, con el objetivo de agregar valor al servicio que prestan, logrando así una adecuada respuesta a los riesgos inherentes.

1.3.2. Factibilidad

El trabajo de investigación se considera factible, ya que se cuenta con recursos bibliográficos como normas técnicas, documentos tecnológicos, tesis, y libros los cuales tratan sobre la evaluación de riesgos y la seguridad de la información.

Además se cuenta con los recursos financieros, con el apoyo de un asesor especialista y un asesor metodológico asignado por la Escuela de Contaduría Pública de la Facultad de Ciencias Económicas de la Universidad de El Salvador, con conocimientos técnicos relacionados al área de estudio, quienes garantizaran que se cumplan con los objetivos, metas y calendarización trazada por la coordinación de trabajos de graduación; se cuenta con la colaboración de las empresas objeto de estudio, que suministraran información relevante para el desarrollo de la propuesta del presente trabajo.

1.3.3. Utilidad Social

Al desarrollar la problemática se pretende aportar a las empresas que comercializan equipos médicos, una evaluación de riesgos informáticos relacionados a la generación de información financiera contable, con el objetivo que sus procesos sean beneficiados agregándoles valor y calidad, robusteciendo su administración y reflejándose en los resultados financieros y rendimiento de las entidades de este sector.

Asimismo, se pretende que la investigación sea útil para los profesionales en contaduría pública que se desempeñan en el área de auditoria interna y externa y los encargados del área de informática, ya que tendrán los lineamientos para realizar un diagnóstico de los procedimientos que incluya el cuidado de las áreas como son software, hardware, seguridad física y lógica, recursos humanos, redes y procesamiento electrónico de datos para implementar medidas correctivas y mitigar riesgos, al momento de realizar una auditoría a los sistemas de información, ya que podrán verificar si los controles aplicados garantizan la integridad, disponibilidad y confiabilidad de los datos.

1.4. OBJETIVOS DE LA INVESTIGACIÓN

1.4.1. Objetivo general

Desarrollar un modelo de evaluación de riesgos informáticos relacionados a la generación de información financiera contable, para determinar su integridad y confidencialidad en la captura, procesamiento, almacenamiento y salida de la información en las empresas que comercializan equipos médicos del área metropolitana de San Salvador que contribuya a determinar las principales amenazas o vulnerabilidades de los activos.

1.4.2. Objetivos específicos

- Realizar una matriz de riesgos asociados a sus activos informáticos, conociendo que elementos son críticos y clasificando los riesgos, para minimizar el grado de ocurrencia.
- Elaborar una lista de verificación que permita establecer controles oportunos al momento de generar la información financiera contable.

- Describir los procedimientos para el control de riesgos asociados en la generación de la información y la seguridad de los activos, que puedan ser evaluados constantemente por los encargados de los sistemas.

1.5. HIPOTESIS

1.5.1. Formulación de la hipótesis

Conforme a la problemática determinada la hipótesis se establece de la siguiente manera:

La propuesta de un modelo de evaluación de riesgos informáticos en la generación de información financiera contable contribuirá a la mejora de la integridad y confidencialidad en la captura, procesamiento, almacenamiento y salida de la información en las empresas que comercializan equipo médico del área metropolitana de San Salvador.

1.5.2. Determinación de variables

Variable independiente: El modelo de evaluación de riesgos informáticos en la generación de información financiera contable.

La variable independiente se considera así porque es la causa o razón de la problemática a investigar, es decir la falta de un modelo de evaluación de riesgos informáticos en la generación de información financiera contable incide directamente en la mejora de la seguridad y contribuye a que sea relevante para la toma de decisiones en las empresas que comercializan equipos médicos del área metropolitana de San Salvador.

Variable dependiente:

La mejora de la integridad y confidencialidad en la captura, procesamiento, almacenamiento y salida de la información.

La variable dependiente es el efecto de no contar con un modelo de evaluación de riesgos informáticos, de manera que, si no se cuenta con tal modelo, este no ayudara a mejorar la seguridad en la generación de información financiera contable y por tanto los procesos de suministro de información a los usuarios se seguirán viendo afectados y la información perderá confiabilidad e integridad.

1.6. LIMITACIONES DE LA INVESTIGACIÓN

- Para la obtención de la información está a disponibilidad de tiempo por parte de las unidades de análisis convirtiéndose en una limitante para la investigación; ya que de acuerdo con el tiempo disponible así será la amplitud o brevedad de las respuestas para la recopilación de la información.
- Debido a políticas internas por parte de las empresas puede ser que no se brinde información relevante o suficiente por ser clasificada como información confidencial del sector.
- Los contadores públicos autorizados carecen de conocimientos en tecnologías de la información, ya que es un área en la cual no se capacitan con frecuencia.
- Cuando se encuesto se obtuvo una limitante en cuanto algunas empresas que no poseen área de tecnologías de la información, sin embargo, se tuvo que suplir la muestra a entidades que tienen una actividad similar al sector objeto de investigación.

CAPÍTULO II: MARCO TEÓRICO, CONCEPTUAL, TÈCNICO Y LEGAL

2.1. ESTADO ACTUAL EN LA SEGURIDAD DE LA INFORMACIÓN EN LAS EMPRESAS QUE COMERCIALIZAN EQUIPOS MÉDICOS.

En El Salvador con el crecimiento acelerado de la tecnología las empresas han tenido la necesidad de realizar inversiones tecnológicas implementando sistemas de información, software, aplicaciones, conexiones en red e internet para hacer más eficientes sus procesos y mejorar sus servicios.

Sin embargo, actualmente la información se ha convertido en uno de los activos principales de las empresas, estando expuesta a diversas amenazas o vulnerabilidades en la generación de información financiera contable, debido al volumen de operaciones procesadas a diario en los sistemas, además los reportes emitidos por estos son de utilidad para la toma de decisiones, por lo tanto se debe tener la certeza que los datos sean seguros en los procesos de captura, procesamiento, almacenamiento y salida de información. (Baca Urbina, 2016)

Debido a lo expuesto en el párrafo anterior, es necesario realizar una evaluación de control interno informático para garantizar la fiabilidad e integridad de los datos, así mismo identificar los principales riesgos en los que se encuentran más vulnerables los activos, en los cuales podría con llevar a la explotación de amenazas en el entorno físico y lógico de las organizaciones de la problemática en estudio.

2.1.1. Generación de la información financiera contable

La información financiera es originada de la contabilidad y cada día tiene un mayor valor, ya que es útil para la toma de decisiones, por esta razón surge la necesidad de una protección adecuada que garantice la disponibilidad y razonabilidad de las cifras, además al realizar una

evaluación de riesgos informáticos se debe considerar el almacenamiento, procesamiento, transmisión, y las tecnologías usadas para el resguardo de los datos.

Los sistemas contables están basados en proveer reportes y estados financieros para identificar todas las operaciones realizadas durante el periodo contable y que facilite las decisiones económicas de la compañía dentro y fuera de la misma para maximizar la riqueza, enfatizando en temáticas como la inversión, financiación y distribución de las utilidades para así cumplir con un plan financiero de manera estratégica teniendo en cuenta la rentabilidad, el endeudamiento y la liquidez

Los registros financieros expresan las transacciones realizadas por la empresa en forma cuantitativa y monetaria, así como los acontecimientos económicos que le afectan, para dar informes útiles a los usuarios externos e internos de la organización, con el objeto de que los datos que se obtienen lleguen con oportunidad, eficiencia y calidad adecuadas para la efectiva toma de decisiones en los diferentes niveles jerárquicos de la entidad. Tiene como principal objetivo organizar y unificar el flujo de la información incluyendo toda la relación entre los derechos y obligaciones de la empresa, así como la composición de su patrimonio en un momento determinado.

La adopción de un software ERP (*Enterprise Resource Planning*), que contribuya a la automatización de los procesos para el ingreso de las cifras financiera, en cada empresa, permite registrar, agrupar y presentar los estados financieros en forma integral, utilizando normas nacionales que logren la compatibilidad con las internacionales para mejorar la operación, administración y control de los recursos de la organización.

En cuanto a la información administrativa la contabilidad se pone al servicio de las actividades internas de la administración para facilitar las funciones de planeación y control. Entre las aplicaciones se encuentran la elaboración de presupuestos, la determinación de los costos de producción y la evaluación de la eficiencia de las diferentes áreas de la entidad. Los datos generados por los sistemas son de utilidad para los usuarios internos los cuales están representados por los gerentes generales, de ventas, financieros y de operaciones, jefes de los departamentos, entre otros. (Perla D. Lezanski, 2016)

Los sistemas contables son la interacción de varias ramas que se simplifican en los estados financieros, es preciso identificar cuáles son los puntos a tener en cuenta para la presentación de la información contable de acuerdo a las directrices

De acuerdo con el avance de las tecnologías y a la inserción en los países, la información puede ser generada a partir de software contable o ERP los cuales permiten obtener informes de inmediato pero que el usuario interactúe constantemente con este para la inclusión de los datos diarios obtenidos. Sin la relación usuario-software, este no se podría ajustar por si solo sin el conocimiento del usuario.

Las tecnologías que han convertido en una herramienta facilitadora para la contabilidad, ya que los avances tecnológicos que son incorporados en los sistemas contables computarizados posibilitan el manejo de gran volumen de datos convirtiéndose en información valiosa para las empresas, para el manejo operativo, gerencial y el cumplimiento de los objetivos estratégicos. A través del uso de sistemas computarizados se logra obtener una ventaja comparativa al realizar un empleo mejor de sus recursos. Por lo tanto, es indispensable contar con un sistema, confiable, seguro, accesible y sencillo que sustente las operaciones de la entidad.

2.1.1.1.Diferencia entre información financiera y contable.

La función principal de la contabilidad es la obtención de información respecto a las actividades financieras de empresas e instituciones, de tal manera que los usuarios se encuentren en condiciones apropiadas para tomar decisiones. Se pueden clasificar a los usuarios de la contabilidad en dos grupos. En el primero se ubican quienes usan la contabilidad para fines internos, es decir la utilización de esta disciplina por parte de los administradores de negocios para ayudar a resolver problemas financieros. Al segundo grupo pertenecen los usuarios que no tienen acceso o contacto con las operaciones de un determinado negocio, como son bancos, inversionistas, proveedores, etc.

Las finanzas son la parte de la economía que se encarga de la gestión y optimización de los flujos de dinero, tienen como objetivo maximizar el valor de la empresa y garantizar que se puede cumplir con las salidas de efectivo.

La contabilidad va a obtener la información que se utiliza, y las finanzas su finalidad es para coordinar y dirigir las entradas y salidas de efectivo. (Roca, 2016)

2.1.2. Procesamiento electrónico de datos (PED)

Consiste en la recolección de los datos primarios de entrada, que son evaluados y ordenados, para obtener información útil, que luego serán analizados por el usuario final, para que pueda tomar las decisiones o realizar las acciones convenientes.

Los sistemas de información deben tener cuatro actividades básicas:

- Ingreso de información: el sistema tiene los datos requeridos
- Almacenamiento: conservar la información

- Procesamiento: transformación de datos como fuente de información para la toma de decisiones
- Salida de información: Mostrar los datos ingresados para el entorno exterior (Cohen Karen, 2009)

Es por esto que se desarrolla un esquema en el cual se demuestra las diferentes etapas para la generación de información financiera contable en los sistemas de información, En la figura 1 se muestra la clasificación del procesamiento electrónico de datos.

Planes de acción para el procesamiento electrónico de datos

- Controles de exactitud: validación de datos y excesos.
- Control de totalidad de datos: conteo de registros y cifras.
- Controles de redundancia: cancelación por lotes, verificación de secuencias.
- Control de existencia: bitácora de datos, mantenimiento de activos dados de baja.
- Periodicidad de cambio de claves del sistema aplicativo
- Procedimientos contra caídas del sistema (Reyes, 2017)

2.1.3. Procesamiento de información en los sistemas informáticos

Los sistemas y las tecnologías son una nueva herramienta presente en las organizaciones, que se suma a otras áreas como las finanzas, la contabilidad, los recursos humanos, la logística y las operaciones además, a partir de su uso se logran importantes mejoras, como la automatización de los procesos operativos que proporcionan información que sirve de apoyo para el logro de los objetivos y lo que es más importante, es su implementación que facilita el logro de ventajas competitivas.

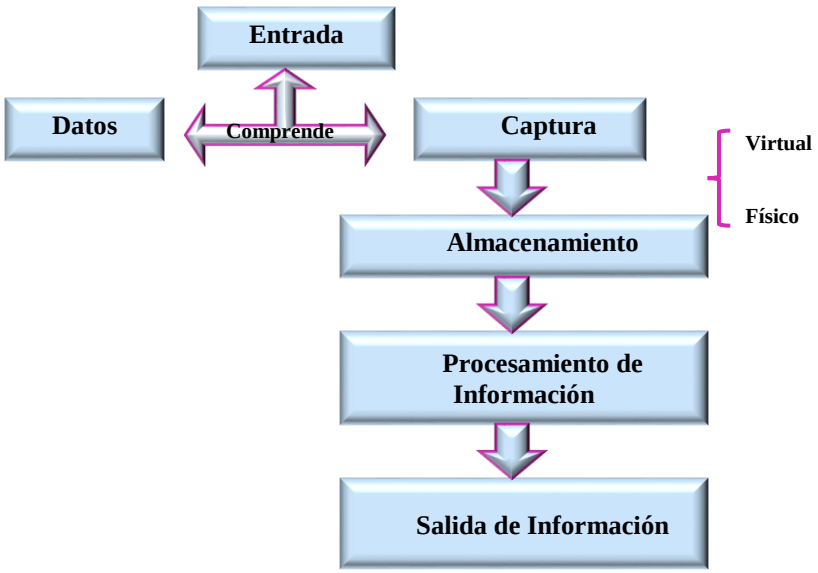


Figura 1: Clasificación del Procesamiento Electrónico de Datos. **Fuente:** Material Didáctico de la Asignatura de Sistemas Contables Computacionales.

Los sistemas de información cumplen tres objetivos básicos dentro de las organizaciones:

- Automatizan los procesos operativos.
- Proporcionan cifras que sirve de apoyo en el proceso de toma de decisiones.
- Logran ventas competitivas a través de su implantación y uso.

Cuando las organizaciones automatizan sus procesos operativos se les llama sistemas transaccionales, ya que su función principal consiste en procesar transacciones, tales como pagos, cobros, entradas y salidas, etc. El complemento de dichos sistemas son los relacionados a la mejora de toma de decisiones, cuya función es la manipulación de la información con el fin de apoyar y fundamentar el cumplimiento de los objetivos. (Cohen Karen, 2009)

2.1.3.1.Ventajas y limitantes

Ventajas: velocidad, volumen de producción, reducción de errores, pases automáticos al mayor, información oportuna, menos costes, entre otros.

Limitantes: disminución en calidad de información, difícil auditoria, altos niveles de capacitación.

2.1.4. Principales riesgos en la generación de información financiera contable

Entre las amenazas principales se encuentran las relacionadas con el hardware, software, seguridad física y lógica, recursos humanos y redes tales como, el daño físico a las computadoras, alteraciones en las aplicaciones; uso inadecuado del equipo informático por parte del usuario ya que todos los sistemas de información son susceptibles al robo de datos, códigos maliciosos, accesos no autorizados por la falta de políticas en la seguridad informática.

Los riesgos antes mencionados se deben disminuir o erradicar a través del diseño e implementación de controles internos informáticos. La seguridad y la protección de los recursos tecnológicos deben relacionarse con la misión y los objetivos pro de la entidad diseñándose a partir de un análisis de las necesidades de la organización.

2.1.5. Activos de información

El primer paso de una evaluación en la seguridad de la información es realizar un levantamiento de inventario completo y exhaustivo de todos los activos de la organización. Los activos de información son los elementos que generan, procesan, utilizan, a su vez brindan valor a la organización y ayudan a cumplir los objetivos estratégicos. Estos pueden incluir software, hardware, personal, sistemas, ambientes físicos, entre otros.

Los activos de son almacenes de información que pueden contener datos como financieros y contables, registros confidenciales y campos que ayudan a rastrear los fines de su utilización. (Knight, 2017, pág. 8)

2.1.5.1.Clasificación

Los activos tienen como objetivo asegurar que se tenga niveles de protección adecuados, ya que con base en su valor y de acuerdo con otras características requiere un manejo especial. Debe estar realizada considerando las dimensiones de confidencialidad, integridad y disponibilidad esto se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados, esta se debe definir de acuerdo con las características de los activos que se manejan en cada entidad.

La clasificación por confidencialidad es la siguiente:

- **Información Pública:** no necesita de un control de acceso, puede ser conocida por terceros sin autorización ya que la información está disponible de forma transparente.
- **Acceso autorizado:** la información es privada y requiere de un acceso para poder ingresar.
- **Sensible**: información crítica y altamente protegida.

La integridad se refiere a la exactitud y completitud, esto permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción.

- **Alta:** pérdida de información que puede tener un impacto negativo ya sea de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
- **Media**: pérdida de información que puede tener un impacto negativo ya sea de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen moderada de la entidad
- **Baja:** información cuya pérdida no tiene un impacto significativo para la entidad o entes externos. (Condori Rivera, 2017, págs. 18-20)

2.1.5.2.Amenazas y vulnerabilidades

La implementación de una evaluación en la seguridad de la información financiera contable, en esta se pueden identificar las áreas más vulnerables, determinar cómo debe ser tratada cada una de ellas y las acciones que dan respuestas a la amenaza. Como resultado de esta evaluación hemos de tener:

- Priorización de los sistemas.
- Definición de roles y responsabilidades respecto a la gestión.
- Identificación, para cada software y tecnología, de fuentes relevantes de información.
- Análisis de un evento o acontecimiento para incorporar una actualización relacionado con una vulnerabilidad, para determinar los pasos a realizar, que puede incluir la realización de nuevos controles para evaluar que no hay efectos adversos sobre otros sistemas. (Publishing, 2011)

En la figura 2 se expresa como los activos de información se encuentran expuestos cuando existen amenazas que pueden explotar las vulnerabilidades existentes.

2.1.6. Control interno informático.

Este controla diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijadas por la dirección informática, así como los requerimientos legales.

La misión es asegurarse de que las medidas que se obtienen de los mecanismos implementados por cada responsable sean correctas y válidas.

2.1.6.1.Tipo de control interno

El control interno se materializa fundamentalmente en dos tipos:

- **Manuales:** son aquellos que son ejecutados por el personal del área de informática sin la utilización de herramientas computacionales.
- **Automáticos:** son incorporados en el software, llámense estos de operación, comunicación, gestión de datos y programas de aplicación.

Según su finalidad:

- **Preventivos:** para tratar de evitar la producción de errores o hechos, fraudulentos.
- **Detectivos:** tratan de descubrir a posteriori errores o fraudes que no haya sido posible evitarlos con controles preventivos.
- **Correctivos:** estos tratan de asegurar que se subsanen todos los errores identificados mediante los controles detectivos. (Piattini, 2011, pág. 30)

2.1.6.2.Evaluación del riesgo informático

La información es un activo valioso para las organizaciones empresariales y se hace necesario brindarles una protección adecuada frente a las posibles intrusiones derivadas de los riesgos existentes en sus sistemas contables. Una manera efectiva de descubrir estas vulnerabilidades y amenazas es iniciando los procesos de diagnósticos que permitan establecer el estado actual de la seguridad y monitoreo de los controles internos dentro de la organización, teniendo en cuenta la normativa vigente y los procesos de análisis y evaluación de los conflictos externos e internos.

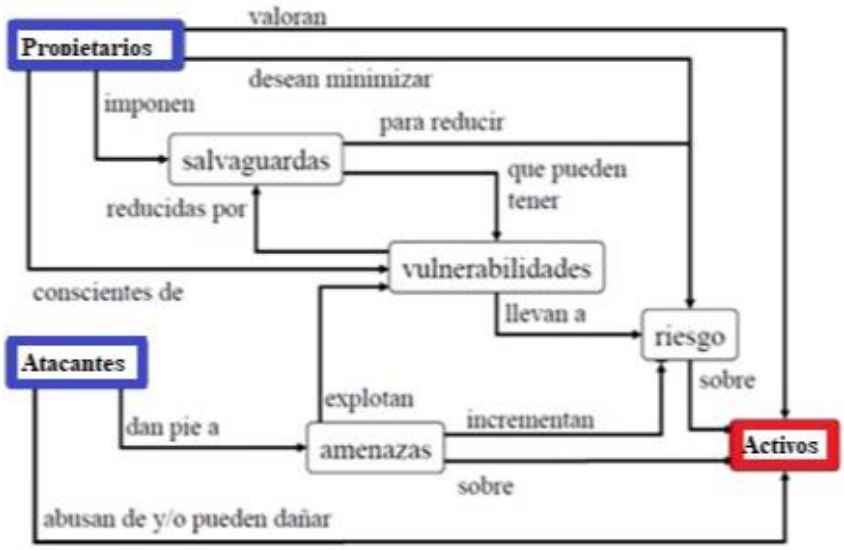


Figura 2: Relación de las Vulnerabilidades con los Otros Elementos de la Seguridad de la Información. **Fuente:** QANEWBLOG "Evaluación de la Seguridad de los Sistemas Informáticos: Políticas, Estándares y Análisis de Riesgos"

La administración de riesgos es reconocida como una parte integral de las buenas prácticas gerenciales. Es un proceso iterativo que consta de pasos, los cuales, cuando son ejecutados en secuencia, posibilitan una mejora continua en el proceso de toma de decisiones. Las herramientas derivadas de una buena administración sirven precisamente para estas funcionalidades, ayudan a identificar los recursos importantes en la entidad,

El análisis y evaluación de riesgos, la verificación de la existencia de controles de seguridad, las pruebas con software y el monitoreo de los sistemas de información permiten establecer el estado actual de la organización, identificar las causas de las vulnerabilidades y proponer soluciones de control que permitan su mitigación de las mismas.

2.1.6.3.Importancia de una evaluación de riesgos

Si la empresa no conoce sobre el riesgo que corren sus activos de información difícilmente llegara a estar preparada para evitar su posible ocurrencia, de ahí la importancia de realizar una

eficiente evaluación en los procedimientos de la entidad, ya que ayuda a la gerencia a tomar decisiones, basadas en los resultados del análisis sobre los riesgos que necesitan tratamiento y las prioridades para brindar una solución.

La evaluación del riesgo implica comparación del nivel de riego hallado durante el proceso de análisis con los criterios establecidos, se deben considerar los objetivos a cumplir dentro de la organización, con el fin de alinearlos a la oportunidad que podría generarse al realizar esta gestión.

Los activos de información deben ser identificados por su impacto en las organizaciones, luego se debe de realizar un análisis para determinar que activos están bajo riesgos y pueden llegar a afectar en la generación de la información financiera contable. (Freitas, 2009, pág. 47)

En cuanto a las directrices para gestionar el riesgo, análisis y tratamiento existe un estándar ISO 31000:2018 que incluye una serie de recomendaciones y actividades para que las organizaciones mejoren sus procesos de una forma más adecuada y eficaz, la norma proporciona ocho principios fundamentales con el propósito de crear valor, mejora el desempeño y fomentar la innovación que contribuirá al logro de los objetivos.

En la figura 3 se muestran los principios que toma en cuenta la ISO31000:2018 que contribuyen a la orientación sobre las características de una gestión eficaz y eficiente comunicando su valor y explicando su intención y propósito.

Después de introducir los principios y el marco de trabajo, se debe desarrollar un conjunto de fases y pasos recomendados para que las organizaciones lo adapten e implante correctamente, consiguiendo mejoras en la efectividad y precisión ante posibles amenazas.

Figura 3: Principios Generales de la ISO31000. ***Fuente:*** NTS ISO 31000:2018, Gestión del Riesgo. Directrices

2.1.7. Identificación de los riesgos y errores materiales.

Según lo establecido en la NIA 315 se debe evaluar los riesgos a través del conocimiento y la comprensión de sus operaciones, la estructura de su gobierno y su entorno interno y externo de la organización, se realizará un análisis de las cinco fuerzas de Porter que son esencialmente un concepto en los negocios por medio del cual se pueden maximizar los recursos y superar a la competencia.

Según Porter, si no se cuenta con un plan perfectamente elaborado, no se puede sobrevivir en el mundo de los negocios de ninguna forma; lo que hace que el desarrollo de una estrategia competente no solamente sea un mecanismo de supervivencia, sino que además también te da acceso a un puesto importante. Se tomará en cuenta también el análisis de PESTEL (Político,

Económico, social, tecnológico, ecológico, legal), para detectar aquellas variables que tendrían algún tipo de influencia en el desarrollo de la entidad y el entorno.

2.1.8. Evaluación del riesgo

Es el proceso global de identificación, análisis y valoración del riesgo; esta se debería llevar acabo de manera sistemática, iterativa y colaborativa, basándose en el conocimiento y los puntos de vista de las partes interesadas. Se debería utilizar la mejor información pertinente, complementada investigación adicional, si fuese necesario.

2.1.9. Identificación del riesgo

Su propósito es encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a una organización lograr sus objetivos, se necesita contar con una herramienta o técnica adecuada definida por cada entidad, además de que las personas que ejecuten esta actividad deben tener el conocimiento apropiado sobre el proceso a evaluar. Se deben tener en cuentas todos los riesgos, esto quiere decir que se deben listar tanto los que tienen controles aplicados, como los que no.

La entidad debería identificar los riesgos, tanto si sus fuentes están o no bajo su control. Se debe tomar en cuenta que puede haber más de un tipo de resultado, que puede dar lugar a una variedad de consecuencias tangibles o intangibles.

2.1.10. Análisis del riesgo

Consiste en comprender la naturaleza del riesgo y sus características incluyendo, cuando sea apropiado. El análisis implica una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su eficacia. Un evento puede tener múltiples causas y efectos que pueden afectar a los objetivos de la entidad.

Sin embargo, se pueden realizar un análisis con diferentes grados de detalle y complejidad, dependiendo del propósito, la confiabilidad de la información y los recursos disponibles.

El análisis de riesgos debe considerar factores tales como:

- La probabilidad de los eventos y sus consecuencias.
- La naturaleza y la magnitud que pueden originar.
- La complejidad e interconexión.
- Los factores relacionados con el tiempo y la volatilidad.
- Eficacia de los controles existentes.

El análisis proporciona una entrada para la valoración del riesgo, para las decisiones sobre la manera de cómo tratarlo y si es necesario hacerlo.

2.1.11. Valoración del riesgo

Existen dos aspectos generalmente usados para este fin; la probabilidad que se entiende como la posibilidad de ocurrencia de un evento y esta puede ser medida con criterios de frecuencia, si se ha realizado o de factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar, aunque este no se haya materializado. En conclusión, se entiende como la cantidad de veces que se puede repetir el riesgo.

Su propósito es apoyar a la dirección en la toma de decisiones, también implica hacer una comparación de los resultados del análisis con los criterios establecidos para determinar cuándo se requiere de una acción adicional.

Los resultados de la valoración deberían registrar, comunicar y luego validar a los niveles apropiados de la organización.

2.1.12. Tratamiento del riesgo

Está basado en la identificación de los mejores métodos definidos, para tomar una decisión sobre cada uno de estos teniendo en cuenta una serie de aspectos como: Aceptar, transferir,

mitigar y evitar el impacto que se genere por la ejecución de las actividades diarias de los usuarios en los equipos informáticos.

Se selecciona e implementa opciones para abordar el riesgo. El tratamiento implica un proceso iterativo de:

- Formular y seleccionar opciones para el tratamiento del riesgo.
- Planificar e implementar.
- Evaluar la eficacia de ese tratamiento.
- Decidir si el riesgo residual es aceptable.

2.1.13. Seguimiento y revisión

El propósito de esta fase es mantener actualizado los procedimientos para la mitigación de los riesgos, ya que a medida que ocurren cambios en el contexto interno y externo en la organización, puede ser necesario ajustar el marco de trabajo para asegurar que sigue siendo eficaz.

Los resultados del seguimiento y la revisión deberían de incorporarse en todas las etapas del proceso en estas se incluyen la planificación, recolección, registrar y analizar los resultados y así proporcionar una retroalimentación para una adecuada gestión de riesgos. (ISO, 31000:2018)

2.1.14. Registro e informe

El proceso de gestionar los riesgos y sus resultados se deberían documentar e informar a la alta dirección a través de los mecanismos apropiados, los cuales pretende:

- Comunicar las actividades realizadas por la gerencia y sus resultados a la organización.
- Proporcionar información para la toma de decisiones.
- Mejorar las actividades para la gestión del riesgo.

2.2. PRINCIPALES DEFINICIONES

A continuación, se detallan los principales conceptos que están directamente relacionados con el trabajo de investigación.

Activo: recurso del sistema de información necesario para el funcionamiento apropiado de la organización y la consecución de los objetivos previstos. Los activos pueden estar sujetos a amenazas tanto internas como externas.

Amenaza: es una condición del entorno de los sistemas, áreas o dispositivos que contiene información importante (persona, equipo, suceso, idea) que ante determinada circunstancia podría dar lugar a que se produjese una violación de seguridad (no cumplimiento de alguno de los aspectos mencionados) afectando parte de la información y de la TI de la organización. (Baca Urbina, 2016)

Confidencialidad: es preservar las restricciones autorizadas sobre el acceso o divulgación, incluyendo los medios para proteger la privacidad y la información propietaria. (ISACA, 2012)

Control interno informático: se define como el sistema integrado al proceso administrativo, en la planeación, organización, dirección y control de las operaciones con el objeto de asegurar la protección de todos los recursos informáticos y mejorar los índices de economía, eficiencia y efectividad de los procesos automatizados.

Integridad: consiste en proteger contra la destrucción o modificación inadecuada de la información e incluye asegurar el no repudio y autenticidad de la información. (ISACA, 2012)

Políticas: directrices operativas que establecen como una organización desarrolla su actividad. Focalizan procesos y procedimientos internos. (Soy i Aumatelli, 2013)

Riesgo informático: se refiere a la incertidumbre existente por la posible realización de un suceso relacionado con la amenaza de daño respecto a los bienes o servicios informáticos.

Vulnerabilidad: constituye un hecho o una actividad que permite concretar una amenaza. Si es vulnerable en la medida en que no hay suficiente protección como para evitar que llegue a suceder una amenaza. (Baca Urbina, 2016)

2.3. NORMATIVA TÉCNICA APLICABLE

Tabla 1

Base técnica

Normativas implicadas en la aplicación del trabajo	Contenido relacionado de la Normativa a la investigación	Descripción especifica.
COBIT 5.0 Seguridad de la Información	Partes interesadas	Externas: sociedad en general, clientes, proveedores, autoridad de contralor, auditores externos Internas: órgano de administración y de gobierno, responsables de los procesos de negocios, del sistema de registro contable, de la TI, del cumplimiento y auditores internos.
	Procesos de gobierno y gestión	-Evaluar, orientar y supervisar (EDM) -Alinear, planificar y Organizar (APO) -Entrega, Servicio y Soporte (DSS)
	Catalizador de información (Apéndice E)	-Políticas de seguridad -Se proporciona detalles sobre el uso y la optimización de los tipos de información relacionados con la con la seguridad de información.
	Catalizador de servicios, infraestructura y aplicaciones (Apéndice F)	-Evaluaciones de seguridad -Efectuar evaluaciones de riesgos en la información: proceso por el que se proporciona una identificación, evaluación, estimación y análisis de amenazas y vulnerabilidades para una determinada entidad, sistema, proceso , procedimiento aplicación, etc.
	Catalizador de personas, habilidades y competencias	Gestión de riesgos de la información
	Mapeos	Mapeo de alto nivel entre varios estándares y marcos de referencia en el área de seguridad de la información, enfocados en el catalizador de procesos
COBIT 5.0 para riesgos	La perspectiva de la gestión de riesgos y el uso de los catalizadores.	Procesos principales de riesgos: Asegurar la optimización y gestionar el riesgo.

	Escenarios del riesgo	Flujos de trabajo en el desarrollo de escenarios de riesgo, factores de riesgo, son aquellas condiciones que influyen en la frecuencia o impacto en el negocio.
	Estructura escenarios de riesgos de TI	Es una descripción de un evento relacionado con TI, que en caso de ocurrir puede conducir a un impacto en el negocio.
	Componentes	-Marco de referencia -Descripciones de los procesos -Objetivos de control -Directrices de control -Modelos de madurez
NTS ISO 27001:2013 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información.	Contexto de la organización	La organización debe determinar asuntos internos y externos que son relevantes a su propósito y que afectan su habilidad para alcanzar los resultados esperados
	Liderazgo	La administración debe asegurar que la política de seguridad sea establecida
	Planeación	Acciones para abordar riesgos y oportunidades, evaluación y tratamiento del riesgo de seguridad de la información
	Soporte y operación	La organización debe determinar y proveer los recursos necesarios para el establecimiento, implementación, mantenimiento y la mejora continua. Evaluación de riesgos
	Evaluación del desempeño	Monitoreo, medición, análisis y evaluación, la organización debe establecer que necesita ser monitoreado y medido incluyendo procesos y controles
	Anexo A Objetivos de control y controles de referencia	-Políticas y organización de seguridad de la información -Seguridad de los recursos humanos -Gestión de activos (inventario, propietarios) -Clasificación de la información -Controles de acceso -Seguridad física y ambiental -Seguridad en las operaciones (instalaciones del PED) -Seguridad de las operaciones
NTS ISO 31000:2018 Gestión de riesgos. Directrices	Principios	El propósito de la gestión del riesgo es la creación de valor, mejora el desempeño, fomenta la innovación y contribuye al logro de los objetivos.
	Proceso de gestión del riesgo	Implica la aplicación sistemática de políticas, procedimientos y práctica a las actividades de comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registro e informe del riesgo.
	Criterios del riesgo	La organización debería precisar la cantidad y el tipo de riesgo que puede o no puede tomar, en relación con los objetivos.
	Evaluación del riesgo	Es el proceso global de identificación, análisis y valoración del riesgo. Con el propósito de identificar los riesgos que pueden impedir a una organización lograr sus objetivos.
	Evaluación del desempeño	Se debe evaluar el desempeño de la seguridad y la efectividad del sistema de gestión, incluyendo procesos y controles de seguridad de la información.

	Componentes	-Identificación -Análisis -Valoración -Tratamiento -Seguimiento y revisión -Registro e informe
Modelo del COSO ERM Gestión de Riesgos Empresariales, integrado con estrategia y desempeño	Componentes	-Gobierno y cultura -Estrategia y definición de objetivos -Desempeño -Análisis y revisión, -Información, comunicación y presentación de informes
	Principios	-La junta directiva ejerce supervisión sobre los riesgos, análisis del contexto empresarial, definición del apetito del riesgo, identificación, evaluación severa, priorización de los riesgos, implementación de respuesta, proponer mejoras en la gestión de riesgos empresariales.
	Importancia	-Aclara la gestión de riesgos empresariales en la planeación estratégica y la incorpora a toda la organización, ya que el riesgo influye y está alineado a la estrategia y el desempeño en todas las áreas, departamentos y funciones.
IES 2: Normas Internacionales de Formación	Contenido de los programas profesionales de formación en Contaduría	-Su objetivo principal es que los participantes posean conocimientos contables avanzados suficientes para poder actuar como contadores profesionales competentes en un entorno cada vez más complejo y cambiante.
IEPS 2: Declaraciones de Prácticas Internacionales de Educación	Tecnología de la Información para Contadores Profesionales	-Orienta en la implementación de IES 2 en relación con el componente de conocimiento de tecnología de información del profesional. -Al implementar los IES se debe garantizar que los profesionales poseen los conocimientos y competencias generales necesarios en materia de control de tecnologías de información. -Se pretende que los candidatos tengan conocimiento de por lo menos uno de los tres roles como Gerente, Evaluador y Diseñador de sistemas de información o una combinación de estos roles.

Elaborado por el grupo de investigación en base a normativa técnica para la evaluación de riesgos informáticos, consultadas a través de medios físicos obtenidos de las instituciones autorizadas localmente, así como información obtenida de página web oficial de las diferentes instituciones nacionales e internacionales que regulan todo lo relacionado con la problemática de estudio.

2.4. LEGISLACIÓN APLICABLE

Tabla 2
Normativa legal

Leyes aplicables al trabajo	Contenido de la ley relacionado a la investigación	Descripción específica
	Contabilidad	**Art. 435.** Establece que los comerciantes podrán llevar la contabilidad haciendo uso de sistemas electrónicos o de cualquier otro medio técnico idóneo para registrar las operaciones contables.

Código de Comercio		**Art. 439:** Regula que los comerciantes deben asentar sus operaciones diariamente y llevar su contabilidad con claridad, en orden cronológico, sin señales de alteración. **Art. 443.** Manifiesta que todo balance general debe expresare con veracidad y con la exactitud compatible con sus finalidades, la situación financiera del negocio en la fecha a que se refiera **Art. 455.** Establece que 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 emitan.
Código Tributario	Emisión de documentos	**Art. 107.** Determina que los contribuyentes del impuesto del IVA están obligados a emitir y entregar, por cada operación a otros contribuyentes comprobantes de crédito fiscal o facturas de consumidores finales. **Art. 109.** Reconoce la obligación de emitir y entregar una Nota de Remisión si el Comprobante de Crédito Fiscal no se emite al momento de efectuarse la entrega real o simbólica de los bienes y tal documento amparará la circulación o tránsito de los bienes y mercaderías.
	Obligación de llevar contabilidad formal, registros, inventarios y métodos de valuación	**Art. 139 al 141.** Determina la obligación de llevar contabilidad formal, registros especiales de la documentación para establecer su situación tributaria, llevar libros de compras y ventas, los sujetos pasivos cuyas operaciones consistan en transferencia de bienes muebles corporales estarán obligados a llevar registros de control de inventarios que reflejen clara y verazmente su real movimiento.
	Inventarios	**Art. 142.-** Los sujetos pasivos cuyas operaciones consistan en transferencias de bienes muebles corporales están obligados a llevar registros de control de inventarios que reflejen su valuación, resultado de las operaciones, el valor efectivo y actual de los bienes inventariados.
	Obligación de conservar informaciones o pruebas	**Art. 147.** Cuando la contabilidad sea llevada en forma computarizada, deberán conservarse los medios magnéticos que contengan la información, al igual que los respectivos programas para su manejo. También deberán conservarse por el mismo lapso de tiempo los programas utilizados para facturar mediante sistemas computarizados; así como los documentos que se resguarden por medio de sistemas tales como microfichas o microfilm.
Reglamento de aplicación al Código Tributario	Documentos no válidos para transportar transferencias de bienes	**Art. 36**. Los contribuyentes en IVA únicamente deberán emitir y entregar, los documentos establecidos por el Código Tributario. **Art. 37.-** Los contribuyentes del Impuesto a la Transferencia de Bienes Muebles y a la Prestación de Servicios, deberán portar las Notas de Remisión, Facturas y Comprobantes de Crédito Fiscal.
	Requisitos de documentos a presentar	**Art. 66.** Los estados financieros a presentar serán los que establecen las Normas Internacionales de Contabilidad.
	Contabilidad formal, registros de inventarios	**Art. 73-78.** Dispone lo relacionado a la contabilidad formal que deben llevar los obligados, con el fin que puedan ser comprensibles y que estén actualizados, y determinados de la

		forma en que podrá ser llevada la contabilidad de forma computarizada.
	Sistemas de registros computarizados	Cuando un contribuyente adopte el sistema de registro computarizado de contabilidad, deberá conservar como parte integrante de la misma toda la documentación relativa al diseño del sistema.
	Control de inventarios	**Art. 81.** Regula que los contribuyentes deben llevar registros de control de inventarios.
Código Aduanero Uniforme Centroamericano Arancelario	Declaración de mercancías	**Art. 77.** Con la declaración de mercancías se expresa libre y voluntariamente el régimen al cual se someten las mercancías y se aceptan las obligaciones que este impone.
	Importación definitiva	**Art. 92** La importación definitiva es el ingreso de mercancías procedentes del exterior para su uso o consumo en el territorio aduanero.
Reglamento del Código Aduanero Uniforme Centroamericano Arancelario	Medidas de seguridad	**Art. 167.** Los sistemas informáticos deberán garantizar la privacidad, confidencialidad, no repudiación e integridad de los datos y documentos que son transmitidos y almacenados, así como la autenticidad del ente emisor de los mismos y de los usuarios que utilizan los sistemas de información del Servicio Aduanero.
	Permisos	**Art. 557** La presentación de los permisos correspondientes de importación para los envíos de socorro, podrá efectuarse con posterioridad al ingreso de las mercancías.
	Acceso al sistema informático.	**Art. 171.** Para transmitir al sistema informático del Servicio Aduanero, se requerirá estar previamente autorizado como usuario de dicho sistema, mediante la firma del documento compromisorio que el Servicio Aduanero establezca.
Ley de Medicamentos	Agentes de distribución y venta	**Art. 27.** La distribución y venta de medicamentos, se podrá realizar a través de laboratorios, Droguerías, Farmacias y personas naturales, nacionales o extranjeras debidamente inscritas en el registro especifico, quienes solo podrán comercializar productos debidamente registrados garantizando un servicio de calidad y cumplimiento de buenas prácticas vigentes.
	Autorización de medicamentos	**Art. 29.** Toda persona natural o jurídica podrá fabricar, importar, distribuir, comercializar, almacenar, transportar, dispensar, prescribir, experimentar o promocionar medicamentos, materias primas o insumos médicos, previa autorización de la Dirección Nacional de Medicamentos.

Elaborado en base a normativa legal para el registro y control en la generación de información financiera contable, usando como fuentes bibliográficas, leyes y reglamentos relacionadas a la problemática de estudio y consultadas a través de la página web oficial de instituciones nacionales.

CAPÍTULO III: METODOLOGÍA DE LA INVESTIGACIÓN

3.1. ENFOQUE Y TIPO DE INVESTIGACIÓN.

3.1.1. Tipo de investigación

La presente investigación está basada en el método hipotético deductivo ya que cuenta con pasos esenciales, los cuales son: observar un fenómeno el cual se estudió, la falta de controles apropiados para afrontar los riesgos informáticos, y como respuesta a la problemática identificada, se establece la hipótesis para explicar dicho fenómeno, la cual fue confrontada con la realidad del sector, determinando así la relación entre las variables dependiente e independiente.

De esta manera se ha cumplido con el propósito de identificación de las causas y consecuencias de la problemática para elaborar una evaluación de riesgos informáticos de los aspectos legales y técnicos establecidos que ha de implementar el sector venta de insumos médicos, permitiendo así la formulación de una propuesta concreta y viable.

3.1.2. Enfoque

El enfoque de investigación utilizado fue descriptivo ya que se realizó recolección de datos por medio de cuestionarios estructurados con preguntas cerradas y de opción múltiple posteriormente se analizaron los datos obtenidos de los cuales se obtuvo una perspectiva más amplia del fenómeno en estudio.

3.2. DELIMITACIÓN ESPACIAL Y TEMPORAL

3.2.1. Espacial

La problemática en investigación, se desarrolló para las empresas que comercializan equipo médico en el área metropolitana de San Salvador, debido a los avances tecnológicos existe la necesidad de auxiliarse en las tecnologías de información para la generación de su información

financiera contable. La falta de una evaluación de riesgos informáticos afecta la integridad y confidencialidad de la información.

3.2.2. Temporal

El estudio del problema se realizó con información obtenida a partir de los años 2011 a 2017, dado que según la investigación preliminar realizada en las entidades que comercializan equipos médicos en el área metropolitana de San Salvador, estas han venido implementando en este periodo de tiempo nuevos sistemas informáticos, además de hardware según las necesidades del mercado.

3.3. SUJETOS Y OBJETOS DE ESTUDIO

La investigación se dirigió a las empresas que comercializan equipos e insumo médico, las cuales trabajan para brindar las mejores opciones en el área de salud, integrando el talento así como las tecnologías innovadoras para brindar calidad en sus procesos.

3.3.1. Unidad de análisis

Las unidades de análisis para el estudio fueron los encargados o administradores de tecnología de la información de las empresas que comercializan equipos médicos en el área metropolitana de San Salvador; además se consultó con los profesionales de contaduría pública para fortalecer los resultados del diagnóstico de la problemática objeto de investigación.

3.3.2. Población y marco muestral

La población objeto de estudio fueron las empresas que se dedican a la comercialización de equipo médico, de acuerdo a la información proporcionada por la Dirección General de Estadísticas y Censos en el Directorio Económico 2016 se encuentran registradas 12 entidades;

en este caso se utilizó este año ya que al momento de solicitar los datos a la entidad correspondiente no estaban actualizados.

Por lo tanto, por las características del estudio, el tamaño de la muestra que se utilizará para esta unidad de análisis estará constituida por el total de la población por lo cual, no será necesario utilizar una fórmula estadística ya que el universo se puede administrar en su totalidad.

Sin embargo, para fortalecer el análisis de los resultados de la problemática investigada se aplicó un cuestionario a los contadores públicos tomando de base el listado publicado por el Ministerio de Economía 2017, con la finalidad de investigar la necesidad de desarrollar una evaluación de riesgos informáticos en la generación de información financiera contable y valorar la utilidad para su desarrollo profesional.

Para determinar la muestra de los Contadores Públicos se utilizó la formula estadística para poblaciones finitas, sin embargo para la elección de los profesionales se utilizó un método no probabilístico.

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

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

Dónde:

n = Tamaño de la muestra

z = Nivel de confianza 95%

p = Probabilidad de éxito

q = Probabilidad de fracaso

e = Error permisible

Sustituyendo

n = ?

z = 1.96 Nivel de confianza 95%

p = 98 % Probabilidad de éxito

q = 2 % Probabilidad de fracaso

e = 5 % Error permisible

$$n = \frac{(218)(1.96)^2(0.98)(0.02)}{(0.05)^2(218-1)+(1.96)^2(0.98)(0.02)}$$

$$n = \frac{16.4144}{0.6178}$$

$$n = 26.57$$

$$n \approx 27$$

3.3.3. Variables e indicadores

Las variables utilizadas como parámetro para llevar a cabo dicho estudio y con ello medir su comportamiento son las siguientes:

Variable independiente: Modelo de evaluación de riesgos informáticos en la generación de información financiera contable.

Variable dependiente: Mejora de la integridad y confidencialidad en la captura, procesamiento, almacenamiento y salida de la información.

Indicadores

Variable independiente: El modelo de evaluación de riesgos informáticos en la generación de información financiera contable.

- Directrices de seguridad para los activos de información
- Verificar si la entidad tiene identificados los riesgos asociados al PED
- Políticas en los recursos de información

Variable dependiente: Integridad y confidencialidad la información.

- Conocimiento y competencias
- Integración de la información en los sistemas
- Controles de autenticación para usuarios.

3.4. TÉCNICAS E INSTRUMENTOS

Para la obtención de la información necesaria en relación a la problemática en estudio durante el desarrollo del trabajo se utilizaron técnicas y procedimientos como se detalla a continuación:

3.4.1. Técnicas y procedimientos para la recopilación de la información:

La recolección de la información se realizó en parte por medio de técnicas documentales, bibliográfica como libros de texto, revistas, publicaciones, trabajos de graduación, sitios web, documentos de sitios web, todo ello con relación a los diferentes entes que tratan la evaluación y gestión de riesgos informáticos y otros temas relacionados.

Se utilizó además como técnica de investigación de campo la encuesta a través de un cuestionario en el cual se adquirió información confiable y relevante para el desarrollo de la problemática en estudio.

3.4.2. Instrumentos de medición

El instrumento utilizado fue el cuestionario, en el cual se detallaron una seria de preguntas cerradas que permitieron medir las variables enfocadas a la evaluación de riesgos informáticos con el objetivo de obtener información suficiente y veraz de las empresas seleccionadas.

3.5. PROCESAMIENTO Y ANÁLISIS DE LA INFORMACIÓN.

3.5.1. Procesamiento de la información

La información que se obtuvo al momento de realizar el cuestionario, fue procesada a través de hojas de cálculo de Microsoft Excel, para la representación gráfica, estadística y análisis e interpretación de los resultados obtenidos.

3.5.2. Análisis e interpretación de los datos procesados

Una vez tabulada la información recolectada mediante los cuestionarios, se procedió con el análisis e interpretación de la misma, la cual fue presentada a través de tablas y gráficos destacando la frecuencia en términos absolutos y porcentuales, que mejor representen los datos obtenidos, realizando cruces de variables para una mejor interpretación de los resultados; seleccionando lo más relevante y común entre estos, mostrando las respectivas conclusiones.

3.6. CRONOGRAMA DE ACTIVADADES

ACTIVIDAD/ SEMANA	MESES																																																						
	FEBRERO				MARZO				ABRIL				MAYO				JUNIO				JULIO				AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMBRE				ENERO				FEBRERO				MARZO			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
ELABORACIÓN DE ANTEPROYECTO																																																								
Entrega primer avance anteproyecto			■	■	■	■	■	■																																																
Aprobación del tema									■	■	■																																													
Presentación de anteproyecto												■	■	■	■																																									
Aprobación de anteproyecto																■																																								
CAPITULO I PLANTEAMIENTO DEL PROBLEMA																																																								
Situación Problemática																	■																																							
Enunciado del problema																	■																																							
Justificacion de la investigacion																	■	■																																						
Objetivos de la investigacion																		■																																						
Hipotesis del trabajo																		■	■																																					
Determinación de variable																		■	■	■																																				
Limitaciones de la investigación																				■																																				
CAPITULO II MARCO TEORICO																																																								
Estado actual																				■	■																																			
Marco teorico																				■	■	■																																		
Marco legal																					■	■	■																																	
Marco Tecnico																							■	■																																
Marco Normativo																							■	■																																
CAPITULO III METODOLOGIA DE LA INVESTIGACIÓN																																																								
Enfoque y tipo de investigación																									■	■																														
Delimitación de la investigacion																										■																														
Sujeto y Objeto de estudio																										■	■																													
Tecnicas materiales e instrumentos																										■	■																													
Cronograma de actividades																										■	■																													
Presentación de los resultados																										■	■	■																												
CAPITULO IV PROPUESTA																																																								
Generalidades																												■	■																											
Esquema Operativo de la guia																												■	■	■	■																									
Caso practico																															■	■	■	■	■	■																				
Conclusión y Recomendación																																					■	■	■	■																
Defensa de trabajo de graduacion																																									■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

3.7. PRESENTACIÒN DE RESULTADOS

Según los datos obtenidos, se muestra la percepción de los encargados o administradores de tecnologías de información y contadores públicos con respecto a la evaluación de riesgos informáticos en la generación de la información financiera contable, conforme a los resultados **se** puede determinar el nivel de conocimiento que poseen sobre la problemática desarrollada.

Cada cuestionario se elaboró considerando los indicadores relacionados a la investigación que contiene un objetivo por cada pregunta tomando como base conceptos fundamentales para dar respuesta a la problemática en donde se presentaron los datos obtenidas por los profesionales en tablas, grafico de barras y pastel con los análisis e interpretación de los mismos.

3.8. Diagnóstico de la investigación

Este apartado fue elaborado para presentar de forma secuencial los resultados obtenidos a través de las encuestas suministradas a los sujetos de estudio, para sustentar la problemática identificada en las empresas que comercializan equipos e insumos médicos, las cuales carecen de controles para garantizar que la información financiera contable sea integra y confiable, la cual es útil para la toma de decisiones de la entidad, así como a usuarios externos para informarles sobre la situación económica de las organizaciones pertenecientes a este sector.

Con los resultados de la encuesta se determinó que existen elementos suficientes para respaldar la existencia de la problemática, en donde las empresas de este sector tiene el conocimiento de los riesgos relacionados en el procesamiento electrónico de datos, sin embargo no se realiza una evaluación riesgos informáticos en las cuales les permita identificar las principales amenazas y vulnerabilidades presentes en los componentes de los sistemas de

información como lo son: hardware, software, seguridad física, seguridad lógica y recursos humanos.

3.8.1. Unidad de análisis de los encargados o administradores del departamento de tecnologías de la información

Tabla 3
Indicador sobre el conocimiento y competencia de los encargados de tecnologías de la información

N°	Alternativa	Pregunta	Frecuencia Absoluta	Frecuencia Relativa
1	Grado académico de las unidades de TI	1		
	Técnico		2	17%
	Licenciado/a		4	33%
	Ingeniero/a		6	50%
2	Profesional encuestado que tienen más de 10 años de experiencia	2	6	50%
3	Importancia de capacitar al personal encargado de los sistemas de información	4	5	42%
4	Áreas de capacitación de los profesionales	5		
	Gestión de riesgos informáticos		7	58%
	Auditoría de sistemas		5	42%
	Nunca se capacita		4	33%
3	Conocimiento de los activos de información	6	12	100%

De la población encuestada el 50% de los encargados del área de informática son ingenieros, por lo tanto, conocen y se apoyan en los marcos normativos y técnicos para identificar los parámetros en los sistemas y reducir el riesgo al momento que se genere la información en especial la financiera y contable. El 33% son licenciados y el otro 17% son técnicos cubriendo de manera más general los riesgos. El 50% tienen más de 10 años de experiencia laboral, adquiriendo los conocimientos necesarios para identificar las áreas críticas que pueden afectar el logro de los objetivos de la administración, es importante que la persona encargada del departamento informático se capacite en las diferentes ramas como son: gestión de riesgos en el

cual el 58% de la población optó por esta opción, mientras el 42% en auditoría de sistemas y el 33% no se capacita; lo cual es importante para salvaguardar los recursos informáticos de la entidad.

Es necesario que las empresas contraten personal que conozca sobre los riesgos informáticos en el procesamiento electrónico de datos, las buenas prácticas en la gestión de riesgos, las normativas aplicables y los estándares internacionales, esto con el fin de proteger, mantener y resguardar los activos en los cuales se capturan, procesan y almacenan su información más valiosa para la organización; los encargados del área de informática son los responsables de establecer los lineamientos para una adecuada gestión de los recursos tecnológicos; de manera que el 100% de la población conoce que son los activos de información.

Tabla 4

Indicadores riesgos asociados al procesamiento electrónico de datos y directrices de seguridad para los activos de información.

No.	Alternativa	Pregunta	Frecuencia Absoluta	Frecuencia Relativa
1	Conocimiento sobre los riesgos en el procesamiento electrónico de datos	3	12	100%
2	Importancia de llevar un reporte de los activos de información	7	5	42%
3	Nivel de clasificación según el valor de la información	8	5	42%
4	Frecuencia de evaluación en controles preventivos	9		
	Mensual		6	50%
	Nunca		3	25%
5	Aplicación de una evaluación de riesgos en la generación de información financiera contable	10	7	58%
6	Utilidad de una evaluación de riesgos informáticos	11	12	
	Si es útil una evaluación de riesgos			100%

La mayoría de errores en los sistemas de información ocurren por el mal manejo del usuario. Los resultados de la encuesta indican que el 100% de la población conoce los riesgos en el procesamiento electrónico de datos y considera que esta nueva era de tecnología y sistematización, en donde la información financiera contable se realiza por medios electrónicos, en los cuales se procesan los registros y transacciones diarias que son desarrolladas por los sistemas contables en los que radica la utilización y seguridad que se brinda desde la captura, procesamiento y salida de esta, para contribuir al cumplimiento de los objetivos de la dirección.

Los estándares internacionales de las Normas Internacionales de Estandarización, se manifiesta que los activos de información tienen que estar identificados de una forma clara y documentados en función de su importancia y así minimizar los riesgos garantizando que los inventarios de activos de información tengan una protección eficiente ante cualquier desastre. La información debe poseer una clasificación según el grado de importancia que representa para prevenir que no esté susceptible o vulnerable a posibles pérdidas o robo de la misma, careciendo en muchos casos de ser oportuna y confidencial.

El 50% de las empresas encuestadas afirma que mensualmente realiza una evaluación de los controles preventivos, para tratar de evitar incidentes antes de que estos aparezcan, efectuando un monitoreo de las operaciones, así como del ingreso de datos a los sistemas de información, su procesamiento y salida, no obstante, un 25% nunca efectúa una evaluación de sus controles preventivos por lo que están expuestos a riesgos que aún no han considerado ni valorado y no le dan la importancia debida a su información, como resultado de la falta de capacitación en el área de tecnologías de la información y en la gestión efectiva de riesgos.

De manera que el 58% de las entidades respondieron que no cuenta con una evaluación de riesgos informáticos, en el cual les permita identificar las principales vulnerabilidades y amenazas presentes en la captura, almacenamiento, procesamiento y salida de información comprometiendo la integridad y confidencialidad en la generación de información financiera contable. En consecuencia, por la falta de capacitación en modelos de gestión de riesgos de tecnologías como COBIT 5, ISO, ITIL e ISO 31000:2018 que establece directrices para una adecuada gestión del riesgo en todos los niveles de la organización.

Para los encargados de informática contar con modelo de evaluación de riesgos en los cuales se asegure la integridad y confiabilidad de la información financiera contable contribuirá agregando valor y calidad a sus procesos de entrada, procesamiento y salida de datos en los sistemas, robusteciendo su administración y así se refleje en sus resultados financieros y rendimiento económico.

Tabla 5
Indicador políticas en los recursos de información

No.	Alternativa	Pregunta	Frecuencia Absoluta	Frecuencia Relativa
1	Importancia de aplicar una política de cambio de contraseña	12	5	42%
2	Tiempo cambio de contraseña	13		
	Semestral		1	8%
	Anual		4	33%
	No se realiza el cambio		3	25%
3	Personal autorizado para un cambio de contraseña	14		
	Gerente General		5	38%
	Encargado de TI		8	62%

Los resultados de las encuestas indican que un 33% de la población realiza el cambio de contraseñas en los sistemas anualmente, reduciendo el riesgo cada año, y un 25% no realiza el cambio de contraseña, debido a esto se les solicita a los usuarios una clave que cumpla con los

más altos criterios de seguridad lógica, considerando que en algunas empresas no aplican una política o esta no es recurrente con relación al cambio de claves de acceso lo que representa una amenaza que puede traer como consecuencia la sustracción o revelación de las mismas. El encargado de tecnología de la información es la persona responsable de administrar y de otorgar privilegios en los niveles de la seguridad para acceso en los activos de información, ya que cuentan con la experiencia y capacitaciones en la gestión de riesgo en informática, y solamente el 38% el Gerente General es el encargado que realizar esta operación.

Las empresas no cuentan con manuales o instructivos escritos en el que se detallen los procedimientos a seguir para el ingreso de la información en los sistemas informáticos, generando así una deficiencia en los controles necesarios para llevar un registro detallado los activos de información de la entidad donde se almacena información sensible e identificar al personal responsable del manejo de los sistemas aplicando planes de contingencia ya que son una herramienta que permiten afrontar de manera oportuna y efectiva, la eventualidad de incidentes o accidentes que podrían generar pérdidas económicas.

Tabla 6
Indicador controles de autenticación para usuarios

No.	Alternativa	Pregunta	Frecuencia Absoluta	Frecuencia Relativa
1	El personal cuenta con accesos restringidos	17		
	Si poseen accesos restringidos		11	92%
2	Controles para autenticación de usuarios	18		
	Encriptación		3	25%
	Listas de control de acceso		5	42%
	Contraseñas		6	50%
	Ninguno		2	17%

El 50% de la empresas encuestadas utilizan controles de autenticación como las contraseñas para resguardar que la información sea mal utilizada por personal no autorizado o personas externas a la entidad, la cual pueda perjudicar su reputación, sin embargo también se auxilian de listas de control de acceso en donde solo personas especificas tienen los permisos a los datos de acuerdo a las funciones o áreas a los que pertenecen, ya que la información se ha convertido en un activo valioso, y para asegurar que sea integra, confiable la mayoría cuenta con una clasificación de acuerdo a la importancia que tiene para la entidad para minimizar los riesgos asociados como la manipulación, alteración de la información financiera contable que pueda perjudicar los objetivos estratégicos de la organización, a su vez es necesario que el personal se capacite en estándares y buenas prácticas para la implementación de una cultura de gestión de riesgos

Tabla 7

Indicador riesgos en el procesamiento electrónico de datos

N°	Alternativa	Pregunta	Frecuencia Absoluta	Frecuencia Relativa
1	**Software utilizado en las empresas**	15		
	Software a la medida		6	50%
	Software ERP		6	50%
2	**Integración de módulos**	16		
	Ventas		9	75%
	Inventarios		9	75%
	Activos Fijos		1	8%
	Presupuesto		3	25%
	Bancos		5	42%
	Todos los anteriores		3	25%

El 50% de la población encuestada utiliza un software a la medida debido a que las entidades contratan solo a profesionales que cuenten con la experiencia y estén capacitados en el área de informática; que puedan ser capaces de desarrollar softwares o aplicaciones de acuerdo con las necesidades del sector al que pertenece. El 50% restante posee un software ERP estándar el cual

los procesos deben ser adaptados a los sistemas, ocasionando una desventaja para la organización ya que no se tiene acceso a todos los módulos que conforman el sistema contable por el alto costo de adquisición. EL 75% solo tienen integrados los de ventas e inventario, ya que se puede obtener un control de los productos existentes de la entidad, así al integrarse con el módulo de ventas se manejan las salidas de la bodega y la facturación. EL 42% respondió que es necesario incluir en el sistema de contabilidad el módulo de bancos en el cual se registran los movimientos de las remesas y los cheques con el fin de tener un control sobre los flujos de efectivo.

8.8.2. Unidad de análisis de los profesionales de Contaduría Pública inscritos en el CVPCPA.

Tabla 8

Indicador conocimiento y competencia de los profesionales de contaduría pública

No.	Alternativa	Pregunta	Frecuencia absoluta	Frecuencia Relativa
1	**Formación profesional**	1		
	Informática		8	30%
	Contabilidad		13	48%
	Auditoria Externa		18	67%
	Auditoria Interna		14	52%
	Impuestos		23	85%
2	**Frecuencia de capacitación**	2		
	Anualmente		9	33%
	Pocas veces		12	44%
3	**Evaluación de oferta de capacitaciones**	3		
	Buena		10	37%
	Escasa		6	22%
4	Necesidad de auxiliarse de un experto para una evaluación de riesgos informáticos	8	27	100%

La Norma de Educación Continuada obliga a los profesionales en contaduría pública, a capacitarse principalmente en las áreas de auditoría, contabilidad e impuestos, según los resultados obtenidos por los encuestados, se puede corroborar que las áreas de mayor interés para los profesionales son: los impuestos con un porcentaje del 85%, seguido de auditoría externa con

un 67% y auditoria interna el 52% y solo el 30% se capacita en el área de informática. Por lo cual se considera que los profesionales no le dan la importancia que requiere al área de informática, ya que con la nueva era tecnología para agilizar los procesos de la entidad se están implementando nuevos sistemas de contabilidad automatizados que permitan disminuir los tiempos de registro de información y obtener los reportes en el menor tiempo posible para la toma de decisiones.

De manera que los 27 encuestados, el 44% prácticamente no se capacita en el área de tecnologías de la información, siendo esta una deficiencia ya que es necesario evaluar los sistemas para poder realizar los trabajos de auditoría. Sin embargo, los profesionales califican a las diferentes instituciones que brindan el servicio como "bueno", mientras que el 22% indicó que las ofertas son "escasas" puesto que no consideran impartir aspectos de suma importancia para el auditor. Además, es importante la intervención de un profesional que tenga las competencias suficientes para realizar una evaluación de riesgos para garantizar que la información financiera contable facilite a la toma de decisiones a los usuarios internos y externos.

Tabla 9

Indicadores de riesgos para los contadores públicos que son asociados al procesamiento electrónico de datos

No.	Alternativa	Pregunta	Frecuencia absoluta	Frecuencia Relativa
1	Evaluación de riesgos			
	COBIT 5		9	33%
	ISO 27001/27002		7	26%
	ISO 31000/2018		4	15%
	COSO ERM	4	16	59%
	ITAF		1	4%
	NIA 315, NIA 620		1	4%
	COSO III		1	4%
5	Aplicación de controles en el procesamiento electrónico de datos	9	13	44%

Los marcos de referencia técnicos más utilizados por los encuestados son el Modelo de COSO ERM con el 59%, ya que este marco técnico forma parte de las buenas prácticas de gestión empresarial más conocidas, difundidas y de mayor aceptación general, en segundo lugar, se encuentra COBIT 5 con 33% que integra el gobierno de la entidad con la gestión de tecnologías de la información. Sin embargo la norma ISO 31000:2018 por ser de reciente presentación y ante la falta de capacitación en tecnologías de la información aún no se aplica ampliamente en todas las entidades en la cual permita evaluar los controles en la entrada, procesamiento y salida de datos, y no cuenten con un modelo escrito que asegure la confidencialidad e integridad en la generación de la información financiera contable, un 44% de los profesionales afirma que no aplican los principios del PED probablemente por la falta de capacitación en tecnologías de la información.

Tabla 10
Políticas de los recursos de información y directrices de seguridad para los activos de información

No.	Alternativa	Pregunta	Frecuencia absoluta	Frecuencia Relativa
2	Áreas de vulnerabilidad en los sistemas de información	5		
	Seguridad lógica		13	48%
	Seguridad Física		11	41%
	Software		15	56%
	Hardware		5	19%
	Recursos Humanos		14	52%
3	Importancia de aplicar controles internos	6	27	100%
4	Frecuencia de evaluación de riesgos	7		
	Mensual		4	15%
	Trimestral		5	19%
	Semestral		5	19%
	Anual		4	15%
	Siempre		10	37%
6	Importancia de un modelo de evaluación de riesgos informáticos	10	27	100%

Según los datos de la encuesta el 56% contestó que el área más vulnerable al realizar una evaluación de riesgos informáticos es la de software debido a los continuos avances y cambios en este ámbito que obligan a capacitarse frecuentemente, además el 52% de profesionales considera como segunda área más susceptible la de recursos humanos ya que la mayoría de errores surgen por la falta de desconocimiento o falta de capacitaciones en cuanto al uso de los recursos informáticos. De tal manera que los profesionales de Contaduría Pública consideran que una evaluación de riesgos informáticos será una herramienta útil para las empresas del sector de equipos médicos para identificar las principales vulnerabilidades a las cuales se encuentran expuestas las organizaciones.

Una de las tareas claves de la administración es la gestión del riesgo, normalmente estos controles no se encuentran escritos en la entidad, sino que los usuarios los conocen de manera empírica, los problemas se van solucionando a medida van apareciendo, en resumen, el 100% de los profesionales encuestados están de acuerdo con que deben de existir controles internos. Por lo tanto, para salvaguardar la información financiera contable es de suma importancia realizar una evaluación de los controles de manera constante, como lo indican los resultados de la encuesta el 37% de los encuestados contestaron que las empresas deben estar en constante evaluación que permitirá obtener una seguridad razonable de la información, el 19% consideran que se debe realizar trimestral o semestral con el fin de mitigar y prevenir los riesgos

CAPÍTULO IV: EVALUACIÓN DE RIESGOS INFORMÁTICOS RELACIONADOS CON LA GENERACIÓN DE LA INFORMACIÓN FINANCIERA EN EMPRESAS QUE COMERCIALIZAN EQUIPOS MÈDICOS.

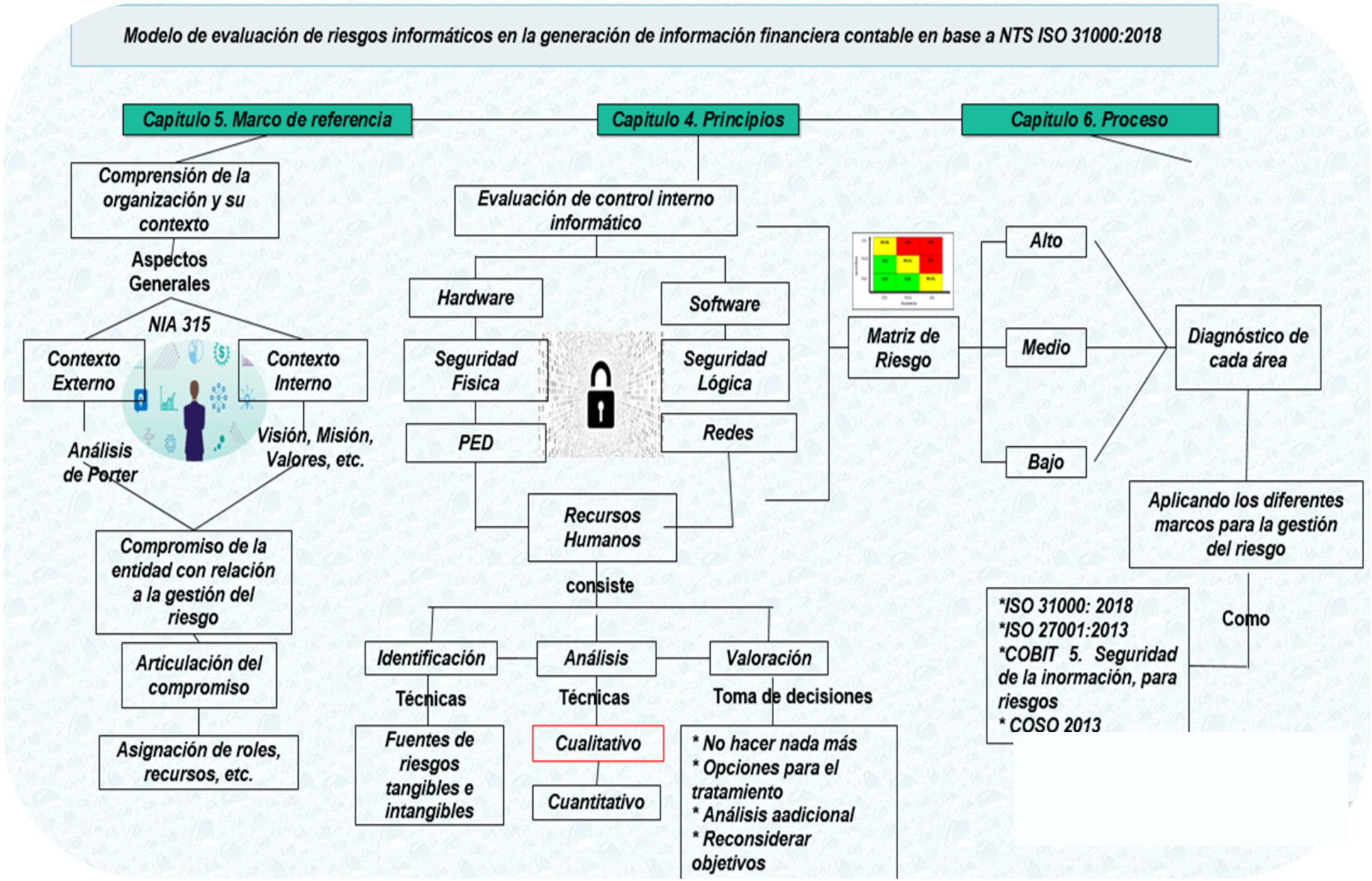
4.1. PLANTEAMIENTO DEL CASO

Se presenta en este capítulo la propuesta de solución del trabajo de investigación que consiste en la elaboración de una evaluación de riesgos informáticos en la generación de información financiera contable aplicando la Norma Técnica Salvadoreña ISO 31000:2018 en la cual se describe los procedimientos para realizar una adecuada gestión de riesgos que permitirá identificar las principales debilidades en el control interno informático.

También se toma en consideración el marco de referencia NIA 315 identificación y valoración de los riesgos de incorreción material mediante el conocimiento de la entidad y su entorno. Para la elaboración del plan de solución se toma en consideración a una organización denominada Medical Company, S.A de C.V, dedicada a la comercialización de insumos y equipos médicos del área metropolitana de San Salvador.

Es importante que las empresas tengan conocimientos sobre las vulnerabilidades en el procesamiento electrónico de datos, aunque la mayoría de errores que se presentan en los sistemas se dan por el usuario, por falta de capacitaciones en cuanto al uso del software o aplicaciones informáticas, es importante aplicar controles generales y específicos para proteger el activo informático más importante de la organización, el cual es la información contable que se genera a través de los sistemas computarizados y es utilizada por los usuarios internos o externo para la toma de decisiones.

4.2.ESTRUCTURA DEL PLAN DE SOLUCIÓN



Las organizaciones tienen presente los riesgo implícitos en las operaciones del negocio que pueda impedir el logro de los objetivos planteados; una evaluación de riesgos en la generación de la información financiera contable contribuye a minimizar las amenazas y vulnerabilidades a las que se enfrentan constantemente, la Norma Técnica Salvadoreña ISO 31000:2018 donde se detallan directrices que les permita anticiparse a las posibles inseguridades que pudieran producirse. La versión actualizada tiene la finalidad de destacar el liderazgo de la alta dirección, así como también mejorar los controles de cada etapa del proceso en la organización.

Al aplicar la norma técnica es importante considerar conocer el contexto externo e interno en el que se desenvuelve la entidad, los objetivos propuestos y los criterios sobre cómo evaluar los principales amenazas y vulnerabilidades tecnológicos en los que se encuentran presentes el ingreso, procesamiento, almacenamiento y salida de la información de las operaciones diarias en la entidad, lo cual contribuye a la toma de decisiones de los usuarios.

4.3. BENEFICIOS Y LIMITANTES

4.3.1. Beneficios del modelo de evaluación de riesgos informáticos.

- Seguridad razonable en la información financiera contable.
- Integración de una cultura de gestión del riesgo.
- Brindar una adecuada respuesta ante incidentes.
- Mayor importancia en los controles generales y específicos.
- Una confiable toma de decisiones para la administración.
- Se tiene como referencia una matriz de riesgos en el cual se puede identificar las amenazas de mayor impacto para la entidad.

4.3.2. Limitantes de la aplicación de una evaluación de riesgos

- Poco tiempo para involucrar a todo el personal, que es parte integral en los procesos de la entidad.
- Deficiente cultura de gestión de riesgos por parte de la administración.
- Falta de una política que gestione la seguridad de la información en el procesamiento electrónico de datos.
- No se ha establecido un comité que gestione la seguridad de la empresa.

4.4. DESARROLLO DEL CASO PRÁCTICO

4.4.1. Introducción

La generación de información financiera contable se realiza en un sistema integrado, el cual tiene riesgos relacionados en la captura, procesamiento, almacenamiento y salida, que se realiza con la ayuda de los diferentes componentes como el software, hardware, recursos humanos, redes, seguridad física y lógica. Con los elementos anteriores se obtiene información que contribuya a la toma de decisiones en las gerencias, por lo que es importante evaluar los controles que puedan ser aplicables para garantizar que los datos ingresados y generados por los sistemas sean confiables, verificables e íntegros.

Sin embargo, es importante considerar que la propuesta se ha elaborado según la Norma Técnica Salvadoreña ISO 31000:2018 siguiendo las directrices para una adecuada gestión de riesgos, en donde el propósito fundamental es la creación y protección de valor.

La evaluación inicia con un entendimiento del ambiente de control interno informático y sus componentes como el hardware, software, seguridad física, lógica, recursos humanos, redes y procesamiento electrónico de datos, aplicando el marco de referencia la Norma Internacional de

Auditoría 315 identificación y valoración de los riesgos, mediante el conocimiento de la entidad y su entorno la cual establece como objetivo para el auditor indagar sobre las principales deficiencias que poseen los sistemas de información de la entidad, dicha evaluación tiene la finalidad de proporcionar una base para que la gerencia de respuesta a los riesgos valorados de incorrección material en los estados financieros, los diferentes tipos de transacciones y saldos contables.

4.4.2. Objetivos de la propuesta

Objetivo General

Desarrollar una evaluación de riesgos que permita a las empresas que comercializan equipos médicos del área metropolitana de San Salvador, evaluar los controles generales y específicos aplicados a los sistemas de información, para disminuir los riesgos asociados al procesamiento electrónico de datos para garantizar la integridad y confiabilidad de la información.

Objetivos específicos

- Conocer el compromiso de la entidad a la política de la gestión del riesgo.
- Realizar una investigación preliminar a través de cuestionarios de control interno informático para identificar las principales amenazas y vulnerabilidades.
- Elaborar una matriz de riesgos para identificar los principales amenazas de la compañía.

4.4.3. Comprensión de la organización y de su contexto (NTS 31000:2018, 5.4.1)

Aspectos Generales de la entidad

Medical Company, S.A de C.V, es una empresa especializada en los sectores médico, industrial e investigativo, que nació en el año 1968 en Panamá. Actualmente, son líderes del

mercado en la mayoría de las actividades que se desarrollan, liderazgo logrado a través del crecimiento de las unidades de negocio y grupos tácticos que desempeñan labores estratégicas y altamente profesionales en las áreas de ventas, soporte y servicio técnico.

- **Constitución de la sucursal en El Salvador**

  La sociedad fue constituida el día 24 de febrero de 2006, según Escritura Pública de Constitución otorgada en la ciudad de San Salvador, y fue inscrita en el Registro de Comercio bajo el No.79, del Libro No. 2844 del Registro de Sociedades, del Folio 413 al Folio 427, con fecha 28 de febrero de 2006.

- **Modificación y reorganización de la sociedad**

Se modificó el pacto social para adaptarlo a las reformas del Código de Comercio, el día 21 de octubre de 2009, según Escritura Pública de Constitución otorgada en la ciudad de San Salvador y fue inscrita en el Registro de Comercio bajo e N° 81, del Libro N°3188 del registro de Sociedades, del Folio 1,089 al 1,096, con fecha 31 de octubre de 2009.

- **Domicilio:** Colonia Escalón, 5° Calle poniente, pasaje "J" y Calle la Loma número 154, San Salvador, El Salvador.
- **Actividad:** Compra y venta de equipos médicos, reactivos, equipo de laboratorio clínico y equipo de diagnóstico por imágenes.

Análisis del contexto externo de la entidad

Para realizar un conocimiento profundo del conocimiento de la entidad Medical Company, S.A de C.V, se utilizará el análisis de las cinco fuerzas de Porter, el cual consiste en un modelo estratégico que establece un marco para analizar el nivel de competencia dentro de una industria, para poder desarrollar una estrategia de negocio.

a) Análisis de las cinco fuerzas de porter aplicada a la entidad Medical Company, S.A de C.V., del sector que comercializan equipos médicos. (Párrafo 5.4.1 lit. a)

Fuerzas competitivas del sector (PORTER)	Poder	Observaciones:
Amenazas de nuevos competidores	**Poder alto**	Las principales barreras de entrada de nuevos competidores son: **Requerimientos de capital:** la necesidad de invertir una importante cantidad de recursos financieros en las instalaciones, equipos de tecnología, insumos médicos para competir crea una barrera de entrada alta. **Política gubernamental:** los gobiernos no limitan la entrada de nuevos competidores a la industria, es un caso de competencia monopolística, en el cual las barreras de entrada al mercado no son muy fuertes. Los productos son muy semejantes. **Experiencia - curvas de aprendizaje**: disminución de costos unitarios de análisis a través de la acumulación de experiencia en el proceso de certificación de los equipos médicos. Lo anterior se convierte en una barrera de entrada siempre y cuando la compañía logre mantenerse como propietaria de tal experiencia. **Diferenciación del servicio de atención al cliente:** ocurre cuando las compañías establecidas poseen una identificación de marca y lealtad de los clientes, adquiridas a través del servicio entregado. Lo anterior, significa que los participantes en esta industria deben invertir fuertemente para adquirir este nivel de diferenciación, lo cual en la mayoría de los casos trae consigo grandes pérdidas iniciales y considerable tiempo de recuperación.

Fuerzas competitivas del sector (PORTER)	Poder	Observaciones:
Rivalidad entre competidores de la industria	**Poder medio**	**Número de competidores. Poder bajo:** el número de competidores que prestan servicios de comercialización de equipos médicos e insumos son muchos. **Capacidad. Poder alto:** en este sentido existe una alta capacidad en el mercado nacional, para abastecer a los clientes, brindado el soporte técnico en los equipos. **Barreras de Salida. Poder bajo:** los equipos utilizados para análisis son específicos en esta industria, sin embargo, actualmente existen empresas que prestan servicios similares con diferentes marcas, por lo tanto, los costos de estos insumos son menores a los de vendidos por la entidad. Si existiese el deseo de no continuar con las operaciones en esta industria los equipos pueden ser vendidos a los competidores.

Fuerzas competitivas del sector (PORTER)	Poder	Observaciones:
Productos sustitutos	**Poder bajo**	La participación en el mercado podría verse amenazada por las siguientes causas: Los equipos médicos e insumos pueden adquirirse un 75% en el mercado internacional, de los cuales los fabricantes otorgan un permiso para poder comercializar sus equipos, y estos se tienen que inscribir, otorgar un permiso de licencia y comercialización en la Dirección Nacional de Medicamentos. Por lo cual existen productos que puedan sustituir lo que comercializan la entidad. Si bien existen alternativas para nuestro servicio, los beneficios de contar con insumos médicos producidos en el mercado nacional con certificación son mejores, considerando los menores riesgos de tipo de cambio y/o pérdida de licencias por incumplimiento de información.

Fuerzas competitivas del sector (PORTER)	Poder	Observaciones:
Poder de negociación de los compradores	**Poder medio**	Los compradores en esta industria poseen poder de negociador escaso en el mercado. Los clientes tienen bajo nivel de influencia en el precio final. Las ventas una parte son por medio de licitaciones con el gobierno. Se podría considerar que un cliente potencial tendrá poder sobre los precios, en la siguiente situación: Poca diferenciación con la competencia en términos de venta de producto o servicio de mantenimiento en los equipos.
Fuerzas competitivas del sector (PORTER)	**Poder**	**Observaciones:**
Poder de negociación de los proveedores	**Poder Bajo**	Poder de los proveedores de equipos e insumos es alto por las siguientes razones: Existen varios proveedores de equipos e insumos en el mercado internacional, pero los proveedores con los que se negocian los productos cumplen con los estándares de calidad requerido por los clientes. No se identifica un interés de proveedores por mejorar los precios en la adquisición de los equipos.

Fuente: (Alejandro Rojas Molina , 2014)

Conclusión del análisis de PORTER: Conforme a los puntos anteriores se puede concluir que el segmento en el que estará la compañía resulta atractivo considerando la actual demanda y el crecimiento constante de las certificaciones autorizadas por las entidades, lo que facilita una buena negociación de los precios con los clientes, riesgo medio de ser sustituido en el largo plazo y bajo poder de negociador con los proveedores.

b) Impulsores claves y tendencias (Párrafo 5.4.1. Lit. b)

- Nuevas tecnologías el reto reside precisamente en adoptar, conseguir e implementar estas nuevas tecnologías con éxito y saber gestionar su adaptación a la organización.
- Seguimiento de procesos como elemento esencial para ir midiendo el impacto de la gestión de riesgos.
- Elaboración de indicadores sencillos para medir los resultados propuestos en los planes de trabajo.
- Recurso humano y tecnología: los directores tienen la responsabilidad de lograr un desarrollo integral de la gente y hacer converger los objetivos de las personas con los de la institución. Por su parte, la tecnología es fundamental para apoyar el trabajo no solo en la simplificación de procesos sino también para almacenar y proporcionar información que apoye la toma de decisiones.
- Medición del desempeño debe tener en cuenta la retroalimentación y asociarse al logro de los objetivos de la entidad, más los compromisos personales.

c) Análisis político, económico, social, tecnológico, ecológico, legal (Párrafo 5.4.1. Lit. c)

Político y legales: la regulación en el país para asegurar la oferta en el mercado de productos efectivos, de mayor calidad, certificados por las entidades, les otorgan a las empresas que comercializan equipo médico oportunidades de desarrollo y crecimiento. Independientemente de la tendencia política del gobierno, se aprecia un mercado altamente regulado, ofreciendo una canasta amplia de productos certificados que permitan mejorar la calidad de vida de las personas y asegurar la accesibilidad de los insumos.

Económicos: el mercado de venta de equipos médicos e insumos es altamente atractivo, sin embargo, para llegar hacer más competitivos a mediano plazo la entidad tendrá que buscar nuevos proveedores que ayuden a disminuir los costos de importación.

Sociales: existe un aumento en el poder adquisitivo de las instituciones gubernamentales y privadas de los equipos médicos e insumos con el fin de prevenir las enfermedades para mejorar la salud y calidad de vida de los usuarios.

Tecnológicos: la industria al estar en constante crecimiento y encontrarse en un mercado cada vez más globalizado, con amplio acceso a la tecnología de punta, requiere ser cada vez más competitiva y eficiente, por tanto, los participantes en el mercado estarán continuamente innovando para mejorar sus procesos, generando alianza con proveedores e inversionistas estratégicos, que facilitan el acceso a la tecnología vanguardista.

Conclusiones del análisis de PESTEL

La mayor conciencia creciente en el cuidado de la salud, aumento de la cobertura, mayor calidad exigida a los equipos e insumos médicos, precios más competitivos, una mayor regulación y exigencia en la calidad de los procesos, en los últimos años se abren oportunidades de desarrollo y crecimiento.

d) Compromisos contractuales (Párrafo 5.4.1. Lit. d)

La organización tiene compromisos contractuales con las entidades de gobiernos por la instalación y mantenimiento de los siguientes equipos

- Fuente de Iridio.
- Equipo de Braquiterapia

- Tomógrafo de ultrasonografía

e) Complejidad de las redes y dependencias (Párrafo 5.4.1. Lit. e)

Los procesos de globalización se presentan como redes de integración crecientes y complejas en los medios ambientes a los que se enfrentan la organización lo que causa que existan estructuras de redes para compartir la información, datos y conocimiento de los activos en done el funcionamiento de cualquiera se entiende que es en función de las demás.

La entidad trabaja bajo la complejidad de las redes para incrementar su mercado tanto a nivel Nacional y Centroamericano.

Análisis interno de la entidad

a) Visión (Párrafo 5.4.1 f)

Ser una empresa con un modelo único e inspirador, reconocido por los clientes, proveedores y la comunidad, integrando el talento y las tecnologías innovadoras para impulsar la salud y la calidad.

b) Misión (Párrafo 5.4.1 f)

Contribuir con soluciones tecnológicas innovadoras que impacten y agreguen valor a nuestros clientes.

c) Valores (Párrafo 5.4.1 f)

- Confianza.
- Orientación al cliente.
- Desarrollo profesional.
- Calidad y mejora continua.

d) Estructura de la organización (5.4.1.g)

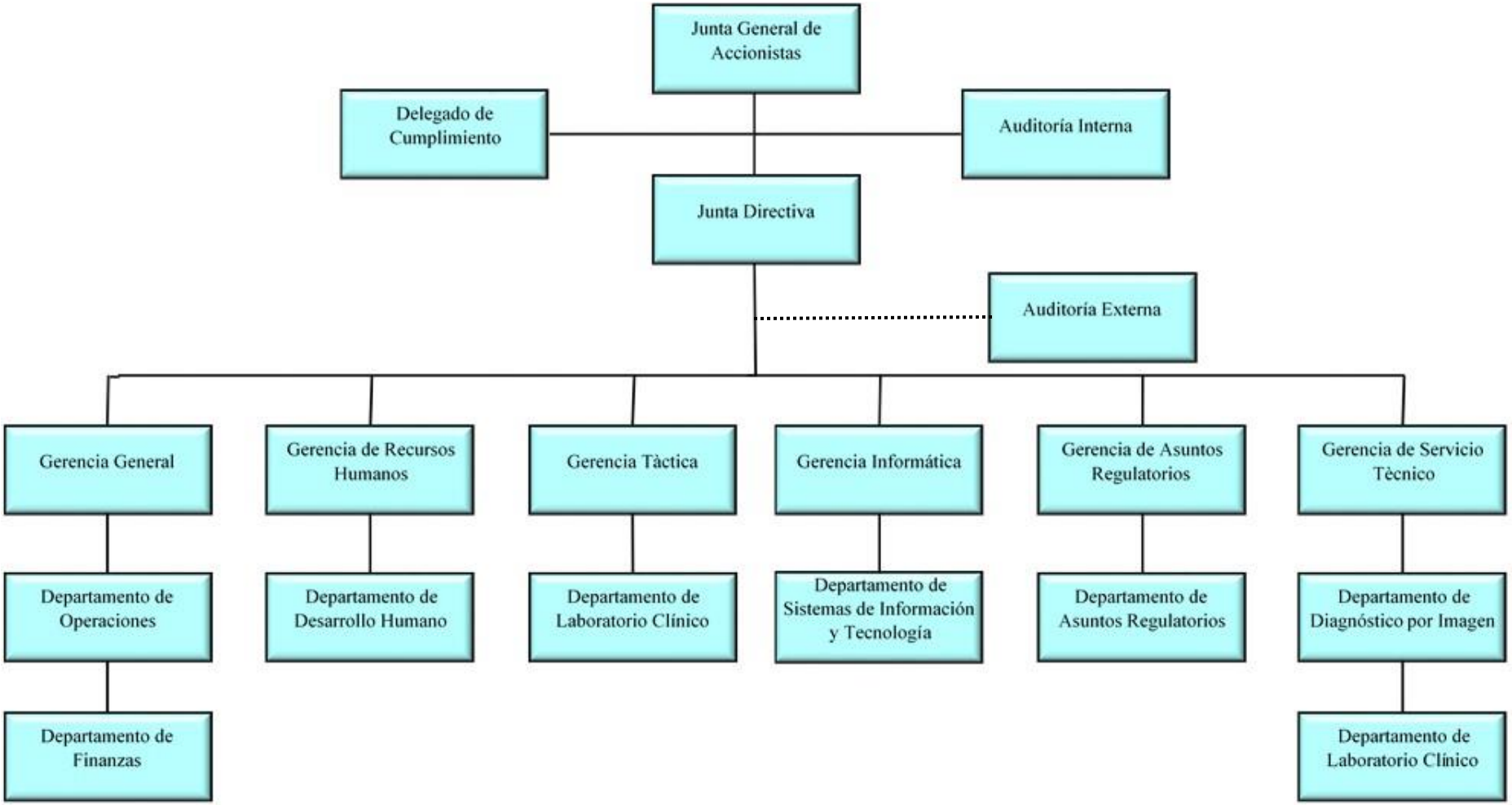
Tabla 11
Estructura organizativa de Medical Company, S.A de C.V

Del negocio	Departamento de gestión financiera	Control interno	Ciclos financieros contables
Líneas de negocios.	Estructura del departamento de finanzas.	Sistema de control interno.	Ciclo de ingresos.
Estructura corporativa del negocio.	Tesorería.	Sistema del control interno del entorno.	Ciclo de egresos.
Organización funcional corporativa.	Planificación financiera.	Controles de procedimientos.	Ciclo de activos fijos.
	Inventario.	Sistema contable.	Ciclo de administración financiera.
	Contabilidad y tributación.	Sistema del ciclo contable.	Ciclo de nóminas.
			Ciclo de acumulados y preparados.

e) Política de calidad A-003 (Párrafo 5.4.1 h)

Medical Company, S.A. de C.V., tiene como objetivo satisfacer a los clientes y partes interesadas, ofreciendo productos, servicios y tecnologías desarrolladas mediante un trabajo en equipo planificado, innovador y productivo en el cual participan todos los grupos de negocios y de apoyo de la organización, aplicando procedimientos para la mejora continua y creación de valor en sus procesos. También se han adaptado políticas de gestionar los riesgos especialmente en el ambiente de tecnologías de la información para agregar valor a su información.

f) Estructura organizacional (5.4.1.g)



g) Principales políticas y procedimientos.

Tabla 12
Resumen de políticas y procedimientos de Medical Company, S.A de C.V

	Propósito
Estructura corporativa de negocios	Medical Company, ha diseñado una estrategia de negocios mediante la cual las distintas especialidades de productos y servicios son distribuidas en forma separada en 11 unidades de negocios que mantienen autonomía para negociación y cierre de ventas. Para darle soporte a estas unidades de negocios se han creado los grupos de apoyo como lo son los de distribución, logística y finanzas entre otros.
Organización funcional corporativa	La Junta Directiva de Medical Company es el órgano rector, que es responsable de la orientación y supervisión.
Estructura departamento de gestiones financieras	Garantizar que los recursos y la información financiera están siendo debidamente resguardados, procesados, registrados, resumidos y reportados en un tiempo oportuno y de manera exacta, y de esa manera asegurar la protección de los recursos, y la medición de los resultados en forma sostenible que contribuya a evaluar los resultados cuantitativos y cualitativos sobre los objetivos y metas propuestas de la Corporación.
Estructura del departamento de tesorería	Asegurar que la administración financiera de todos los recursos de liquidez garantice que estén debidamente resguardados, procesados, registrados, resumidos y reportados en un tiempo oportuno y de manera exacta. Además de planificar e implementar las estrategias y acciones necesarias para garantizar el flujo oportuno, exacto y sostenible de los fondos requeridos para la operación e inversiones de la empresa.
Estructura del departamento de inventarios	Garantizar la confiabilidad y sostenibilidad a la estructura de costos de los productos, el sistema de valoración y de los saldos del inventario.
Estructura del departamento de contabilidad y tributación	Asegurar que la administración financiera cuente con todos los registros de la contabilidad debidamente documentados y resguardados, procesados con la suficiente información descriptiva de la transacción, resumidos y reportados en un tiempo oportuno y de manera exacta Además de asegurarse que las transacciones hayan sido autorizadas según los procedimientos descritos en las normas de controles internos y de procedimientos adoptadas por la organización. Elabora distintos informes financieros gerenciales para la toma de decisiones. Los registros financieros, así como sus responsabilidades tributarias son supervisados y revisados por esta gerencia para lo cual se mantiene comunicación y reportes continuos.
El control del entorno	Ubicar el control interno como parte de sus actividades diarias corporativas. Los factores que influye el control del entorno incluyen la gestión y la filosofía, estructura organizacional, la manera de asignar autoridad y responsabilidad, métodos de administración y control, políticas y prácticas del personal y una influencia externa de la Junta Directiva.
El sistema contable	La Contabilidad de COINSA es el módulo central de todas las aplicaciones que conforman el núcleo, ya que reúne toda la información de carácter financiero y contable que genera la empresa al desarrollar sus transacciones diarias
Sistema y ciclo contable	El sistema y ciclo contable es para asegurar que los procesos de transacciones financieras aseguren la homogeneidad y consistencia de los registros financieros según su esencia económica. Que dichos registros y reportes estén el momento oportuno y que sean consistentes con los estándares de contabilidad y del sistema financiero contable

	Propósito
Diagnóstico por imagen	**Ultrasonografía** lacionadas que se originan de es asegurar que los procesos de transacciones financieras, resumen de los registros y reportes estén al momento oportuno y que sean consistentes con los estándares de contabilidad.
Ciclo de egresos o desembolsos	Comprende la generación de egresos o desembolsos en procesos y actividades para las operaciones principales que se involucran y se asocian con la adquisición y/o pago.
Ciclo de activos productivos	Incluye las transacciones vinculadas con los bienes de carácter material (tangibles) o inmaterial (intangibles) adquiridos con el propósito de utilizarlos en la actividad que desarrolla la entidad.
Ciclo de administración financiera	El ciclo contable comprende la generación de todas las entradas de efectivos de la gestión y todos sus procesos y cuentas relacionadas que se originan de la naturaleza de las transacciones que generan efectivo y equivalentes de efectivo en el curso de ingresos operativos normales.
Ciclo de reportes financieros	Comprende la generación de todas informaciones, transacciones y registros que se procesaron dentro del ciclo de vida mensual de la empresa. Estos son; estados financieros consolidados, evaluación financiera de cambios y los comparativos con presupuesto. El objetivo es asegurar que los procesos de transacciones financieras, resumen de los registros, y reportes estén al momento oportuno.

h) Principales clientes y proveedores

Clientes

- Instituto Salvadoreño del Seguro Social
- Hospitales Nacionales
- Hospitales Privados
- Clínicas

Proveedores

- Boston Scientific
- Grifols
- Brainlab
- Ge Medical System

i) Principales productos

Diagnostico por Imagen

ACELERADOR LINEAL VARIAN MEDICAL

NUCLEAR MAGNETIC RESONANCE IMAGING SISTEM

Ultrasonografia

SISTEMAS DE DIAGNOSTICO DE ULTRASONIDO

ULTRASOUND SYSTEM IMAGING CARDIOVASCULAR VIVID

Sistemas Médicos

POLARIS X STEERABLE DECAPOLAR MAPPING CATHETERS

SISTEMA DE ESPIRAL

Banco de Sangre

BARKEY WARMING CENTER II

TRANSFER GRIFOLS PEDIATRIC

Laboratorio Clinico

ALERE TRIAGE METERPRO

CL ANALYZER

Equipo Médico

CASE/CARDIOSOFT

INCUBATOR NEONATAL

j) Cultura de la organización (Párrafo 5.4.1. Lit. i)

Los siguientes elementos constituyen la guía de actuación que debe motivar a los usuarios la búsqueda de la máxima calidad y desempeño en el trabajo diario. •

- **El cliente es primero:** las interacciones deben enfocarse en informar a los profesionales del cuidado de la salud sobre productos, proporcionando información científica, clínica y educacional, así como el recibir información acerca de sus necesidades para el desarrollo de su trabajo.
- **Creencia en la innovación:** el suministro de equipos y/o productos por parte de la empresa a los clientes, para propósitos de una evaluación sobre las nuevas innovaciones les permite tomar una decisión informada de la compra.
- **Creencia en la comunicación honesta:** en cuanto a las transacciones y compromisos entre las partes.
- **Excelencia a través del mejoramiento continuo:** promover directrices que busque nuevos y mejores productos que aumenten el nivel de calidad de los insumos y servicios ofertados.
- **Sentido de pertenencia a la organización:** establecer políticas que beneficien a los colaboradores, y teniendo en cuenta sus opiniones para resolver diferentes conflictos**.**
- **Respeto:** Debe existir integridad con las partes involucradas en una relación de negocios.

k) Normas, directrices y los modelos adaptados por la organización (Párrafo 5.4.1. Lit. j)

- Código de Comercio
- Código Tributario
- Reglamento de aplicación al Código Tributario

- Ley de Impuesto a la Transferencia de Bienes Muebles y Prestación de Servicios
- Código Aduanero Uniforme Centroamericano Arancelario
- Reglamento del Código Aduanero Uniforme Centroamericano Arancelario
- Ley de Medicamentos

l) Las capacidades, entendidas en términos de recursos y conocimiento (Párrafo 5.4.1. Lit. k)

Cargo	Nombre
Presidente	Gonzalo Sánchez
Vicepresidente de sistemas de información	Jorge Sánchez
Vicepresidente de laboratorio clínico	Luciana Sánchez
Director de tecnología y sistemas	Janette Batres
Director de finanzas	Juan González
Directora de comunicaciones	Marta López
Director de asuntos regulatorios	Pablo Salazar
Asistente ejecutivo	Gladys Martínez
Asesor legal	Lourdes Carrillo
Director de desarrollo humano	Stephanie Torres

- **Capital social**

El Capital Social está representado por 1,000 acciones comunes con un valor nominal de $ 12.00 cada una suscritas y pagadas en su totalidad.

Suscrito y Pagado – Mínimo	12,000.00
Suscrito y Pagado – Variable	27,960.00
	39,960.00

m) Los datos, los sistemas de información y los flujos de información (ISO 31000:2018 Párrafo 5.4.1 Lit. l)

COINSA es la solución financiera-administrativa compuesta de varias aplicaciones totalmente integradas, desarrolladas sobre plataforma Oracle, las cuales pueden ser adquiridas e instaladas de manera modular, dependiendo de las necesidades de información de cada empresa.

Los módulos que la componen son: contabilidad general, cuentas por cobrar, facturación, inventarios, compras e importaciones, consolidación de estados financieros, cuentas por pagar, activos fijos, bancos.

n) Principales Módulos

Contabilidad: es el módulo central de todas las aplicaciones, ya que reúne toda la información de carácter financiero y contable que genera la empresa al desarrollar sus transacciones diarias, por su naturaleza pueden existir riesgos como el sistema no puede cumplir con las necesidades de la empresa, el ingreso de los registros contables no estén bajo la regulación aplicable, errores en los cambios de moneda extranjera, los asientos contables con errores y reportes no cumplan con los requerido por la entidad.

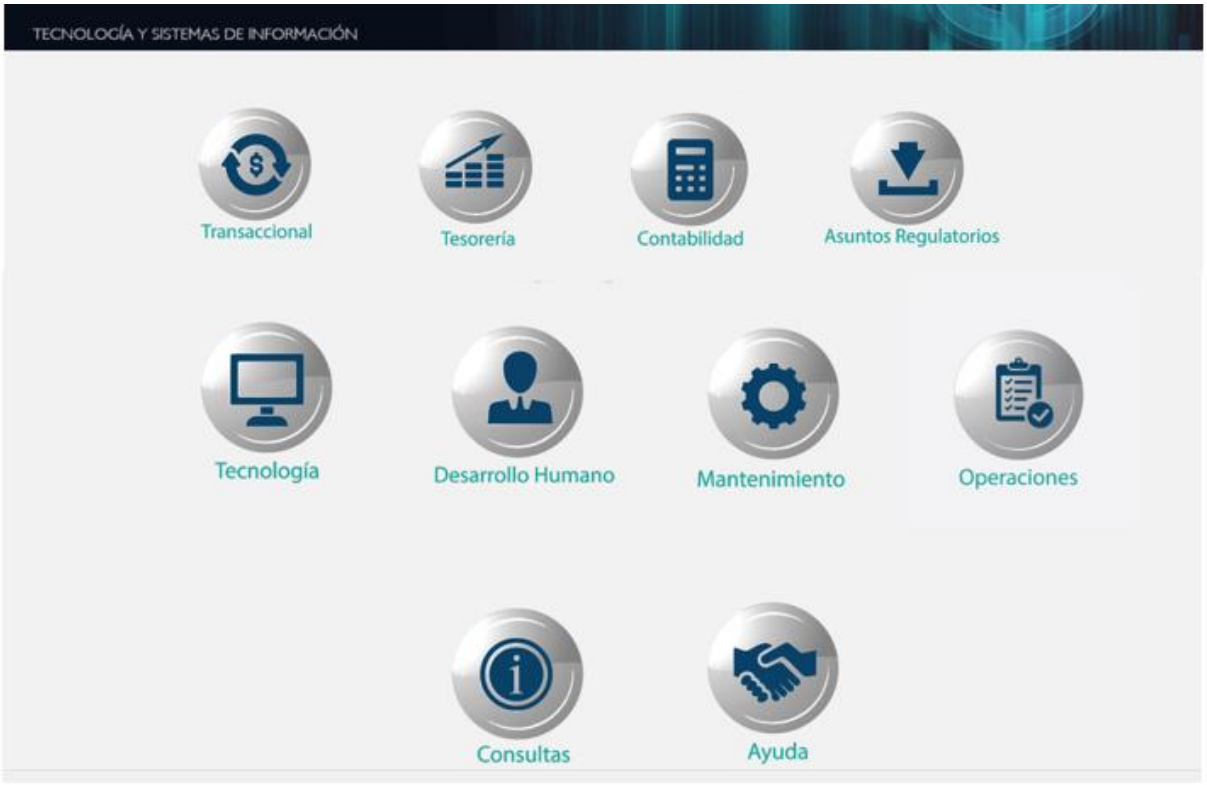


Figura 4*: Módulos del Software Contable COINSA*

Tesorería: administra en una forma eficiente los compromisos adquiridos por sus clientes a partir de la facturación de los productos o servicios que la compañía distribuya o comercialice, permite una mejora sustancial en los procesos de cobro, existiendo en este módulo riesgos inherentes en la interfaz con el de facturación para corroborar que los datos en las cuentas por cobrar son reales, la falta de compromiso de los usuarios al momento de ingresar al sistema los parámetros del cliente y los estados de cuenta que se envían.

Operaciones: es la herramienta ideal para llevar un control detallado de las mercancías, u otros productos adquiridos por la empresa con el objeto de ser comercializados, por su naturaleza existe el riesgo de no ingresar los productos, las salidas se realicen con formularios manuales, errores en el ingreso de las cantidades que aumenten el costo.

Transacciones: en este módulo se registra y se lleva un control de las cuentas por pagar adeudadas por la empresa a los proveedores que suplen sus necesidades de compra de insumos, servicios y demás adquisiciones en que incurra la empresa para su desempeño diario. La deficiencia es que no efectúa las retenciones reguladas por las normativas fiscales.

Asuntos regulatorios: se ingresa los productos que están inscritos en la Dirección Nacional de Medicamentos (DNM), y su estatus si están en procesos, genera reportes detallado de las características de los equipos, el usuario responsable de este módulo está en la obligación de ingresar los datos para que la información que se obtiene en los reportes sea actualizada.

Desarrollo humano: es la solución adecuada para ejercer un control detallado y flexible de los pagos realizados al personal. Esta función se realiza mediante la parametrización de todos los componentes del salario, tales como: ingresos, deducciones, adelantos, provisiones, entre otros. Sin embargo, existe riesgo en la fiabilidad de la información porque es ingresada por cada empleado y al final no se corroboran los datos.

o) Flujo de la información

Figura 5: Ciclo de información de Medical Company, S.A de C.V.

p) Manejo de objetivos en conflicto (Párrafo 5.4.2 Lit. f)

OBJETIVOS	METODOLOGÍA QUE SEGUIR	RECURSOS NECESARIOS	RESPONSABLE
Capacitación virtual con evaluaciones en línea por puesto de trabajo.	Implementar la capacitación virtual de la información que el director de desarrollo humano considere necesaria para que el personal se apoye considerando los requisitos aplicables a las normas y reglamentos de la organización.	Económicos, personal, tiempo y una plataforma para elaborar las presentaciones de capacitaciones y sus pruebas.	Director de desarrollo humano.
Automatización del manejo de bodega.	─ Desarrollo de los requerimientos del software. ─Reuniones semanales y quincenales de avances en el módulo. ─ Pruebas con los usuarios para validar los cambios, ─ Correcciones de errores que salen de los entrenamientos.	Económicos, Programadores, Personal que levante y actualice la información de productos, Tiempo para recibir los entrenamientos y personal que mantenga seguimiento a los avances.	Grupo de Bodega y Distribución de Panamá y Grupo de Tecnología y Sistemas de Información.

Mejorar los procedimientos para la confidencialidad e integridad de la generación de la información financiera contable	Consultar los marcos normativos relacionados a la protección de la información, realizar una evaluación interna para cerrar brechas y lograr que la información sea íntegra y confiable.	Inversión económica, Auditores internos, Personal Entrenado, responsables comprometidos.	Gerente de informática y los auditores internos
Garantizar que los recursos y la información financiera estén siendo debidamente resguardados	- Trabajar en conjunto con el Comité de ejecutivos de la Junta Directiva - Reuniones una vez al mes para discutir los avances.	Personal capacitado. Inversión económica	Director de finanzas
Asegurarse de la integridad de los saldos con los proveedores en los sistemas	- Analizar y verificar las cuentas por pagar con los estados de cuenta enviados por los proveedores - Registrar las facturas de compra locales	Integración de las cuentas por pagar al sistema contable. Inversión económica	Gerentes de informática Gerentes del departamento de finanzas
Asegurar el adecuado mantenimiento de la infraestructura, garantizando un ambiente de trabajo seguro	-Implementar controles preventivos. - Mantener los activos en ambientes seguros	Personal capacitado Contratos de mantenimiento con otra empresa	Gerente de informática

4.4.4. Diagnóstico de aplicación de la 31000:2018

a) Compromiso de la entidad con relación a la gestión del riesgo Párrafo 5.4.2

Tabla 13

Articulación del compromiso de la gestión del riesgo

No	Preguntas	Siempre	Casi siempre	Nunca	ISO 31000:2018
1	¿Se realizan actividades de integración enfocadas en las principales operaciones sobre el registro de la información financiera contable que contribuya a una oportuna toma de decisiones?		X		5.4.2. (c
2	¿Existe la responsabilidad y la obligación de rendir cuentas sobre la información que se genera en los sistemas a las autoridades correspondientes?	X			5.4.2. (d
3	¿Cuenta la organización con la política de evaluar los riesgos en la generación de la información y la relación de los vínculos con sus objetivos?		X		5.4.2. (a

4	¿Se integra a la cultura de la organización procedimientos para gestionar los riesgos en la información?			X	5.4.2. (b
5	¿La organización mantiene disponible los recursos necesarios para el buen funcionamiento de los activos en los que se genera la información financiera?		X		5.4.2. (c
6	¿La organización mide e informa sobre los indicadores de desempeño para evaluar la gestión de riesgos en los procedimientos de los registros contables, que contribuya a las bases para tomar acciones?			X	5.4.2. (g
7	¿Se realizan actividades de mejora continua para disminuir los riesgos en la generación de la información que puedan afectar los objetivos de la entidad?		X		5.4.2. (h

b) Roles y recursos en el marco de trabajo de la gestión del riesgo

Tabla 14

Asignación de roles y recursos en el diseño del marco de trabajo de la gestión del riesgo.

Objetivo: Verificar si la entidad toma en consideración en la gestión todos los recursos disponibles para mitigar los riesgos relacionados con la generación de información financiera contable, que permita asegurar la integridad de los reportes utilizados en la toma de decisiones.

No	**5.4.3 Asignación de roles, autoridades, responsabilidades, y obligación de rendir cuentas en la organización**	**Siempre**	**Casi siempre**	**Nunca**	**ISO 31000:2018**
1	¿La administración enfatiza que la gestión de riesgos en la generación de información financiera contable representa una responsabilidad principal para la organización?		X		5.4.3. a)
2	¿La entidad tiene asignada a una persona específica para rendir cuentas sobre la información financiera contable generada por los sistemas informáticos?		X		5.4.3. b)
3	¿El gerente general informa a los accionistas mensualmente sobre el cumplimiento de los objetivos de la organización?		X		5.4.3. b)

4	¿El contador es el responsable de presentar a la gerencia los estados financieros y otros reportes que solicite la administración después del cierre?		X		5.4.3. b)
5	¿Se verifica la fidelidad de las cifras en los estados financieros por la persona responsable cada vez que el contador presenta los reportes a la gerencia general?		X		5.4.3. b)
6	¿El delegado de cumplimiento verifica la fidelidad de los estados financieros y otros reportes que presenta el contador de la entidad?		X		5.4.3. b)
7	¿El auditor externo emite a la alta dirección informes financieros y los que la regulación exige sobre hallazgos encontrados en la evaluación de riesgos en la entidad sobre los controles internos informáticos?		X		5.4.3. b)
8	¿El encargado de recursos humanos documenta el desempeño laboral del personal mediante una carpeta o archivo individual de cada empleado?		X		5.4.3. b)
9	¿El gerente de finanzas presenta informes financieros mensuales a la administración de la entidad?		X		5.4.3. b)
10	¿El gerente de operaciones informa periódicamente sobre anomalías en el inventario de productos, mediante un reporte mercadería por vencer, en obsolescencia o dañada?		X		5.4.3. b)
	5.4.4. Asignación de recursos				
11	¿Se cuenta con personal encargado del departamento de informática que da soporte a los sistemas contables?	X			5.4.4.a)
12	¿Al implementar la gestión de riesgos se tienen en consideración la falta de conocimiento de los usuarios para realizar los procedimientos en el ingreso de los datos en los sistemas de información?		X	X	5.4.4.a)
13	¿Se asignan personal con experiencia y las competencias necesarias para implementar la gestión de riesgos eficaz en la información financiera?			X	5.4.4.a)
14	¿Al gestionar los registros de las operaciones contables se toman en cuenta los procesos, métodos y las herramientas a utilizar?		X		5.4.4.b)
15	¿La organización documenta los procesos y procedimientos para asegurar una adecuada gestión en la información financiera de la entidad?	X			5.4.4.c)
16	¿Se realizan mejoras aplicando controles en la seguridad de la información financiera contable?			X	5.4.4.d)
17	¿La administración toma en consideración el desarrollo profesional y la formación académica de los encargados del departamento de informática y contabilidad?		X		5.4.4.e)

c) Establecimiento de la comunicación y consulta

Tabla 15

Cuestionario de comunicación y consulta.

Objetivo: Identificar si la entidad desarrolla planes de comunicación y consulta para tratar los riesgos relativos a la generación de la información, sus causas y las posibles consecuencias.

No	Comunicación y consulta	Siempre	Casi siempre	Nunca	ISO 31000:2018
1	¿Las partes interesadas comprenden la definición de riesgo en la generación de la información, las bases con las que se toman decisiones y las razones por las que son necesarias acciones específicas?	X			5.4.5
2	¿Se busca promover la toma de decisiones y comprensión de los riesgos generados de la información?		X		5.4.5
3	¿Se realizan consultas para obtener una retroalimentación de la información para apoyar a las partes interesadas en la toma de decisiones?		X		5.4.5
4	¿Se toman en cuenta las diferentes áreas de experiencia para realizar el proceso de gestión de seguridad de la información?	X			5.4.5
5	¿La entidad considera los diferentes puntos de vista de los usuarios involucrados en el ingreso de datos para definir los criterios de riesgos y su valoración?		X		5.4.5.
6	Existe un sentido de inclusión y propiedad entre las personas afectadas por el riesgo informático		X		5.4.5
7	¿Se poseen planes de comunicación y consulta para tratar temas relativos a los riesgos de la información?			X	5.4.5
8	¿La empresa cuenta con principios de comunicación que especifique las formas de informar a las partes interesadas para la mejora de la información?		X		5.4.5
9	¿Existe una estrategia de comunicación teniendo en cuenta las partes interesadas relacionadas a la gestión de los riesgos informativos?		X		5.4.5
10	¿Existe una política de comunicación, para que todas las partes interesadas tengan la posibilidad de consultar los riesgos del en el ingreso de datos en los sistemas de información?		X		5.4.5

d) Implementación del marco de referencia de la gestión del riesgo (Párrafo 5.5)

Tabla 16

Cuestionario sobre la implementación de la gestión del riesgo

Objetivo: Conocer si la organización implementa los marcos de referencia en la gestión de riesgos informático, que contribuya a la mejora de sus procesos en la generación de la información.

No	Implementación	Siempre	Casi Siempre	Nunca	ISO 31000:2018
1	¿La entidad realiza un plan apropiado para la gestión del riesgo en la generación de información financiera contable?			X	5.5 a)
2	¿Se tienen en cuenta los principios del marco de referencia al momento de establecer los objetivos?			X	5.5.a)
3	¿Se establecen los plazos para implementar el plan de gestión en la información sensible de la empresa?			X	5.5.b)
4	¿Se implementan eficazmente los principios en los procesos internos sobre la generación de la información?		X		5.5.a)
5	¿El plan de gestión del riesgo detalla donde, cuando, como y quien toma los diferentes tipos de decisiones para resguardar la información en los sistemas informáticos?			X	5.5.b)
6	¿El sistema de información financiera se adapta a los cambios en los procesos definidos por la organización con relación a la generación de la información financiera contable?			X	5.5.c)
7	¿La organización asegura que las disposiciones para la gestión del riesgo en la generación de información financiera contable son claramente comprendidas y se practican?		X		5.5.d)
8	¿Los objetivos de la entidad están integrados a las otras actividades del proceso administrativo para crear y proteger los activos?			X	5.5.d)
9	¿La empresa tiene designado a una persona responsable de elaborar un plan que dé respuesta a las vulnerabilidades y amenazas en relación con la generación de la información?			X	5.5.c)
10	¿La alta dirección y los ejecutivos comprenden la importancia de monitorear el plan de gestión de riesgos?		X		5.5.d)
11	¿Con qué frecuencia se les da seguimiento a los controles internos informáticos?			X	5.5.d)

e) Valoración de la gestión del riesgo

Tabla 17

Valoración del marco de referencia de la gestión de riesgos

Objetivo: Valorar la eficacia en la gestión del riesgo informático relacionado a la generación de in formación financiera contable, mediante los procedimientos establecidos por el marco de referencia.

No	Valoración	Siempre	Casi Siempre	Nunca	ISO 31000:2018
1	¿La organización mide periódicamente el desempeño del manejo de su información?		X		5.6 a)
2	¿Se valora la eficacia del marco de referencia en la gestión de riesgos de la información financiera?			X	5.6. a)
3	¿La organización mide periódicamente el desempeño de la gestión del riesgo en la generación de información financiera contable en relación con sus indicadores?			X	5.6. b)
4	¿La organización determina si es idóneo apoyar el logro de los objetivos estratégicos al aplicar medidas de seguridad en la información confidencial?			X	5.6. b)
5	¿Existen procedimientos en el sistema contable para generar la orden de compra de los inventarios?			X	5.6. a)
6	¿La empresa controla la facturación que son realizadas en forma manual?		X		5.6. a)
7	¿La organización lleva un control de los gastos mediante un presupuesto?		X		5.6. a)
8	¿El inventario es ingresado al sistema al momento de recibirlo por el área de bodega?			X	5.6. a)
9	¿La documentación que soporta los gastos de importación se entregan al departamento de contabilidad?		X		5.6. a)
10	¿Los vendedores siguen los procedimientos establecidos para la entrega de los productos a los clientes?		X		5.6. a)
11	¿La organización cuenta con una política sobre el cierre de los módulos cuando termina el mes?	X			5.6. a)
12	¿Se informa a la gerencia sobre los productos próximos a su vencimiento?			X	5.6. a)
13	¿Se revisa el ingreso de las pólizas en el módulo de importación para tener los costos reales en los reportes de inventarios?		X		5.6. a)
14	¿La organización tiene programada las fechas límites para los cierres contables?	X			5.6. a)
15	¿El proceso de gestión de riesgo es parte integral de las actividades de la organización?		X		5.6. a)

16	¿La empresa tiene definido al personal responsable que está involucrado en la toma de decisiones?	X			5.6. a)
17	¿Se conocen cuáles son las incertidumbres asociadas al contexto interno y externo que puedan afectar en la toma de decisiones?		X		5.6. b)
18	¿Se realizan reuniones con el personal responsable de ejecutar los procedimientos en la implementación de los controles?			X	5.6. a)
19	¿Cuándo se establecen metas al personal informático, se consideran los objetivos del departamento?	X			5.6. b)
20	¿Se realiza al personal de cada área evaluaciones cruzadas entre las diferentes jerarquías?			X	5.6. a)
21	¿Se desarrollan planes de mejora del desempeño basado en los resultados de los procesos contables?		X		5.6. a)
22	¿Es recurrente la supervisión sobre el cumplimiento de los objetivos en la organización?		X		5.6. b)

f) Mejora del marco de referencia de la gestión del riesgo

Tabla 18

Mejora en los cambios de gestión de riesgos

Objetivo: Evaluar si se monitorean los procesos del marco de referencia relacionados a la mejora continua en la gestión de riesgos para que la entidad logre los objetivos.

No	Mejora	Siempre	Casi Siempre	Nunca	ISO 31000:2018
1	¿La organización realiza un seguimiento continuo para la gestión del riesgo en la generación de información financiera contable ante los cambios internos y externos?			X	5.7.1
2	¿Cuándo se adapta el marco de referencia de gestión de riesgos en tecnologías se contribuye a la mejora de valor?			X	5.7.1
3	¿Se asigna a una persona responsable que se encarga de formular el plan de mejoramiento?			X	5.7.2
4	¿Se formula el plan de mejora teniendo en cuenta todas las fuentes de información?			X	5.7.2
5	¿La alta dirección revisa y aprueba los procesos que serán implementados en el plan de mejora?			X	5.7.2
6	¿El responsable designado por la gerencia registra la información soporte de los resultados obtenidos de las acciones y metas planteadas en el plan de mejoramiento?			X	5.7.2
7	¿Se evalúa los resultados alcanzados y presentados en el plan de mejoramiento para la generación de la			X	5.7.2

	información?				
8	¿El modelo evaluación para la gestión del riesgo en la generación de información financiera contable contribuye a mejorar sus procesos?			X	5.7.2
9	¿La entidad desarrolla planes y tareas ante las brechas y oportunidades de mejorar al implementar sistemas informáticos en los cuales se genera información integra?			X	5.7.2
10	¿Se realizan actividades de mejora en la integración de los módulos contables en la aplicación de la gestión de riesgo para la obtención de la información financiera?		X		5.7.2

4.4.5. Cuestionarios de evaluación del control interno informático (Capítulo 6, proceso ISO 31000:2018)

Tabla 19

Cuestionario de control interno al hardware

Objetivo: Obtener el entendimiento suficiente y adecuado sobre los riesgos en la generación de la información financiera, mediante la evaluación de los procedimientos internos de la entidad, conforme a las áreas de hardware.

No.	Área hardware	Siempre	Casi siempre	Nunca	Observación	ISO 31000:2018
	Identificación del riesgo					
1	¿Son idóneos los lugares donde se encuentran instalados los equipos informáticos en los cuales se procesa y genera la información financiera contable?		X			4. c) Adaptada
2	¿El ambiente climático para instalar los equipos de computación y comunicación en los que se procesa la información financiera, está protegido por medio de barreras y controles físicos para evitar las amenazas que afecten su normal funcionamiento?		X			4. c) Adaptada
3	¿Se aplican los procedimientos para el resguardo de la información cuando los equipos informáticos comienzan a deteriorarse?			X		4. b) Estructurada y exhaustiva

4	¿La entidad implementa los procedimientos para el resguardo de las USB o dispositivos externos en los que se almacena la información?		X			4. c) Adaptada
5	¿La organización tiene servidores que forman parte de la red y a la vez provee servicios a otros equipos como impresiones, correos, telefonía, accesos remotos, web, base de datos y seguridad en la generación y divulgación de la información financiera?	X				4. c) Adaptada
6	¿Los medios de procesamiento de la información que manejan la data confidencial se ubican de manera que se restrinja el ángulo de visión para evitar que esta sea vista por personas no autorizadas?		X			4. d) Inclusiva
	Análisis del riesgo					
7	¿La organización cuenta con una política sobre el uso del equipo informático en donde se procesa la información fuera de la entidad?		X		Esto autorizado por sus superiores.	4. b) Estructurada y exhaustiva
8	¿Se restringe a los usuarios el acceso a las redes sociales en sus dispositivos móviles asignados por la empresa en los que contiene información confidencial?		X			4. c) Adaptada
9	¿La empresa tiene identificados los activos en los que se procesa y resguarda la información financiera?	X			Se tiene identificado un 40% de sus activos	4. b) Estructurada y exhaustiva
	Valoración del riesgo					
10	Se efectúan comparaciones periódicas entre el inventario de activos de información físico y los registrados en los reportes.		X			4. d) Inclusiva
11	¿Se da seguimiento a la política de no ingerir alimentos ni bebidas en las estaciones donde se encuentra el equipo informático que genera la información?			X		4. g) Factores humanos y culturales
12	¿Se tiene en cuenta la capacidad del procesador en los activos de información con respecto a la instalación del software donde se genera la información?	X				4. a) Integrada
13	¿Llevan un control del personal que puede hacer uso del equipo informático en donde se procesa la información fuera de las instalaciones?			X		4. c) Adaptada
14	¿Cuenta la empresa con una política sobre el personal que está autorizado para manipular los dispositivos de información externos?			X		4. c) Adaptada

Tratamiento del riesgo						
15	¿Se establecen procedimientos sobre quiénes son los encargados de subir y administrar la información que se encuentra en el servidor cuando se realizan los respaldo de la información?			X		4. b) Estructurada y exhaustiva
16	¿En los periféricos de salida solo el personal autorizado puede brindar mantenimiento y realizar reparaciones preventivas para optimizar la salida de la información?	X				4. c) Adaptada
17	¿Se aplican procedimientos para realizar copias de seguridad periódicamente?		X			4. e) Dinámica
18	¿La empresa establece una política para revisar las computadoras con el fin de evaluar su estado físico y deterioro de los componentes que generan la información?		X		Se revisan cuando presentan problemas	4. c) Adaptada
19	¿Existe un plan de mantenimiento preventivo al equipo?			X		
Comunicación y consulta						
20	¿Con que frecuencia se le comunica al personal involucrado en el procesamiento y generación de la información, cuando se realizan cambios en la configuración de los componentes en los activos de la empresa?			X		4. f) Mejor información disponible
21	¿Se comunica al personal involucrado en la generación de la información los conocimientos obtenidos para resguardar y la aplicación de los procedimientos para la ejecución de la misma?		X			4. f) Mejor información disponible
22	¿La organización lleva una bitácora sobre los problemas reportados por los usuarios, que contribuyan a mejorar los procedimientos para la generación de la información?	X				4. f) Mejor información disponible
Seguimiento y revisión						
23	¿Las revisiones en el equipo informático son realizadas por el encargado del proceso de tecnología de la información?		X			4. h) Mejora continua
24	¿La empresa evalúa regularmente si los procedimientos aplicados al resguardo y confidencialidad de la información, se tiene en cuenta la integridad de los datos?		X			4. c) Adaptada
25	¿Se realizan procesos de monitoreo periódicamente para identificar los equipos informáticos que comienzan a deteriorarse?			X		4. h) Mejora continua
Registro e informe						

26	¿Los reportes emitidos por la entidad con respecto al detalle y deterioro de los activos de información, están elaborados para que la gerencia pueda tomar las decisiones pertinentes?		X			4. d) Inclusiva
27	¿Se lleva un registro sobre los usuarios que conocen sobre las directrices estratégicas del resguardo de la información?			X		4. c) Adaptada
28	¿Existen fuentes de mejoramiento en la empresa sobre las innovaciones de los activos informático que generan la información?			X		4. h) Mejora continua
29	¿El encargado del área informática elabora un informe del entorno, los avances tecnológicos y el marco normativo aplicado a la seguridad de la información?		X			4. f) Mejor información disponible
30	¿Cuándo se le da mantenimiento al equipo se realiza un informe sobre el estado de los equipos informático?		X			4. f) Mejor información disponible
31	¿La entidad lleva un registro sobre los eventos de riesgos en tecnología de la información que se hayan materializado?			X		4. f) Mejor información disponible

Tabla 20

Cuestionario de control interno al software

Objetivo: Evaluar el software que posee la entidad para identificar los procedimientos de control que implementa para gestionar los riesgos a los que se encuentra expuesta la información financiera, además se pretende verificar que el software sea compatible con las características del hardware.

No.	Área Software	Siempre	Casi siempre	Nunca	Observación	ISO 31000:2018
	Identificación del riesgo					
1	¿Se poseen licencias originales para el sistema de información contable?	X				4.a) Integrada
3	¿Se aplican accesos privilegiados a los usuarios en la base de datos contable de la entidad?		X			4.d) Inclusiva
4	¿Se realizan pruebas en los sistemas de información financiera para asegurar que no existan errores de diseño?			X		4.c) Adaptada

	Análisis de riesgos					
5	¿El personal de contabilidad conoce los riesgos asociados software contable?		X			4.g) Factores humanos y culturales
6	¿Se cuenta con accesos restringidos en el software de aplicación contable?	X				4.b) Estructurada y exhaustiva
7	¿Se implementan controles para instalar aplicaciones ofimáticas en los equipos informáticos?	X				4.d) Inclusiva
8	¿Se poseen antivirus en los sistemas de almacenamiento de información?	X				4.d) Inclusiva
9	¿La entidad aplica controles de restricción al personal de contabilidad para instalar o desinstalar programas en el software?		X			4.b) Estructurada y exhaustiva
10	¿Se realizan actualizaciones al equipo informático para asegurar que la información se encuentre disponible para los usuarios internos y externos?		X			4.a) Integrada
11	¿Cuenta la empresa con software antivirus que protejan el Sistema Operativo?	X				4.a) Integrada
12	¿El departamento de informática instala aplicaciones que detecten errores o irregularidades en los equipos realizadas por los usuarios?			X		4.a) Integrada
13	¿La entidad registra el software desarrollado internamente?			X		4.a) Integrada
	Valoración del riesgo					
14	¿La organización establece jerarquías en el acceso a los módulos del sistema contable informático?		X			4.f) Mejor información disponible
15	¿El departamento de informática realiza mantenimiento preventivo al software de la entidad así como a los equipos?		X			4.d) Inclusiva
16	¿Se establecen mecanismos necesarios para el resguardo de información del sistema contable?		X			4.c) Adaptada
	Tratamiento del riesgo					
17	¿Se realizan mantenimientos preventivos con regularidad al sistema operativo de los equipos?		X			4.d) Inclusiva
20	¿Se aplican controles al software libres para prevenir daños a los sistemas informáticos?		X			4.f) Mejor información disponible
	Comunicación y consulta					
21	¿Se comunican al departamento de informática sobre los fallos o errores en los módulos software contable?		X			4.d) Inclusiva

22	¿Los usuarios notifican al encargado de TI sobre cualquier sospecha de incidente de seguridad en los sistemas de información?		X			4.d) Inclusiva
23	¿Se informa a los empleados, sobre los riesgos existentes al acceder a enlaces sospechosos o al descargar archivos adjuntos en el correo electrónico de remitentes desconocidos?			X		4.d) Inclusiva
24	¿Se crea a los empleados de la entidad correo empresarial para comunicar información interna como externa de la organización?		X			4.g) Factores humanos y culturales
	Seguimiento y revisión					
25	¿Se aplican controles para mitigar riesgos relacionados con la generación de información financiera contable?			X		4.b) Estructurada y exhaustiva
26	El encargado de TI realiza las actualizaciones de los software de manera oportuna, con la finalidad de que la información financiera se encuentre disponible para la toma de decisiones		X			4.h) Mejora continua
	Registro e informe					
27	¿Se realizan planes o procedimientos para resguardar información sobre activos intangibles dados de baja cuando se actualizan o se cambian?	X				4.b) Estructurada y exhaustiva
28	¿Se registran los intentos de accesos no autorizados los diferentes módulos la entidad para evitar la fuga de información?			X		Estructurada y exhaustiva
29	¿El departamento de informática registra la actividad diaria al módulo de transacciones para detectar errores u omisiones?		X			4.d) Inclusiva
30	¿Se registran el límite de errores en las contraseñas al ingresar al sistema de contabilidad?		X			4.g) Factores humanos y culturales

Tabla 21

Cuestionario de control interno informático a la seguridad física.

Objetivo: Identificar de forma independiente las amenazas y vulnerabilidades que intervienen en el área de seguridad física, que permita verificar el cumplimento de los procedimientos implementados en la generación de la información.

N°	Área seguridad física	Siempre	Casi siempre	Nunca	Observación	ISO 31000:2018
	Identificación del riesgo					
1	¿Los interruptores de energía están debidamente protegidos y sin obstáculos para alcanzarlos?		X			4.c) Adaptada
2	¿Existe seguridad en el voltaje y cableado en las instalaciones eléctricas?		X			4.e) Dinámica
3	¿El departamento de informática es el responsable de resguardar los accesorios en los cuales se almacena los respaldos de información?		X			4.f) Mejor información disponible
4	¿Existe en la entidad impresoras que son utilizadas para todos los usuarios?			X		4.c) Adaptada
5	¿Se efectúan mantenimientos en los techos de las instalaciones en las que se encuentran los activos que almacenan la información?	X				4. d) Inclusiva
6	¿Se le asigna a cada personal responsable del equipo informático su respectivo UPS?		X			4.c) Adaptada
7	¿Se restringe el acceso de personal no autorizado al departamento de contabilidad, cuando abandonan su estación de trabajo	X				4.e) Dinámica
	Análisis del riesgo					
8	¿La entidad tiene una planta generadora de electricidad en caso de interrupciones de energía?			X		4.c) Adaptada
9	¿Existen contratos vigentes con otras entidades responsables del mantenimiento de aire acondicionado?	X				4. b) Estructurada y exhaustiva
10	¿Se protegen los sitios donde se encuentren sistemas de procesamiento informático o de almacenamiento, implementando accesos autorizados y utilizando tecnologías de autenticación?			X		4. e) Dinámica

11	¿En el área de informática existen materiales que sean inflamables o causar algún daño a los equipos?		X			4.c) Adaptada
	Valoración del riesgo					
12	¿Existe clasificación de bienes susceptibles de daño entre los que se encuentren: los activos de información?		X			4. e) Dinámica
13	¿Se registra el acceso de personas ajenas al departamento de informática?		X			4.c) Adaptada
	Tratamiento del riesgo					
14	¿La organización cuenta con una política sobre la destrucción de sus equipos informáticos en los que se genera la información?			X		4.e) Dinámica
15	¿El sistema de vigilancia mediante cámaras de seguridad, comprende el área de informática en donde se protege la información?	X				4. d) Inclusiva
16	¿Los recursos de la infraestructura tecnológica son suficientes para atender las demandas del usuario que generan la información?		X			4.c) Adaptada
17	¿Existen en la empresa señalizaciones adecuada en caso de siniestros?	X				4.c) Adaptada
18	¿Las instalaciones tienen puertas con control de acceso restringido, en los que se encuentran los servidores que protegen los datos?	X				4.c) Adaptada
19	¿Se cuentan con planes de contingencia en caso de terremotos, incendios o inundaciones?			X		4.e) Dinámica
	Comunicación y consulta					
20	¿La empresa cuenta con una política de difundir formalmente a los usuarios los planes de seguridad en informática para proteger los activos e infraestructura?		X			4. d) Inclusiva
	Seguimiento y revisión					
21	¿Con que frecuencia son revisado las cámaras de vigilancia del personal que entra al departamento de informática y tiene acceso a la información de los servidores?			X		4. d) Inclusiva
	Registro e informe					
22	¿Existe una evaluación documentada del proceso de servicios proporcionados en el mantenimiento de la infraestructura?			X		4. b) Estructurada y exhaustiva

Tabla 22

Cuestionario de control interno informático a la seguridad lógica.

Objetivo: Examinar las principales fuentes de riesgos en las cuales se encuentra expuesta la información, así como el acceso ordenado y autorizado de los usuarios verificando las medidas aplicadas por la administración y administradores de TI para minimizar los riesgos de seguridad en la información financiera contable.

No	Área Seguridad lógica	Siempre	Casi siempre	Nunca	Observación	ISO 31000:2018
	Identificación del riesgo					
1	¿La organización tiene una política de privilegios de contraseñas de los usuarios para el acceso a los módulos de contabilidad?	X				4.c) Adaptada
2	¿Cada usuario posee su propia clave de acceso para ingresar al software de aplicación contable?		X			4.c) Inclusiva
3	¿Se utilizan antivirus con licenciamiento que detecten accesos no autorizados para evitar la fuga de información contable?	X				4.a) Integrada
4	¿Se tienen asignación de roles y privilegios para acceder al módulo de transacciones de la entidad?		X			4.h) Factores humanos y culturales
5	¿Se verifica que los respaldos de los registros contables se realicen periódicamente?			X		4.e) Dinámica
	Análisis del riesgo					
6	¿Se utilizan técnicas criptográficas para el resguardo de la información financiera contable?			X		4.b) Estructurada y exhaustiva
7	¿La entidad realiza copias de la información procesada por el sistema, y éstas estás se resguardan en un lugar seguro?		X			4.b) Estructurada y exhaustiva
8	¿Se cuenta con un listado de acceso a los equipos informáticos para garantizar que solo personal adecuado ingrese a la información financiera?			X		4.d) Inclusiva
9	¿Se realiza un respaldo periódico del sistema operativo y del sistema informático para obtener la información disponible para los usuarios internos como los externos?		X			4.d) Inclusiva

	Valoración del riesgo					
10	¿Se cuentan con controles de identificación y autenticación para el acceso del software contables y la nube de la entidad?		X			4.a) Integrada
11	¿Existe una adecuada asignación de responsables para los equipos informáticos que procesan información financiera?		X			4,g) Factores humanos y culturales
12	¿Se establecen políticas de cierre de sesión seguras para el departamento de contabilidad?			X		4.e) Dinámica
13	¿Se limita y controla al personal en cuanto al uso de programas utilitarios para procesar información financiera?		X			4.d) Inclusiva
	Tratamiento del riesgo					
14	¿El sistema registra en cada uno de los reportes emitidos la fecha, hora, nombre del usuario, para controlar el uso de la información por el personal de la organización?		X			4.b) Estructurada y exhaustiva
15	¿Se le da cumplimiento a la política para cambiar las contraseñas de acceso con regularidad a los módulos de contabilidad?			X	No se realizan cambios	4.h) Mejora continua
16	¿Se otorgan privilegios mínimos a los usuarios del sistema informático en cuanto a la información financiera?		X			4.b) Adaptada
17	¿Existen software de aplicación para detectar códigos maliciosos que puedan afectar la información de la organización?		X			4.d) Inclusiva
	Comunicación y consulta					
18	¿Existe acceso restringido a los usuarios para instalar actualizaciones de los sistemas contables?	X				4.b) Estructurada y exhaustiva
19	¿Se comunica a los usuarios sobre los controles aplicables para transferir información contable por medio de correo electrónico, memorias USB?		X			4.b) Estructurada y exhaustiva
20	¿Se informa a los empleados que los contraseñas se deben estructurar incluyendo, mayúsculas, minúsculas, números, etc.?			X		4.b) Estructurada y exhaustiva
21	¿La entidad comunica las políticas de seguridad de la información para el uso de los recursos tecnológicos?			X		4.d) Inclusiva
	Seguimiento y revisión					
22	¿Se realiza un reporte donde se lleve un registro detallado de cada uno de los usuarios existentes en la entidad del departamento de contabilidad para evitar			X		4.h) Mejora continua

	la fuga de información?					
23	¿Se verifica que la longitud de las contraseñas de acceso a los sistemas informáticos tenga un mínimo de caracteres?		X			4.b) Estructurada y exhaustiva
24	¿Existe algún procedimiento para garantizar que los usuarios cambien las contraseñas asignadas por defecto?		X			4.h) Mejora continua
25	¿El encargado de tecnología de la información verifica que los empleados realicen los respaldos de información?		X			4.d) Inclusiva
	Registro e informe					
26	¿Se le da seguimiento a las actividades que realizan los usuarios para prevenir el riesgo de modificación o borrado de la información?			X		4.h) Mejora continua
27	¿Se realizan reportes de acceso de todos los procedimientos realizados por los usuarios en los módulos contables?			X		4.c) Adaptada
28	¿El departamento de informática controla y registra los cambios de contraseñas realizados por los usuarios?	X				4.h) Mejora continua
29	¿Se realiza un informe de los accesos borrados y/o modificados del personal que ya no labora para la organización?	X				4. g) Factores humanos y culturales
30	¿Existen medios de almacenamiento externos en caso de fallo o destrucción del sistema informático?		X			4.d) Inclusiva

Tabla 23

Cuestionario de control interno informático a recursos humanos.

Objetivo: Evaluar si se aplican los principios del marco de referencia en el área de recursos humanos para la integridad de la información generada en los sistemas

No.	Área recursos humanos	Siempre	Casi siempre	Nunca	Observación	ISO 31000:2018
	Identificación del Riesgo					
1	¿Se brinda una inducción al personal reclutado en cuanto al proceso de manejo de la información?			X		4.g) Factores humanos y culturales.

2	¿Existe una política de capacitación al personal en los diferentes marcos normativo sobre seguridad de la información?			X		4.e) Dinámica
3	¿Se implementan medidas de seguridad en los recursos informáticos asignados al personal cuando éstos cesan de sus funciones			X		4.g) Factores humanos y culturales
4	¿Se aplican procedimientos de seguridad cuando se contrata personal eventual para utilizar los equipos informáticos donde se registra la información financiera contable?			X		4.b) Estructurada y exhaustiva
5	¿El personal contratado ha firmado un acuerdo formal que indique su obligación de cumplir con el requisito de confidencialidad?			X		4.e) Dinámica
	Análisis del Riesgo					
6	¿El personal asignado aplica en las estaciones de trabajo los procedimientos establecidos por la entidad, para que la información sea integra?		X			4.g) Factores humanos y culturales.
7	¿Se concientiza a los empleados acerca de la importancia de la seguridad de la información especialmente en el área financiera y contable?		X			4.e) Dinámica
8	¿Existen procedimientos para verificar que la información registrada en aplicaciones ofimáticas sea ingresada en el módulo de contabilidad?			X	El 65% de la facturación se realiza en Microsoft Excel	4.b) Estructurada y exhaustiva
	Valoración del Riesgo					
9	¿La entidad cuenta con procedimientos definidos para la asignación, atención y seguimiento en los incidentes generados por los usuarios al momento de ingresar los datos a los sistemas de información contable?			X		4.e) Dinámica
10	¿La capacitación que se brinda a los usuarios es efectiva para que puedan utilizar eficaz y eficientemente los recursos informáticos en los que se genera la información financiera contable?		X		Se capacita al personal sobre los recursos informáticos	4.c) Adaptada
11	¿El personal cuenta con las actitudes y aptitudes requeridas para hacer uso de la información por medio de las soluciones automatizadas?			X		4.g) Factores humanos y culturales
12	¿El personal cuenta con el tiempo suficiente para recibir, de manera completa las capacitaciones correspondientes a los módulos que están utilizando?			X		4.e) Dinámica

	Tratamiento del Riesgo					
13	¿Se envían correos de recordatorio a los empleados para el caso de los cierres contables?	X				4.h) Mejora continua
14	¿Se limita el acceso a la información a los usuarios que no pertenezca a su área o departamento?		X			4.b) Estructurada y exhaustiva
15	¿Se capacita a los empleados para el ingreso correcto de datos a los sistemas de información?			X	Estas capacitaciones son por medio de video conferencias.	4.h) Mejora continua
16	¿Los empleados siguen los procedimientos escritos según su rol o función?	X				4.g) Factores humanos y culturales
17	¿Se aplican controles para bloquear el acceso de correos maliciosos			X		4.h) Mejora continua
	Comunicación y consulta					
18	¿Los usuarios conocen sobre los procedimientos que se debe seguir para reportar los incidentes relacionados a la generación de la información?			X		4.b) Estructurada y exhaustiva
19	¿La organización utiliza los diferentes canales de comunicación para informar a los usuarios sobre nuevas directrices de seguridad en el ingreso de los datos?		X			4.f) Mejor información disponible
20	¿Se les comunica a los usuarios sobre los planes de trabajo y compromisos de la entidad orientada al logro de los objetivos?	X				4.h) Mejora continua
	Registro e informe					
21	¿Existen manuales de usuario para ingresar la información a cada módulo del software contable?			X	Estos manuales los manejan los del área de informática.	4.f) Mejor información disponible
22	¿Existen parámetros de seguridad en los reportes para evitar que los usuarios puedan manipular los informes que se generan desde los sistemas informáticos?			X	Los reportes se generan en Excel o PDF y pueden ser modificados	4.c) Adaptada

Tabla 24

***Control interno informática al procesamiento electrónico de datos*.**

Objetivo: Evaluar el funcionamiento de los sistemas de información contable en la captura, procesamiento, almacenamiento y salida de información, para asegurar la exactitud de los registros de la organización.

No.	Área procesamiento electrónico de datos	Siempre	Casi Siempre	Nunca	Observación	ISO 31000:2018
	Identificación del riesgo					
1	¿Se verifica los documentos de compra ingresados en el sistema, estén de acuerdo a los comprobantes de créditos fiscales físicos?	X				4.d) Inclusiva
2	¿Existe una política y procedimientos aplicados al control interno informático en el procesamiento electrónico de datos?			X		4.g) Factores humanos y culturales
3	¿Se verifica que la información este validada antes de ser procesada en el sistema, con la finalidad de asegurar la integridad de la información?	X				4.a) Integrada
4	¿La entidad controla que la información almacenada en el sistema posea la documentación física o digital que la respalde?	X				4.d) Inclusiva
5	¿El procesamiento de la información en los módulos de contabilidad se realiza en línea permitiendo la actualización de los procesos de la entidad?	X				4.a) Integrada
6	¿Existen controles para autenticidad de datos mediante la validación al ser ingresado al sistema contable?		X			4.f)Mejor información disponible
7	¿Se llevan reportes de las fallas de exactitud en los procesamientos de información?			X		4.c Adaptada
8	¿Existe personal autorizado para realizar cambios en los registros ingresados en los módulos contables?			X		4.b) Estructurada y exhaustiva
	Análisis del riesgo					
9	Se ingresan los productos al módulo de inventarios siempre y cuando estén debidamente autorizados y se verifiquen físicamente		X			4.h Mejora continua

10	¿Se verifica que todas las transacciones han sido correctamente registradas, comprendidas y clasificadas en el sistema de información contable?		X			4.b) Estructurada y exhaustiva
11	¿La entidad posee un software de gestión de riesgos para identificar posibles vulnerabilidades?			X		4.h Mejora continua
12	¿El módulo de asientos diarios permite guardar una partida descuadrada?		X		Permite guardar la partida descuadrada, pero no puede ser mayorizada	4.a) Integrada
13	¿Existen controles para verificar que la información que se migra de los módulos se hace adecuadamente?			X		4.d) Inclusiva
14	¿Se aplican controles para estimar el impacto de los riesgos tecnológicos relacionados a la entrada, procesamiento y salida de datos de los sistemas?			X		4.a) Integrada
	Valoración del riesgo					
15	¿El software contable genera informes de excepciones?		X			4.a) Integrada
16	¿Se verifica que en los retaceos originados por las importaciones sean incluidos de forma correcta en el inventario?		X			4.f) Mejor información disponible
17	¿El departamento de contabilidad asigna privilegios de acceso a los usuarios para eliminar, leer, adicionar y modificar registros almacenados en el software contable?	X				4.d) Inclusiva
18	¿Se poseen controles de seguridad en el almacenamiento de la información financiera en la nube?		X			4.c) Adaptada
19	¿Se realizan recalculó manuales para asegurar que el software contable procese de manera correcta los datos numéricos?		X			4.a) Integrada
20	El módulo de facturación no permite ingresar productos que no se encuentra en el inventario	X				4.a) Integrada
21	Se realizan conteos físicos para comparar las cantidades registradas en los módulos de inventarios con la existencia en bodega		X			4.f) Mejor información disponible
22	¿Los datos registrados en el software poseen fecha y hora en la cual fueron ingresados para su procesamiento?	X				4.d) Inclusiva
23	¿Se aplican controles para restringir los cambios no autorizados en los sistemas de información contable?		X			4.h) Mejora Continua

	Tratamiento del riesgo					
24	¿Se restringe el acceso a los sistemas de información de contabilidad en sus diferentes módulos a través de contraseñas?		X			4.a) Integrada
25	¿Existen controles de salidas de las transacciones registradas en los sistemas?		X			4.f) Mejor información disponible
26	¿Se verifica que las órdenes de pedido, de salida, créditos fiscales se encuentren autorizadas y cumplan con los requisitos legales correspondientes?		X			4.f) Mejor información disponible
27	¿Se aplican controles de autorización para la salida de información financiera de la entidad?			X		4.d) Inclusiva
28	El sistema guarda los intentos de cambio en los registros contables realizados por los usuarios			X		4.b) Estructurada y exhaustiva
29	¿Existen procedimientos para validar la información de cálculos aritméticos de los registros y controles contables de la entidad que permita asegurar la integridad de los datos ingresados en el sistema?	X				4.b) Estructurada y exhaustiva
30	¿Existen procedimientos de control para evitar la duplicidad de los datos?		X			4.g) Factores humanos y culturales
31	¿El software contable implementa el método de digito auto verificador para evitar duplicidad de información y validar datos?	X				4.b) Estructurada y exhaustiva
32	¿Existe un software que detecte e inicie una acción correctiva sobre los errores de la información en el procesamiento?			X		4.f) Mejor información disponible
33	¿Existe una metodología para autorizar, priorizar y rastrear los requerimientos de cambios en los sistemas?			X		4.c) Adaptada
34	¿Se realizan planes de capacitación para el procesamiento de la información?		X			4.f) Mejor información disponible
35	¿El software contable realiza búsqueda de registros duplicados?			X		4.b) Estructurada y exhaustiva
36	¿Se utiliza la firma electrónica para la transmisión de datos que aseguren el origen y destino de la información ¿	X			Se utiliza para la autorización de pedidos	4.a) Integrada
37	¿El sistema de información permite la existencia de campos vacíos o espacios en blanco?			X		4.b) Estructurada y exhaustiva
38	Se aplican controles antes de registrar las transacciones para evitar la existencia de errores			X		4.d) Inclusiva

	Comunicación y consulta					
39	¿Los usuarios del departamento de contabilidad comunican los fallos en el software que pueden perjudicar el ingreso de la información de la entidad?		X			4.h) Mejora Continua
40	¿Se comunican a los usuarios los controles de redundancia en los sistemas de información contable?		X			4.f) Mejor información disponible
41	Existen controles al momento de trasladar los asientos diarios al libro mayor en el módulo de contabilidad			X		4.b) Estructurada y exhaustiva
42	Se comunica a los usuarios la existencia de planes de contingencia en caso de fallos del sistema		X			4.h) Mejora Continua
43	La organización comunica a sus empleados que las claves de acceso son confidenciales y no deben ser reveladas	X				4.g) Factores humanos y culturales
	Seguimiento y revisión					
44	¿Existe una adecuada segregación de funciones en cuanto a la autorización y verificación de los registros?		X			4.b) Estructurada y exhaustiva
45	¿Los cálculos, datos e información numérica proporcionada por los reportes del sistema está acorde a los requerimientos de la normativa tributaria aplicable		X			4.c) Adaptada
46	¿Existe controles en el ingreso de la información así como las salidas de los datos?		X			4.d) Inclusiva
47	¿Existe un control de seguimiento a los errores reportados o encontrados en el procesamiento electrónico de datos?		X			4.h) Mejora continua
48	¿El departamento de contabilidad verifica la información antes de ser ingresada al módulo de compras?	X				4.d) Inclusiva
49	¿Existe un control de seguimiento para los errores cometidos en los módulos contables para asegurar la integridad de la información?			X		4.h) Mejora continua
50	¿Se utilizan software de recuperación de información cuando se borra información de forma accidental?			X		4.b) Estructurada y exhaustiva
	Registro e informe					
51	Existe un registro de historial de los cambios realizados por los usuarios en los registros contables		X			4.d) Inclusiva
52	¿Se lleva una bitácora de salida de información financiera contable a través de las impresoras de la entidad?	X				4.h) Mejora continua

53	Los reportes generados por el software contable refleja, fecha, hora, nombre de usuario para controlar quienes han ingresado la información		X			4.a) Integrada
54	Se elabora una bitácora sobre la migración de información contable generados por el sistema de información		X			4.f) Mejor información disponible

Tabla 25
Control interno informático al área de redes

Objetivo: Evaluar los equipos informáticos y software conectados entre sí por medio de dispositivos físicos, que a su vez permiten el transporte de datos, con la finalidad de compartir información a usuarios internos como externos.

No.	Área redes	Siempre	Casi Siempre	Nunca	Observación	ISO 31000:2018
	Identificación del Riesgo					
1	¿Se crea cuentas de usuario para el personal eventual del departamento de contabilidad para la generación de información?			X		4.c) Adaptada
2	¿El personal de informática asigna cuentas de usuario con una solicitud de autorización de los encargados de cada departamento donde se procesa información?	X				4.d) Inclusiva
3	¿Se limita a los usuarios a poder adicionar, eliminar, leer y modificar información a programas y aplicaciones contables?		X			4.b) Estructurada y exhaustiva
4	¿Se les otorga privilegios de acceso a los usuarios de acuerdo al desempeño de las funciones de cada usuario para evitar la divulgación de la información?		X			
5	¿Existen controles de seguridad en la información compartida por medio de la red interna de la entidad?			X		4.f) Mejor información disponible
	Análisis del Riesgo					
6	¿Se deshabilitan los accesos de la red en los equipos del área de contabilidad dados de baja?			X		4.h) Mejora continua
7	¿Existen planes de contingencia en caso de caídas del servicio de internet para evitar pérdidas de información?	X				4.h) Mejora continua

8	¿Se restringen las conexiones de algún nuevo usuario en la red?		X			
9	¿Existe un software de aplicación que gestione a la red de la entidad?			X		
	Valoración del Riesgo					
10	¿Se limitan a los usuarios de contabilidad los accesos a sitios web que no posean el protocolo https?		X			4.d) Inclusiva
11	¿El servicio de internet cuenta con la capacidad necesaria para la efectiva transmisión de información?		X			
12	¿Se implementa controles para asegurar una buena configuración en la red?			X		4.b) estructurada y exhaustiva
13	¿La capacidad de conexión de cada usuario se reparte según las funciones laborales?	X				
14	Se posee historial de las conexiones realizadas por los usuarios		X			
	Tratamiento del Riesgo					
15	¿Se cuenta con una red privada para limitar el acceso a datos financieros de la entidad?	X				4.f) Mejor información disponible
16	¿Existen procedimientos de autenticación para conectar un nuevo equipo a la red?	X				4.a) Integrada
17	¿Se mantiene activo el uso de firewall para proteger el tráfico de información entre los dispositivos de la entidad?		X			4.a) Integrada
18	¿Se restringe el envió de información a servicios de correo electrónico comerciales ajenos a la entidad?			X		4.e) Dinámica
19	Se establece un número determinado de dispositivos que pueden conectarse a la red	X				
	Comunicación y consulta					
20	¿El encargado de TI comunica a los usuarios cuando se realizan mantenimientos en los sistemas de información?		X			4.f) Mejor información disponible
21	¿El usuario informa sobre las caídas en los servidores de la entidad para implementar medidas de seguridad en la información de la entidad?		X			4.h) Mejora Continua
	Seguimiento y Revisión					
22	¿Se monitorea el acceso a páginas no autorizadas para evitar el riesgo de robo de información?			X		4.d) Inclusiva
23	¿Se lleva un seguimiento a los fallos en la red para así evitar futuras fugas de información?		X			

24	Se aplican controles de mantenimiento de la red para asegurar la disponibilidad de la información		X			
	Registro e Informe					
25	¿Se realizan informes donde se registren los helpware solicitados al departamento de informática en caso de fallo en la red de la entidad?			X		

4.4.6. Criterios de evaluación de riesgos

Para la evaluación de riesgos se utilizarán, valores primarios, para la calificación de impacto y probabilidad de cada riesgo. Para ambos casos se tomarán en cuenta tablas de 3 valores con equivalencias que será descritas a continuación, a partir de estos valores se calculará el nivel de exposición y severidad de los riesgos que serán representados en el mapa de calor.

Calificación de la probabilidad

Probabilidad	
3	Alto
2	Medio
1	Bajo

Para calificar el impacto se utilizará una tabla general con 3 valores; que adicionalmente se utilizarán en unas tablas para en los cuales se describirán los criterios para asignarle la calificación de probabilidad e impacto a cada riesgo.

Calificación del impacto

Impacto	
3	Alto
2	Medio
1	Bajo

Mapa de calor

A continuación, se presenta el modelo de mapa de calor en el cual según la calificación de impacto y probabilidad del riesgo es calificado por color en su nivel de severidad. El color rojo representa un riesgo alto, el color naranja riesgo medio y el verde un riesgo bajo:

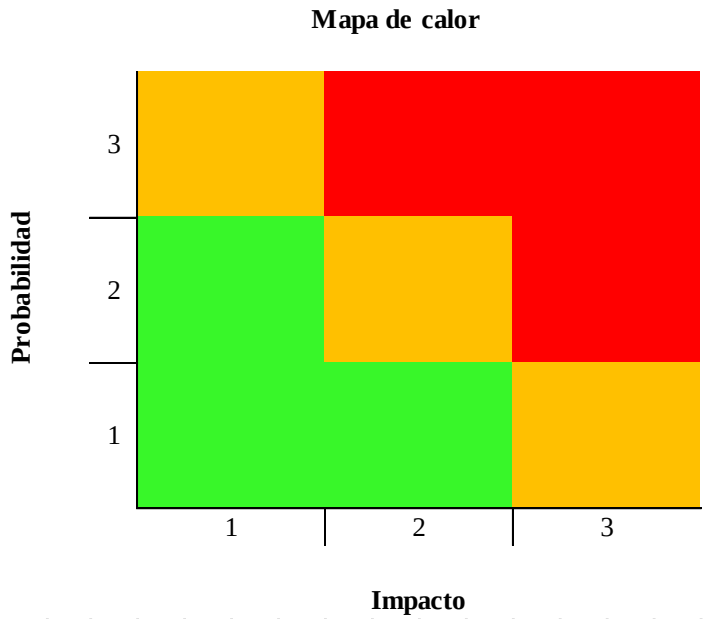


Figura 6: Mapa de calor para matriz de riesgo

Valoración del riesgo

Después de evaluar cada componente de los sistemas de información, en el cual se obtuvo las principales fuentes de amenazas así como las vulnerabilidades existentes, se establecen los criterios de riesgos establecidos cuando se requiere una acción adicional que son los siguientes:

Tabla 26

Valoración del riesgo

Valoración del riesgo	
A	No hacer nada más
B	Considerar opciones para el tratamiento del riesgo
C	Realizar un análisis adicional para comprender mejor el riesgo
D	Mantener los controles existentes

El propósito de la valoración es apoyar a la toma de decisiones sobre la manera de tratar los riegos presentes en el uso de las tecnologías de la información, así como aplicar los métodos más apropiados para el tratamiento de los riesgos.

4.4.7. Resumen de evaluación de cada área de los componentes de los sistemas de información

ÀREA DE EVALUACIÒN	Siempre	Casi siempre	Nunca	Grado del riesgo
Hardware	1,61	4,84	3,55	Medio
Software	2,33	5,33	2,33	Alto
Seguridad física	2,73	4,09	3,18	Medio
Seguridad lógica	2,67	3,33	4,00	Medio
Recursos humanos	1,43	2,38	6,19	Alto
Redes	2,40	4,4	3,2	Medio
Procesamiento electrónico de datos	2,41	4,630	2,96	Medio

Criterio de evaluación de áreas criticas

Riesgos alto	5,01 - 10,00
Riesgo medio	3,01 - 4,99
Riesgo bajo	1.00 - 3.00

A través de la evaluación de los componentes de los sistemas de información, se aplicó un cuestionario para conocer el nivel de riesgos en el que se encuentran presentes en el hardware, software, seguridad lógica, seguridad física, redes, procesamiento electrónico de datos y los recursos humanos, se logró determinar que el área más vulnerable son los recursos humanos ya que la mayoría de errores son cometidos al momento de ingresar los registros a los módulos contables.

Tabla 27

Valoración del riesgo del área de hardware

N°	Actividades	Causa del riesgo	Riesgo	Probabilidad	Impacto	Valoración	Tratamiento
1	Son idóneos los lugares donde se encuentran instalados los equipos informáticos	Los suministros de energía en los equipos informáticos están dañados	Pérdida económica	2	2	**4**	**B**
2	El ambiente climático de los equipos de computación y comunicación en los que se procesa la información financiera, está protegido por medio de barreras y controles físicos para evitar las amenazas que afecten su normal funcionamiento	La organización no da mantenimiento a La infraestructura La infraestructura es alquilada	Pérdida económica	1	3	**3**	**D**
3	Resguardo de la información cuando los equipos informáticos comienzan a deteriorarse	Falta de experiencia en la administración para establecer políticas sobre el resguardo de la información	Pérdida de información	2	3	**6**	**B**

4	Implementación de procedimientos para el resguardo de dispositivos externos	Cada usuario es responsable de sus dispositivos	Pérdida de información	2	2	**4**	**C**
5	Servidores con la capacidad necesaria para soportar los procesos en el ingreso de información	Se tiene un servidor que cuenta con las características para proveer servicio a otros equipos	Pérdida de integridad en la información	1	1	**1**	**D**
6	Los medios de procesamiento de la información que manejan la data confidencial se ubica de manera que se restrinja el ángulo de visión para evitar que esta sea vista por personas no autorizadas	Los equipos están en áreas que se puede visualizar la información de otro usuario	Divulgación de la información	2	2	**4**	**B**
7	Conocimiento de una política sobre el uso del equipo fuera de las instalaciones	La administración no identifica esa área como un riesgo.	Robo de información	1	3	**3**	**B**
8	Se restringe a los usuarios el acceso a las redes sociales en sus dispositivos móviles	Libre acceso a las redes sociales por obligaciones laborales	Divulgación de la información	2	2	**4**	**B**
9	Identificación de los activos utilizados para procesar y resguardar la información financiera contable	Solo se tienen identificados los activos con valor monetario	Pérdidas económicas	1	2	**2**	**A**
10	Se efectúan comparaciones periódicas entre el inventario de activos de información físico y los registrados en los reportes.	El departamento de informática no tiene personal responsable de los activos	Pérdidas económicas	1	3	**3**	**C**
11	Se da seguimiento a la política de no ingerir alimentos ni bebidas en las estaciones de trabajo	El personal de la empresa conoce la política pero no la implementan. La administración no le da seguimiento a la política para que esta se cumpla.	Pérdidas económicas	3	3	**9**	**B**
12	Capacidad del procesador en los activos de información con respecto a la instalación del software contable	Se toma en cuenta los requisitos los Software para la compra del equipo informático	Pérdida de integridad en la información	1	1	**1**	**D**
13	Controles de los equipos informáticos utilizados fuera de las instalaciones de la empresa	Falta de controles del departamento de TI en los reportes del equipo informático utilizado para ingresar información fuera de a la oficina	Robo de información	3	2	**6**	**B**
14	Implementación de política sobre el personal que está autorizado para manipular los dispositivos de información externos	Se libera el equipo de algunas políticas de seguridad cuando estas están fuera de la organización	Robo de información	2	3	**6**	**B**

15	Procedimientos sobre quiénes son los encargados de subir y administrar la información que se encuentra en el servidor	No existen procedimientos para subir archivos al servidor cada usuario sube lo que considera útil	Pérdida de Información	3	2	**6**	**B**
16	En los periféricos de salida solo el personal autorizado puede brindar mantenimiento y realizar reparaciones preventivas para optimizar los recursos	La organización mantiene en arrendamiento los periféricos de salida	Robo y pérdida de información	1	1	**1**	**A**
17	Se aplican procedimientos para realizar copias de seguridad periódicamente	Se realizan copias de seguridad solo al sistema contable una vez por semana	Pérdida de Información	2	2	**4**	**D**
18	Política para revisar las computadoras con el fin de evaluar su estado físico y deterioro de los componentes	No existe una política sobre la evaluación de los equipos	Pérdida de Información	3	1	**3**	**B**
19	Existe un plan de mantenimiento preventivo al equipo	Los costos por los servicios son demasiado altos	Pérdida de Información	3	3	**9**	**B**
20	Se le comunica frecuentemente al personal involucrado en el procesamiento de la información, cuando se realizan cambios en la configuración de los componentes en los activos de la empresa	Falta de comunicación de la administración a personal involucrado en el ingreso de la información	Perdida de Información	3	3	**9**	**B**
21	Comunicación al personal sobre los avances obtenidos en la aplicación de los procedimientos para proteger los activos	Los canales de comunicación son débiles en la organización	Perdidas económicas	1	3	**3**	**B**
22	Se lleva una bitácora sobre los problemas reportados por los usuarios, que contribuyan a mejorar los procedimientos para la generación de la información	En el sistema de información los usuarios reportan los problemas que se generan con los equipos	Perdida de información	1	2	**2**	**D**
23	Las revisiones en el equipo informático son realizadas por el encargado del proceso de tecnología de la información	No se tiene definido a la persona responsable de realizar las revisiones	Perdida de Información	2	2	**4**	**C**
24	La empresa evalúa regularmente si los procedimientos aplicados al resguardo y confidencialidad de la información, se tiene en cuenta la integridad de los datos	El encargo del departamento de TI, lo está tratando de implementar	Perdida de información	3	1	**3**	**C**

25	Se realizan procesos de monitoreo periódicamente para identificar los equipos informáticos que comienzan a deteriorarse.	Los usuarios reportan cuando el equipo se le deteriora	Perdida de información	3	2	**6**	**B**
26	Los reportes emitidos por la entidad con respecto al detalle y deterioro son elaborados para que la gerencia pueda tomar las decisiones pertinentes	La organización no revisa los reportes sobre los activos de información	Perdida de información	2	2	**4**	**B**
27	Se lleva un registro de las personas que conocen sobre las directrices estratégicas de la información para fortalecer el crecimiento y desarrollo de la misma.	Solo los gerentes conocen de las directrices estratégicas para proteger la información	Perdida de información	2	3	**6**	**B**
28	Existen fuentes de mejoramiento sobre las innovaciones de los activos informático que generan la información.	El departamento de informática es el responsable de conocer sobre los nuevos equipos que salen a la venta en el mercado.	Perdida de información	2	3	**6**	**B**
29	El encargado del área informática elabora un informe del entorno, los avances tecnológicos y el marco normativo aplicado a la seguridad de la información.	No se elaboran informes, pero el área de tecnología ésta informado sobre los marcos normativos	Perdida de información	2	2	**4**	**C**
30	Cuando se les da mantenimiento a los equipos se realiza un informe sobre el estado de los equipos informático.	El responsable de dar mantenimiento en ocasiones emite un informe sobre el estado del equipo	Pérdida de información	3	1	**3**	**D**
31	La entidad lleva un registro sobre los eventos de riesgos en tecnología de la información que se hayan materializado	No se registran los eventos que se han materializado con respecto los equipos	Pérdida económica	3	2	**6**	**B**

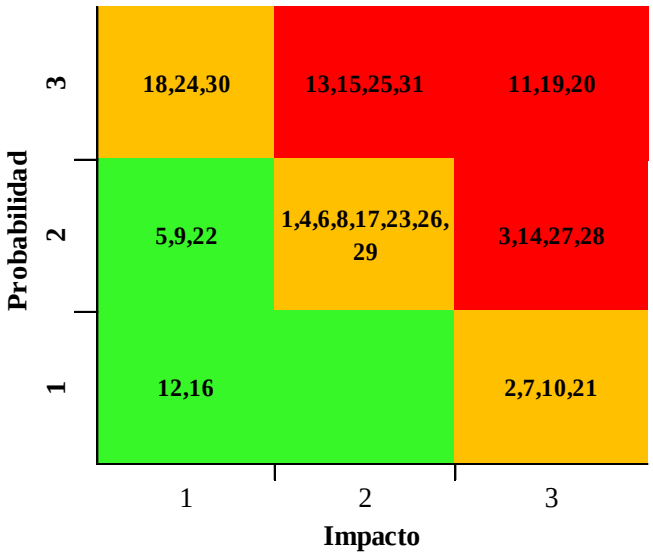


***Figura 6*:** Mapa de calor del área de hardware

Diagnóstico de la evaluación: Es importante gestionar los riesgos que se encuentran presentes en los equipos informáticos, es decir estos dispositivos deben estar en un lugar apropiado, se debe realizar el mantenimiento respectivo, además considerar el uso por parte de los empleados. El resultado de la evaluación indica que existe un nivel de riesgo medio, sin embargo se debe prestar principal atención a los numerales 3, 13, 19, 20,31; ya que podría ocasionar robo o pérdidas económicas para la organización.

Se recomienda que la entidad aplique medidas para mitigar cualquier eventualidad al hardware, es importante considerar los diferentes marcos de referencia en cuanto a controles para implantar una adecuada seguridad de la información. NTS ISO 27001:2013 presenta una lista de objetivos de control y controles de referencia en el anexo A en el apartado A.8 gestión de activos en el cual se recomienda tener un inventario y asignar a un responsable de los aparatos informáticos, también en el apartado A.11.2 donde se describen procedimientos aplicables en cuanto a la ubicación protección, mantenimiento, retiro, seguridad de los equipos.

Así mismo para realizar una evaluación de riesgos, NTS ISO 31000:2018 en su capítulo 6 presenta los procesos a seguir para una adecuada gestión de incidentes de seguridad, ya que el objetivo principal del estándar es la creación de valor en los procesos de la entidad, alineando el marco de trabajo, los principios y el proceso para ser implantada.

También COBIT 5 para riesgos y seguridad de la información provee un marco integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de tecnologías de la información, en su proceso construir, adquirir e implementar por sus siglas en ingles BAI, presenta prácticas de gestión para integrar el hardware e infraestructura tecnológica del software para proteger los recursos.

Tabla 28

Valoración del riesgo del área de software

N°	Actividades	Causa del riesgo	Riesgo	Probabilidad	Impacto	Valoración	Tratamiento
1	Existencia de licencias originales para los software de la entidad	Utilización de software libre o programas craqueados	Pérdida de información	2	1	**2**	**D**
2	Se asigna a una persona determinada para realizar actualizaciones a los sistemas	Se tiene asignada a una persona determinada para darle mantenimiento al software	Pérdida de información	1	2	**2**	**D**
3	Accesos privilegiados a los usuarios en la base de datos contable	Se establecen accesos privilegiados a información confidencial de la organización	Accesos no autorizados	2	2	**4**	**A**
4	Pruebas en los sistemas de información para asegurar la no existencia de errores en el diseño	Falta de procedimientos para detectar la existencia de errores como cálculos aritméticos incorrectos	Manipulación y alteración de la información	3	3	**9**	**B**
5	El usuario del departamento de contabilidad conoce los riesgos existentes en un software contable	Explotación de vulnerabilidades existentes en los sistemas de información contable	Errores humanos	1	3	**3**	**C**

6	Accesos restringidos a software de aplicación contable	Solo el personal encargado de los sistemas puede acceder a las configuraciones del sistema contable	Pérdida de información	1	2	**2**	**A**
7	Aplicación de controles para la instalación de aplicaciones ofimáticas	Es necesario la autorización del administrador para utilizar programas ajenos a la entidad	Pérdida de información	1	1	**1**	**A**
8	Existencia de antivirus en los sistemas de almacenamiento de la información	Existen antivirus para prevenir el daño a los registros contables ante de la presencia de virus	Pérdida de información	1	2	**2**	**D**
9	Controles de seguridad para restringir la instalación o desinstalar programas en el software de la entidad	Ausencia de perfiles de administrador del sistema para la instalación de programas	Accesos no autorizados	2	2	**4**	**B**
10	Actualizaciones al equipo informático por parte de los usuarios de la entidad	Fallos en los procesos para registrar la información de las operaciones de la entidad	Mal funcionamiento del software	1	3	**3**	**B**
11	Protección de software antivirus para el sistema operativo	Existen software antivirus para proteger al sistema operativo de daño o infección de códigos maliciosos	Pérdida de información	2	1	**2**	**A**
12	Instalación de aplicaciones para detectar errores o irregularidades realizadas por los usuarios de los recursos informáticos	Falta de control en la instalación de aplicaciones que podrían afectar los registros contables y por ende en la información financiera	Manipulación o alteración de la información	2	3	**6**	**B**
13	Registro de software desarrollados internamente	Control de deficiencias en los software desarrollados internamente	Errores de diseño del software	1	2	**2**	**D**
14	Establecimiento de jerarquías en el acceso a los módulos del sistema informático contable	Se establecen jerarquías para el acceso a información confidencial de la entidad que puede afectar su reputación	Accesos no autorizados	3	1	**3**	**A**
15	Mantenimiento preventivo al software y equipo informático de la entidad	Daño a los equipos por la falta de mantenimiento preventivo al equipo informático	Disponibilidad de la información	2	2	**4**	**B**
16	Aplicación de mecanismos para el resguardo de la información contable	Falta de controles para el resguardo de la información	Pérdida de información	1	3	**3**	**C**
17	Mantenimiento preventivo con regularidad al sistema operativo	Controles preventivos realizados regularidad para el sistema operativo	Pérdida de información	2	2	**4**	**D**
18	Documentación de las pruebas realizadas a los sistemas informáticos	Ausencia de procedimientos para documentar las pruebas realizadas en los software contables	Errores de diseño del software	2	3	**6**	**B**
19	Existencia de políticas de administración de	La entidad carece de políticas de seguridad de la	Manipulación o alteración de la	1	3	**3**	**B**

	seguridad en la generación de información financiera	información para proteger sus recursos	información				
20	Aplicación de controles para los software libres existentes en la organización, así como la utilización de software piratas	Exposición a daño a los equipos informáticos así como a los software de aplicación para generar información financiera contable	Pérdida de información	2	2	**4**	**C**
21	Comunicación al departamento de informática sobre los fallos o errores en los módulos del software contable	Se debe comunicar al encargado de los sistemas de información sobre los fallos o errores presente en los módulos contables	Fallas técnicas	1	3	**3**	**B**
22	Información sobre cualquier sospecha de incidente de seguridad en los sistemas de información	Comunicación al departamento de informática sobre sospechas de incidentes de seguridad a los sistemas	Accesos no autorizados	2	2	**4**	**B**
23	Se informa a los empleados, sobre los riesgos existentes al acceder a enlaces sospechoso o al descargar archivos adjuntos por remitentes desconocidos a través del correo electrónico	Falta de conocimiento por parte de los usuarios al acceder a enlaces o archivos adjuntos	Fallo en los sistemas	3	3	**9**	**B**
24	Creación de correos empresariales para comunicarse interna y externamente	No hay restricción para la salida de información a correos comerciales de personas ajenas a la entidad	Fuga o Robo de información	2	2	**4**	**C**
25	Aplicación de controles para mitigar riesgos relacionados con la generación de información financiera contable	Se gestionan los riesgos para mitigar las vulnerabilidad en el procesamiento electrónico de datos	Pérdida de información	2	3	**6**	**B**
26	Realización de actualizaciones oportunas por parte del encargado del departamento de tecnología de la información	Se realizan actualizaciones oportunas por parte del encargado de tecnologías de la información	Disponibilidad de la información	2	2	**4**	**D**
27	Existencia de planes o procedimientos para resguardar la información de activos intangibles dados de baja cuando se actualizan o se cambian	Se aplican procedimientos para resguardar la información de activos intangible dados de baja	Disponibilidad de la información	1	2	**2**	**A**
28	Registro de los intentos de acceso no autorizado en los diferentes módulos de la entidad	Se debe controlar el acceso de los usuarios de acuerdo a las funciones de trabajo que desempeñan	Accesos no autorizados	2	3	**6**	**C**
29	Registro de la actividad	Cuando no se realiza	Accesos no		2	**4**	**B**

	diaria al módulo de transacciones para detectar errores u omisiones	monitoreo de los sistemas informáticos, se podría estar generando información errada que puede afectar la toma de decisiones	autorizados	2			
30	Límite de errores en las contraseñas para ingresar al sistema de contabilidad	Controlar los motivos en el cual los usuarios agotan el límite de error en la contraseña para ingresar al sistema	Manipulación o alteración de la información	3	1	**3**	**A**

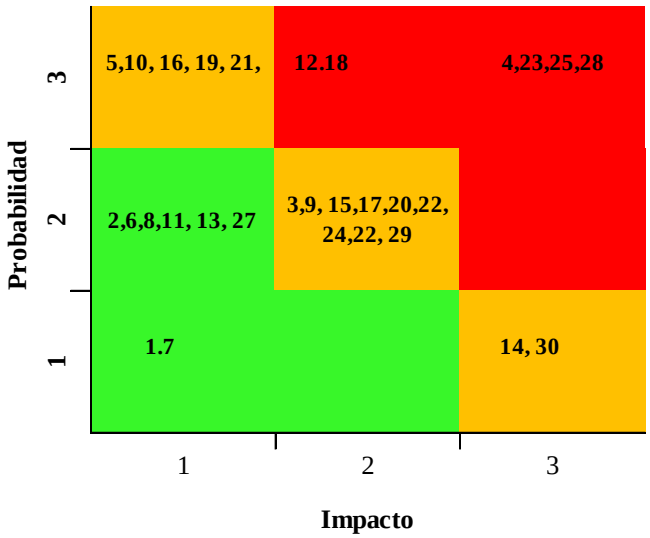


Figura 7: Mapa de calor del software

Diagnóstico de la evaluación: Cuando se evalúan los componentes de los sistemas de información se debe tomar en cuenta que todo sistema debe ser eficiente y confiable que se pueda adaptar a los procesos de la organización, tomando en cuenta que hardware debe cumplir con los requerimientos mínimos del software. A través de la evaluación se pudo identificar que existen riesgos en la pérdida, manipulación o alteración de los registros, fallo en los sistemas, por lo tanto se debe prestar atención en los numerales 1,2, 4, 5,6, para prevenir incidentes de seguridad.

Es importante que la organización gestione la seguridad de los componentes de los sistemas de información, COBIT 5 para la seguridad de la información en su proceso BAI09.05

administración de licencias, en el cual las actividades a seguir es la aplicación de procedimientos para controlar las instalaciones y realizar verificaciones periódicas de la red para detectar software no autorizado, pero se debe tomar en consideración los riesgos que se encuentra inmersos en este componente, por lo tanto COBIT 5 para riesgos, en su Sección 2B presenta escenarios genéricos de incidentes de seguridad, así como ejemplos positivos y negativos para tomar en cuenta en el uso del software.

Sin embargo para evaluar el buen funcionamiento de los sistemas y recursos tecnológicos, la aplicación de NTS ISO 31000:2018 permite conocer y gestionar la seguridad de la información en ambientes tecnológicos, el proceso de evaluación comprende la identificación, análisis y valoración de los riesgos, provenientes de fuentes tangibles o intangibles, que puedan perjudicar la información financiera contable de la organización.

Tabla 29
Valoración del riesgo de la seguridad física

N°	Actividades	Causa del riesgo	Riesgo	Probabilidad	Impacto	Valoración	Tratamiento
1	Protección de los recursos informáticos en los que se genera la información	Las políticas sobre seguridad del equipo informático nos aplican por los usuarios	Pérdidas económicas	2	2	**4**	**C**
2	Seguridad en el voltaje y cableado en las instalaciones eléctricas	Las instalaciones eléctricas no son adecuadas para proteger a los activos de información	Pérdida de información	3	1	**3**	**C**
3	Responsable de resguardar los accesorios en los cuales se almacena los respaldos de información	No se tienen asignado un responsable para el resguardo de los respaldo de información	Pérdida de información	2	2	**4**	**B**

4	Impresiones de información confidencial a personal no autorizado	Los usuarios brindan su contraseña a otras personas ajenas a la entidad, para realizar la impresiones de documentos	Divulgación de información	3	2	**6**	**B**
5	Mantenimiento en la infraestructura de las instalaciones donde se encuentran los activos que almacenan la información	La infraestructura donde se encuentran los activos se le da el respectivo mantenimiento acordado	Pérdidas económicas	1	2	**2**	**D**
6	Cada personal responsable del equipo informático se le asigna su respectivo UPS	Algunos UPS, de los equipos informáticos no están en buen funcionamiento	Pérdida de información	2	2	**4**	**B**
7	Se restringe el acceso de personal ajeno al departamento de contabilidad.	El departamento de contabilidad está ubicado en una oficina cerrada la cual protege los activos de información	Divulgación de información	1	1	**1**	**D**
8	Se tiene una planta generadora de electricidad en caso de interrupciones de energía	Por los costos altos no se cuenta con una planta generadora de energía eléctrica	Pérdida de información	2	3	**6**	**B**
9	Existen contratos vigentes con otras entidades responsables del mantenimiento de aire acondicionado	La organización mantiene vigente los contratos de mantenimiento con el proveedor de los aires acondicionados	Pérdidas económicas	2	1	**2**	**D**
10	Se protegen los sitios donde se encuentran los sistemas informáticos o de almacenamiento, implementando accesos autorizados	No existe un control de acceso en el lugar que se encuentran almacenados los activos de información	Pérdidas económicas	3	2	**6**	**B**
11	Existen en el área de informática materiales que puedan ser inflamables o causar algún daño a los equipos	En el área de informática en ocasiones se tiene material inflamable	Pérdidas económicas	2	2	**4**	**C**
12	Existe clasificación de bienes susceptibles de daño entre los que se encuentren: los activos de información	La entidad no tiene clasificada los bienes que son susceptibles a los daños.	Pérdidas económicas	2	2	**4**	**C**
13	Registro sobre el acceso de personas ajenas al departamento de informática	No se tomen medidas de corrección, para las personas que ingresen sin previa autorización.	Pérdidas económicas	3	1	**3**	**D**

14	La organización cuentan con una política sobre la destrucción de sus equipos informáticos en los que se genera la información	No existen políticas sobre los equipos informáticos cuándo éstos terminen su vida útil.	Divulgación de información	2	3	**6**	**B**
15	El sistema de vigilancia mediante cámaras de seguridad, comprende el área de informática en donde se protege la información	El sistema de vigilancia, comprende el área de informática en donde se protege la información.	Robo de información	2	1	**2**	**A**
16	Los recursos de la infraestructura tecnológica son suficientes para atender las demandas del usuario que generan la información	La infraestructura tecnológica carece de recursos para hacer frente a la demanda del usuario que genera la información.	Pérdidas económicas	2	2	**4**	**D**
17	Señalización adecuada en caso de siniestros	La organización tiene señalizaciones que orienten a los usuarios en caso de un siniestro	Pérdidas económicas	1	1	**1**	**A**
18	Se cuentan con planes de contingencia en caso de terremotos, incendios o inundaciones	No se tienen por escrito los planes de contingencia, se solucionan cuando estos pasan	Pérdidas económicas	2	1	**2**	**C**
19	Seguridad en el acceso donde se encuentran los servidores que protegen los datos	Los servidores se encuentran resguardados en el departamento de informática, bajo llave	Errores humanos	2	1	**2**	**A**
20	Política de difundir formalmente a los usuarios los planes de seguridad en informática para proteger los activos e infraestructura	Falta de comunicación sobre la existencia de planes de seguridad en el área de informática para ser ejecutados por los usuarios	Pérdida de información y económica	2	2	**4**	**D**
21	Revisión de las cámaras de seguridad del personal que entra al departamento de informática y tiene acceso a la información de los servidores	El departamento de informática tienen una puerta de acceso, sin embargo hay usuarios que tienen acceso libre a los servidores	Pérdida de información	3	3	**9**	**B**
22	Existe una evaluación documentada del proceso de servicios proporcionados en el mantenimiento de las infraestructura	El departamento de informática no realiza una bitácora de los mantenimientos realizados a la infraestructura, solo se registran en el departamento de contabilidad	Pérdida de información	3	3	**9**	**B**

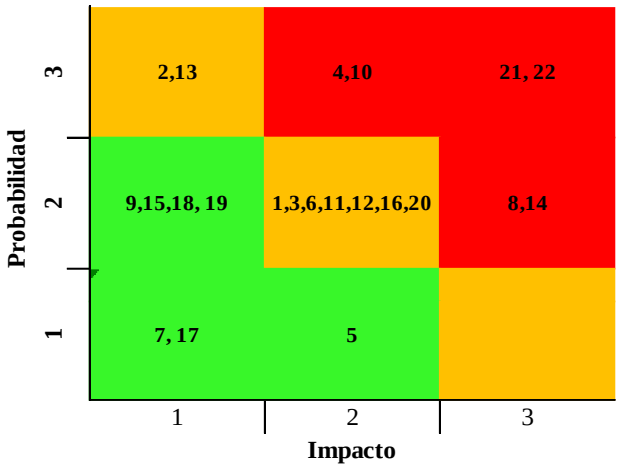


Figura 8: Mapa de calor de seguridad física

Diagnóstico de la evaluación: La seguridad de la información debe estar orientada a la protección de los activos y el resguardo de los datos, para evitar las consecuencias derivadas de amenazas y vulnerabilidades, se evaluó la seguridad física en el cual surgieron las siguientes perdidas económicas y de información, teniendo como resultado un riesgo medio, ya que la entidad esta consiente de proteger el ambiente tanto interno como externo.

Sin embargo, no hay ninguna medida que pueda garantizar un ambiente libre de amenazas o riesgos para la generación e ingresos de los datos por esta razón es que se hace necesarios adoptar y seguir los procedimientos de los marcos de referencia que establecen los parámetros sobre la gestión de la seguridad de la información que permita lograr niveles efectivos de protección basados en la coordinación de los mecanismos existentes en los elementos físicos.

Según la NTS ISO 27001:2013 en el literal A11.1- A11.2.9 detalla los procesos que se deben de seguir para evitar daños en los equipos informáticos ni interferencias en las instalaciones al momento del procesamiento de la información, se deben definir los perímetros de seguridad, controles en las áreas de acceso, seguridad en las oficinas en el equipo informático y mantenimiento en la infraestructura.

COBIT 5 para riesgos en el capítulo 2 sección B comprende los procesos principales en la gestión de riesgos utilizados para implementar un efectivo y eficaz control en las amenazas y vulnerabilidades en los diferentes escenarios de la organización.

Tabla 30

Valoración del riesgo de la seguridad lógica

	Actividades	Causa del riesgo	Riesgo	Probabilidad	Impacto	Valoración	Tratamiento
1	Existencia de políticas de privilegios de contraseñas de los usuarios para el acceso a los módulos contables	Inexistencia de políticas de privilegios de contraseñas de los usuarios	Accesos no autorizados	1	1	**1**	**A**
2	Asignación de contraseñas a cada usuario existente en la entidad que genere información importante para la organización	Asignación de roles para genera la información financiera	Manipulación o alteración de la información	2	2	**4**	**B**
3	Aplicación de antivirus originales y completos para detectar accesos no autorizados	aplicación de controles para detectar accesos no autorizados a los sistemas	Accesos no autorizados	1	2	**2**	**A**
4	Asignación de roles y privilegios para el registro de transacciones al sistema	Asignación y roles para el registro de las transacciones en el sistema	Accesos no autorizados	2	2	**4**	**B**
5	Verificación de los respaldos de registros contables que se realizan periódicamente	Falta de planes de contingencia para resguardar los registros contables	Pérdida de la información	3	3	**9**	**B**
6	Existencia de técnicas criptográficas para resguardar la información financiera contable	No se aplican técnicas criptográficas para asegurar la información	Fuga o Robo de la información	2	3	**6**	**B**
7	Realización de copias de seguridad y resguardadas en un lugares seguros	Ausencia de controles de aplicación para resguardar la información de la organización	Accesos no autorizados	2	3	**6**	**A**
8	Existencia de un listado de accesos a los usuarios que manipulan los equipos informáticos	Existencia de un inventario de activos y asignación de responsables	Accesos no autorizados	2	3	**6**	**B**
9	Realización de copias de respaldo del sistema operativo y los software de aplicación	Se deben realizar copias de respaldo de todos los programas donde se obtiene información	Disponibilidad de la información	1	3	**3**	**A**
10	Controles de identificación y autenticación para el acceso a software contables	Falta de aplicación de controles de identificación y autenticación	Manipulación o alteración de la información	2	3	**6**	**A**
11	Asignación de responsables para los equipos informáticos que procesan información financiera	No se han asignado responsables en el manejo de los recursos informáticos	Errores humanos	1	3	**3**	**D**

12	Existencia de políticas de cierre de sesión seguras para el departamento de contabilidad	Políticas de gestión para los usuarios en cuanto al cierre de sesión al abonar el puesto de trabajo	Accesos no autorizados	2	3	**6**	**B**
13	Limitación y control a los usuarios en cuanto al uso de programas utilitarios	Verificar el buen manejo por parte del usuario de programas diferentes al de contabilidad	Accesos no autorizados	2	2	**4**	**C**
14	El sistema registra en los reportes, el nombre de usuario, fecha, hora para identificar al usuario que genero la información	Los usuarios obtienen la información de acuerdo a las funciones que desempeñan	Robo o fuga de información	1	3	**3**	**A**
15	Se verifica el cumplimiento de política sobre el cambio de contraseñas de acceso con regularidad	Falta de cumplimento de políticas para realizar cambio de contraseña	Accesos no autorizados	3	2	**6**	**B**
16	Otorgamiento de privilegios mínimos a los usuarios del sistema informático contable	Se asignan privilegios de acceso en el sistema informático contables así como en la nube de la entidad.	Accesos no autorizados	1	2	**2**	**A**
17	Existencia de software de aplicación para detectar códigos maliciosos	Infestación por virus	Pérdida de la información	1	3	**3**	**B**
18	aplicación de accesos restringidos en la instalación de actualizaciones al sistema contable	Solo el personal encargado de los equipos informáticos debe realizar las actualizaciones de los programas	Errores humanos	1	2	**2**	**A**
19	Existencia de controles aplicables en la transferencia de información financiera	Se aplican de controles en la salida de la información contable de la entidad+	Robo o fuga de información	1	3	**3**	**D**
20	Controles de estructuración de claves de acceso que incluyan caracteres especiales	No se han establecidos politices para que las contraseñas se estructuren de manera que ninguna persona ajena a la entidad pueda cifrarla	Accesos no autorizados	2	3	**6**	**B**
21	La entidad comunica las políticas existentes de seguridad de la información	Aplicar medidas de seguridad para garantizar que la información es integra	Pérdida de la información	2	3	**6**	**C**
22	Generación de reportes actualizados de los usuarios activos en la entidad	Se Controla que la información de la entidad sea obtenida solo usuarios activos	Robo o fuga de información	3	2	**6**	**B**
23	aplicación de control para la longitud de contraseñas de acceso a los sistemas contables	Las claves de accesos se deben estructurar incluyendo mayúsculas, minúsculas, números, etc.	Accesos no autorizados	2	2	**4**	**C**

24	Procedimientos de control cuando los usuarios realizan cambios de contraseñas	Se verifica que el cambio de contraseña se realice según lo establecido en la política de seguridad	Accesos no autorizados	1	2	**2**	**B**
25	El encargado de tecnologías de información verifica los respaldos de información realizados por los empleados	El encargado de tecnología debe cerciorarse que los empleados realicen el respaldo de información	Disponibilidad de la información	1	3	**3**	**D**
26	Seguimiento de actividades realizadas por los usuarios en los equipos informáticos	Falta de control en las actividades realizadas por los empleados para evitar el riesgo de pérdida de información	Pérdida de la información	2	3	**6**	**B**
27	Realización de reportes de acceso de las actividades realizadas por los usuarios	Se Controlan los accesos de los usuarios con la finalidad de detectar incidentes de seguridad	Accesos no autorizados	3	2	**6**	**A**
28	Registro y control de cambios realizados en las contraseñas de acceso por parte de los usuarios	Se monitorea los cambios realizados por los usuarios para acceder a la información	Accesos no autorizados	1	2	**2**	**D**
29	Elaboración de accesos eliminados de empleados que ya no laboran en la entidad	La entidad controla los accesos de empleados activos de la entidad	Robo o fuga de información	1	2	**2**	**D**
30	Existencia de medios de almacenamiento por fallo en los sistemas	Procedimientos de control que resguarden la información en caso de fallos en el sistema	Pérdida de la información	1	2	**2**	**B**

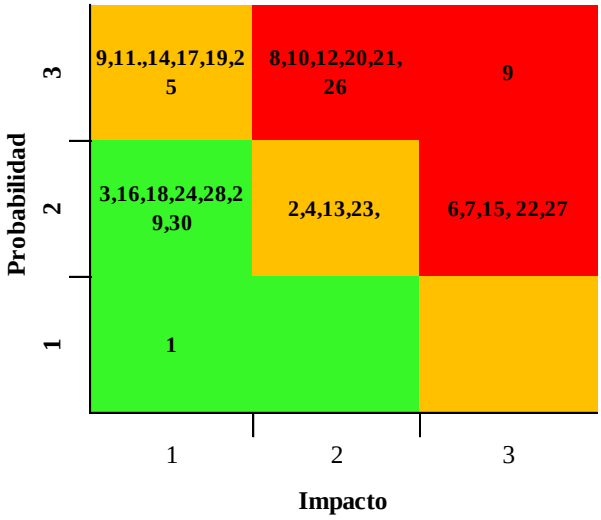


Figura 9: Mapa de calor de seguridad lógica.

Diagnóstico de la evaluación: Comprende la aplicación de procedimientos para resguardar los datos, autorizaciones a personal autorizado, su objetivo principal es restringir el acceso a programar o archivos para prevenir el robo de información confidencial de la entidad.

Con el avance tecnológico las empresas se ven en la necesidad de mecanizar sus procesos, auxiliándose de tecnología para registrar sus operaciones diarias, debido a esto las organizaciones deben aplicar controles o procedimientos de gestión, en la evaluación realizada, presenta un riesgos medio, sin embargo existen amenazas de robo, fuga, pérdida y accesos no autorizados a los módulos de contables que son utilizados para la obtención de información financiera, los numerales a considerar y aplicar medidas son 5, 6, 20, 22, 27.

Una posible solución para gestionar los riesgos presentes en el área de seguridad lógica, es aplicar los controles del anexo A de NTS ISO 27001:2013, ya que el objetivo principal es asegurar la integridad, confidencialidad y disponibilidad de los reportes generados por los sistemas. El apartado A.9 controles de acceso en el cual describe los requerimientos de la organización para limitar a los usuarios y el apartado A.9.3 establece que se debe aplicar una política para restringir el acceso a funcionalidades de los sistemas, inicio de sesión seguro, restricción al código fuente, con la finalidad que solo personal autorizado tenga acceso.

COBIT 5 para riesgos en su capítulo 2B ejemplifica, escenarios negativos de ataques lógicos a los sistemas de información que podría poner en peligro la información confidencial de la organización.

Tabla 31
Valoración del riesgo de Redes

	Actividades	Causa del riesgo	Riesgo	Probabilidad	Impacto	Valoración	Tratamiento
1	Existencia de cuantas temporales para el personal eventual de la entidad	Ausencia de controles para el personal eventual de la entidad	Robo o fuga de la información	3	3	**9**	**B**
2	Asignación de cuentas de usuario por medio de solicitud de autorización de los encargado de cada departamento	La creación de usuarios debe ser solicitada por el jefe de cada departamento	Accesos no autorizados	1	1	**1**	**A**
3	Restricción a los usuarios para poder adicionar, eliminar, leer y modificar la información	Se limitan las opciones de edición según las funciones que desempeñan cada usuario en el registro de la información	Manipulación o alteración de la información	2	2	**4**	**D**
4	Asignación de privilegios de acceso según las funciones desempeñadas en la entidad	No se respetan los privilegios de acceso por parte de los usuarios a los módulos contables	Accesos no autorizados	2	3	**6**	**B**
5	Existencia de controles de seguridad compartida por medio de la red interna	Se restringe el acceso a documentos sensibles compartidos a través de la red	Robo o fuga de información	1	2	**2**	**D**
6	Se deshabilitan los accesos de la red de equipos dados de baja de la entidad	Se desactivan los accesos a la red de equipos dados de baja	Robo o fuga de información	1	3	**3**	**D**
7	Existencia de planes de contingencia en caso de caída del servicio de internet	Falta de planes de contingencia para ayudar a prevenir la recuperación de información valioso para la entidad	Pérdida de información	2	3	**6**	**B**
8	Restricción de nuevos usuarios en la red de la entidad	Se posee una red de invitados para proteger la entidad de cualquier amenaza	Robo o fuga de información	1	2	**2**	**A**
9	Existencia de software para gestionar la red de la entidad	Fallo en la caída de la red interna de la entidad	Disponibilidad de la información	2	2	**4**	**B**
10	Limitación a los usuarios de contabilidad de accesos a sitios web que no posea el protocolo https	El departamento de informática debe aplicar acceso solo a sitios seguros para evitar la infestación de códigos maliciosos	Robo o fuga de información	3	2	**6**	**C**
11	El servicio de internet cuenta con la capacidad necesaria para la trasmisión de información	se cuenta con controles para asegurar que la transmisión de información sea segura	Robo de información	1	2	**2**	**A**
12	Se aplican controles para asegurar una buena configuración de la red	Una mala configuración en la red provocaría fallos en los sistemas	Fallos en los sistemas	2	2	**4**	**C**
13	La red de la entidad se reparte	Para evitar la saturación de la	Disponibilidad	2	3	**6**	**B**

	según las funciones laborales	red debe segregarse según las funciones laborales	de la información				
14	Se verifica el historial de las conexiones realizadas por los usuarios	Se monitorean los accesos a la red de la entidad	Accesos no autorizados	1	2	**2**	**A**
15	La entidad posee una red privada para limitar el acceso a datos financieros	Solo personal autorizado puede tener acceso a información confidencial de la entidad	Accesos no autorizados	1	3	**3**	**D**
16	Existe procedimientos de autenticación para conectar un nuevo equipo a la red	Falta de procedimientos de autenticación para conectar un nuevo dispositivo	Acceso a información de la entidad	3	2	**6**	**B**
17	Se mantiene activo el uso del firewall para proteger el tráfico de información	La entidad mantiene en funcionamiento de los firewall para controlar los accesos a la red	Accesos no autorizados	1	1	**1**	**A**
18	Existe restricción de envió de información a correos electrónicos comerciales ajenos a la entidad	La entidad no restringe el envió de archivos adjuntos o mensajes a correos comerciales ajenos a la entidad	Divulgación de la información	2	2	**4**	**C**
19	Se establece un número determinado de dispositivos que pueden conectarse a la red	Ausencia de medidas de seguridad en cuanto al total de dispositivos conectados en la red	Caídas en los sistemas de información	2	3	**6**	**C**
20	Se comunica oportunamente sobre los manteamientos que se realizan a los sistemas de información	Se comunica oportunamente sobre el mantenimiento que se realizan a los sistemas de información como a los equipos informáticos	Disponibilidad de la información	1	2	**2**	**A**
21	Se informa sobre las caídas en los servidores de la entidad	En ocasiones los usuarios no notifican oportunamente los fallos en los servidores	Caídas en los sistemas de información	2	2	**4**	**B**
22	Restricción de acceso a páginas no autorizadas por la entidad como el envió de información a través de whatsapp web	No se aplican medidas de restricción a páginas web ajenas a la entidad	Infección por virus	3	3	**9**	**B**
23	Se realiza seguimiento de los fallos en la red de la entidad	Se le da seguimiento a los fallos de la red para darle mantenimiento y así evitar fuga de información	Disponibilidad de la información	1	2	**2**	**A**
24	Aplicación de controles de mantenimiento en la red	El departamento de informática aplica controles preventivos dándole mantenimiento a la red	Disponibilidad de la información	2	2	**4**	**D**
25	Se realizan informes donde se registran los helpware solicitados al departamento de informática cuando falla las redes	No se realizan reportes de aviso de fallas en los software	Fallos en los sistemas	2	3	**6**	**C**

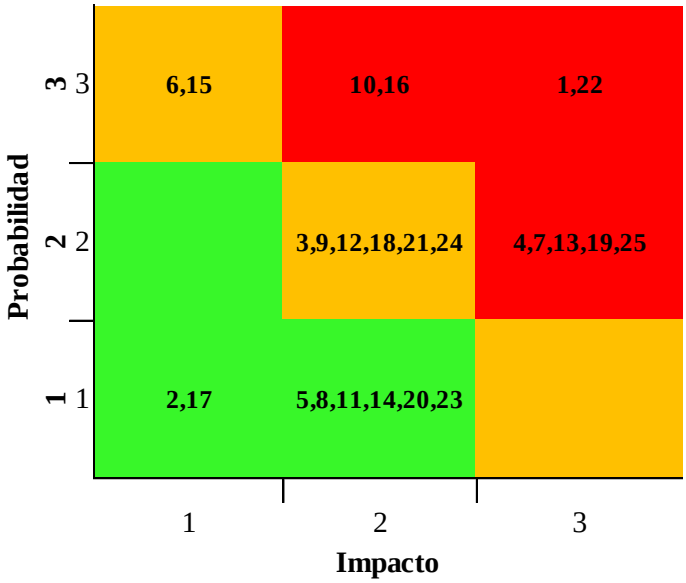


Figura 10: Mapa de calor de Redes.

Diagnóstico de la evaluación: El objetivo de evaluar la red de la organización es monitorear los equipos informáticos conectado entre sí, por medio de dispositivos físicos, además se controla la transferencia de información. El resultado de la evaluación indica que se posee un riesgo medio, es decir existen políticas o procedimientos para asegurar la información financiera contable pero se carece de seguimiento y controles que mitiguen los incidentes de seguridad.

La entidad presenta vulnerabilidades en cuanto al robo o fuga de información, caídas de los sistemas, infecciones por virus, es necesario prestar atención a los numerales 1, 7, 10, 19,22, aplicando medidas de seguridad para controlar o disminuir el riesgo a un valor aceptable para la entidad, para ello la aplicación de la NTS ISO 31000:2018, en el capítulo 6 que trata del proceso de evaluación, ayudará a identificar las principales fuentes de incertidumbre ya sea tangibles o intangibles, y optar por darles el tratamiento adecuado.

En el dominio de entrega, servicio y soporte DSS 05 gestionar los servicios de seguridad de COBIT 5 para la seguridad de la información, se plantea que los datos procesados, almacenados

y transmitidos a usuarios finales debe ser protegido, también que todo el personal debe estar identificado de manera única y tener derechos de accesos según las funciones realizadas en la entidad. Sin embargo, se debe considera la lista de controles del anexo A de NTS ISO 27001:2013 ya que son esenciales para el buen manejo de los recursos tecnológicos de la organización, en el apartado A.13.1 gestión de seguridad en la red manifiesta que la red se debe segmentar los sistema de información y realizar acuerdo de transferencia para la organización así como a entidades externas.

Tabla 32
Valoración del riesgo de Recursos humanos

N°	Actividades	Causa del riesgo	Riesgo	Probabilidad	Impacto	Valoración	Tratamiento
1	Se brinda una inducción al personal reclutado en cuanto al proceso de manejo de la información	La persona que brinda la inducción no tiene la facilidad de transmitir el conocimiento al usuario	Información errónea.	3	2	**6**	**B**
2	Capacitación del personal en marcos normativos sobre seguridad de la información	Falta de una política sobre capacitar al personal	Pérdida de información	2	3	**6**	**B**
3	Seguridad en los recursos informáticos asignados	Personal no entrega el equipo cuando cesa de sus funciones	Pérdida de información y económicas	2	3	**6**	**C**
4	Aplicación sobre procedimientos de seguridad cuando se contrata personal eventual	No se realiza un contrato para la personal eventual y así asignarle el equipo necesario para realizar sus funciones	Divulgación de información	3	3	**9**	**B**
5	El personal contratado ha firmado un acuerdo formal que indique su obligación de cumplir con el requisito de confidencialidad	La empresa no considera necesario la firma de un contrato de confidencialidad	Divulgación de información	2	3	**6**	**B**
6	Se aplican los procedimientos establecidos por la entidad, para que la información sea integra	Los usuarios no siguen los procedimientos tal cual se detallan para cada actividad.	Información errónea.	2	2	**4**	**B**

7	Concientización a los empleados acerca de la importancia en la seguridad de la información	Que las capacitaciones no se den de forma adecuada, y que pierdan su enfoque.	Errores humanos	2	2	**4**	**B**
8	Ingreso de información manual al módulo de contabilidad digitadas en aplicaciones ofimáticas	Existen procedimientos que autorizan a los usuarios a realizar facturación o salidas de inventario con formularios manuales, que regularmente no son ingresados al módulo de contabilidad	Información errónea.	3	3	**9**	**C**
9	Reporte de incidentes generados por los usuarios en el cuido de los recursos informáticos	No queda registrado en una bitácora los incidentes generados por los usuarios en el ingreso de información o mal uso de los recursos informáticos	Pérdida de información	3	2	**6**	**C**
10	La capacitación que se brinda a los usuarios es efectiva para que puedan utilizar eficaz y eficientemente los recursos informáticos	El tiempo asignado para las capacitaciones no se cumpla de acuerdo a lo programado.	Errores humanos	2	2	**4**	**B**
11	El personal cuenta con las actitudes y aptitudes requeridas para hacer uso de la información por medio de las soluciones automatizadas	La utilización del sistema es compleja, no se tiene manuales de apoyo para consultar en los sistemas	Información errónea.	3	3	**9**	**C**
12	El personal no cuenta con el tiempo suficiente para recibir, de manera completa las capacitaciones	Las cargas de trabajo no están balanceadas. No se tiene autorizado un plan de capacitaciones	Información errónea.	2	3	**6**	**C**
13	Se envían correos de recordatorio a los empleados para el caso de los cierres contables	El personal al cual le es difundida la información , no reporte de recibido las notificaciones al encargado de enviarlas	Divulgación de información	1	2	**2**	**B**
14	Se limita el acceso a la información a los usuarios que no pertenezca a su área o departamento	La organización no tiene definido las áreas y las funciones de cada uno de ellos.	Divulgación de información	3	1	**3**	**C**
15	Se capacita a los empleados para el ingreso correcto de datos a los sistemas de información	Las capacitaciones son modalidad en línea , por cual genera deficiencia en el aprendizaje	Errores humanos	3	3	**9**	**B**
16	Los empleados tienen definido sus funciones por escrito	Los manuales no son actualizados de manera continua, pero se les comunica al usuario sus nuevas funciones	Errores humanos	2	1	**2**	**B**

17	Se carecen de controles para bloquear el acceso de correos maliciosos	La información que se almacena en los sistemas computarizados podría ser dañada ya que los códigos maliciosos podrían ser virus informáticos	Pérdida de información	3	3	**9**	**B**
18	Conocimiento de los usuarios sobre los procedimientos que se debe seguir para reportar los incidentes relacionados a la generación de la información	Falta de comunicación de los procedimientos a realizar cuando ocurran incidentes de seguridad en la generación de información financiera	Pérdida de información y tiempo.	3	3	**9**	**B**
19	utilización de diferentes canales de comunicación para informar a los usuarios sobre nuevas directrices de seguridad en el ingreso de los datos	Los canales de comunicación son deficientes.	Errores humanos	2	2	**4**	**C**
20	Comunicación a los usuarios sobre los planes de trabajo	Se les comunica por medio de correo electrónico los planes de trabajo	Pérdida de información y tiempo.	1	2	**2**	**D**
21	Existen manuales de cada módulo sobre el ingreso de información en los sistemas para el personal	Si existen manuales de cada módulo, pero el usuario no los consulta.	Información errónea.	3	3	**9**	**B**
22	Existen parámetros de seguridad en los reportes para evitar que los usuarios puedan manipular los informes que se generan desde los sistemas informáticos	Los usuarios pueden modificar la información con programas como nitro de PDF.	Información errónea.	3	2	**6**	**B**

}}

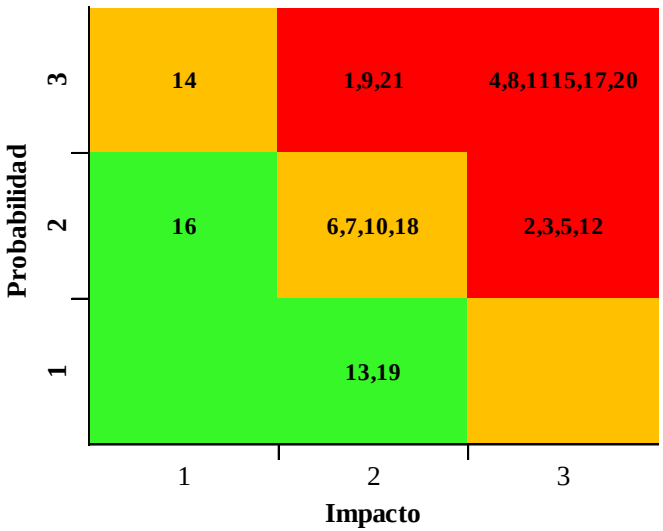


Figura 11: Mapa de riesgo de recursos humanos**. Fuente:**

Diagnóstico de la evaluación: En la evaluación se ha identificado que el área de recursos humanos es en la que se registran más incumplimiento en los procesos, ya que los usuarios son las personas responsables del cuido y resguardo de los activos de información en los que se ingresan datos que son sensibles en el contexto de su actividad y quienes tienen una responsabilidad especial al respecto. Pueden tener derechos especiales de acceso al sistema de información para realizar sus labores diarias.

Según el cuestionario realizado hay que tener énfasis en los numerales 1-5, 8, 9, 11,12 en la que los riesgos asociados son: información errónea, errores humanos, perdida de información, en los marcos de referencia se encuentran los parámetros para mitigar estos riesgos como en la NTS ISO 27001:2013 en su apartado A.6.1.1y 6.1.2 donde establece que todas las responsabilidades de la seguridad de la información deben estar asignadas y segregadas de acuerdo con sus funciones en la organización. En literal A.7.1 al A.7.3.1 que trata de la seguridad de los recursos humanos tienen que existir controles de verificación de los antecedentes del personal a contratar, responsabilidad de la administración para que se aplique la seguridad en la información, las capacitaciones y el conocimiento de cada empleado que pueda beneficiar y agregar valor a los procesos. COBIT 5 procesos catalizadores en el apartado APO07 proporciona un enfoque estructurado para garantizar una óptima gestión de riesgos en el personal contratado,

concientizarlo de la importancia en la optimización de los activos, conocimientos experiencia e iniciativas para la innovación del negocio.

Tabla 33

Valoración del riesgo de Procesamiento electrónico de datos

	Actividades	Causa del riesgo	Riesgo	Probabilidad	Impacto	Valoración	Tratamiento
1	Verificación de los registros ingresados al software contable en relación a la documentación física	Falta de controles de verificación y autorización de datos al ser ingresados en el sistema contable	Manipulación o alteración de la información	1	2	2	A
2	Existencia de políticas y procedimientos aplicados al control interno informático en el procesamiento electrónico de datos	No se aplican controles rígidos en la captura, procesamiento y salida de información	Manipulación o alteración de la información	3	3	9	**B**
3	Se valida la información antes de realizar los registros contables	Se verifica de forma manual que la información este correcto, por ejemplo las facturas, créditos fiscales, etc.-	Errores humanos	1	2	2	**D**
4	Se verifica que la información almacenada en los sistemas contables posea su respectiva documentación física	Se compara que los registros contables sean los mismos de los documentos soportes	Errores humanos	2	1	2	**D**
5	El procesamiento por lotes se verifica para garantizar la seguridad de la información generada por los sistemas	la información de la entidad se actualiza automáticamente después de haber ingresado los datos al sistema de transacciones	Disponibilidad de la información	2	1	2	**D**
6	Existen controles de autenticación en el software contable	Los usuarios deben ingresar su clave de acceso para ingresar a los módulos contables	Integridad de la información	1	3	3	**B**
7	Elaboración de reportes de exactitud en procesamiento de la información	Se debe verificar que los datos en facturas, créditos fiscales sean los mismos que se registran en el libro diario y por ende en el libro mayor	alteración de la información	2	3	6	**B**
8	Aplicación de procedimientos de control para los cambios realizados en los registros ingresados en el sistema de información	No se asigna a personas determinadas para realizar cambios en los registros ingresados en el sistema de información	Manipulación o alteración de la información	3	3	9	**B**

9	Registro de los productos en el inventario de la entidad que se encuentra debidamente autorizados y posea la documentación de respaldo	Ausencia de controles en el ingreso de la información en el módulo de inventario de la entidad	Integridad de la información	2	2	4	**B**
10	Existen procedimientos para asegurar que todas las transacciones han sido registradas, comprendidas y clasificadas en el software contable	En ocasiones no se realiza una verificación exhaustiva para corroborar que la información sea real	Integridad de la información	2	2	4	**C**
11	Los equipos informáticos tienen instalados software para la gestión de riesgos	Falta de un software de aplicación para gestionar riesgos tecnológicos	Disponibilidad de la información	2	3	6	**B**
12	El sistema de información permite guardar asientos contables que no se encuentren cuadrados en sus créditos y débitos	El sistema permite guardar asientos descuadrados pero sin embargo no se puede realizar la mayorización fecha información	Integridad de la información	1	3	3	**C**
13	¿Existen controles para verificar que la información que se migra de los módulos se hace adecuadamente?	Los encargados del departamento de informática no poseen controles para verificar la integridad de la migración de datos	Integridad de la información	2	2	4	**B**
14	¿Se aplican controles para estimar el impacto de los riesgos tecnológicos relacionados a la entrada, procesamiento y salida de datos de los sistemas?	Ausencia de controles en el ingreso de la información en el módulo de inventario de la entidad	Pérdida de información	3	3	9	**D**
15	¿El software contable genera informes de excepciones?	Se generan informes de excepciones para controlar los errores	Manipulación o alteración de la información	2	1	2	**D**
16	¿Se verifica que en los retaceos originados por las importaciones sean incluidos de forma correcta en el módulo respectivo?	El departamento de contabilidad verifica de forma oportuna los desembolsos ocasionados en los equipos médicos de la entidad	Integridad de la información	2	2	4	**D**
17	¿El departamento de contabilidad asigna privilegios de acceso a los usuarios para eliminar, leer, adicionar y modificar registros almacenados en el software contable?	Se asignas privilegios de acceso pero no se cumple al cien por ciento, es decir en ocasiones los propios empleados realizan acciones de edición en la información de la entidad	Manipulación de la información	1	2	2	**D**
18	Aplicación de controles de seguridad en el almacenamiento de la información	Solo personal autorizado puede acceder a información financiera de la entidad	Robo o fuga de Información	2	2	4	**B**

19	¿Se realizan recalculó manuales para asegurar que el software contable procese de manera correcta los datos numéricos?	Los usuarios del departamento de contabilidad verifican que la información generada por los sistemas es correcta	Integridad de la información	3	1	3	**A**
20	El modulo e facturación no permite facturar productos que no hay en existencia	Cuando no hay existencia cierto producto el sistema no permite realizar la facturación respectiva	Manipulación o alteración de la Información	1	2	2	**A**
21	Se realizan conteos físicos para corroborar la información generado en el módulo de inventarios	Verificar de los datos generados en el sistema con el conteo físico	Manipulación o alteración de la información	2	2	4	**D**
22	¿Los datos registrados en el software poseen fecha y hora en la cual fueron ingresados para su procesamiento?	El sistema de información registra la fecha, hora y nombre de usuario cuando genera reportes de información de la entidad	Manipulación o alteración de la información	2	1	2	**A**
23	Aplicación de restricción de cambios no autorizados en los software contable	Solo personas especificas pueden realizar cambios o actualizaciones en el software contable	Accesos no autorizados	1	3	3	**D**
24	¿Se restringe el acceso a los sistemas de información de contabilidad en sus diferentes módulos a través de contraseñas?	Se debe asignar una contraseña estructurada para cada usuario que ingrese al sistema contable	Accesos no autorizados	3	1	3	**B**
25	¿Existen controles de salidas de las transacciones registradas en los sistemas?	La entidad no posee controles robustos en cuanto a la salida o generación de reporte de la entidad	Robo o Fuga de información	1	3	3	**C**
26	¿Se verifica que las órdenes de pedido, de salida, créditos fiscales se encuentren autorizadas y cumplan con los requisitos legales correspondientes?	Para ingresas información a los diferentes módulos contables se debe verificar que los datos se encuentren debidamente autorizados	Manipulación o alteración de la información	3	1	3	**C**
27	¿Se aplican controles de autorización para la salida de información financiera de la entidad?	El departamento de contabilidad carece de controles rígidos en cuanto a la salida de información financiera contable	Robo o Fuga de la información	3	3	9	**C**
28	El sistema guarda los intentos de cambio en los registros contables realizados por los usuarios	Se carece de controles para verificar los cambios realizados en los registros del sistema de información	Manipulación o alteración de la información	2	3	6	**B**
29	Existen procedimientos para validar la información de cálculos aritméticos de los registros contables	Se verifica que los cálculos realizados por los sistemas se han correctos	Integridad de la información	1	2	2	**A**

30	El sistema se puede configurar para evitar la duplicidad de información y validar datos	Se controla que el sistema no genere información duplicada y la validación de información errónea	Integridad de la información	2	2	4	**D**
31	El software contable tiene activo el método de digito auto verificador para evitar la duplicidad de la información	El sistema está estructurado para que los campos registros solo fechas, números o la combinación de ambos	Duplicidad de la información	1	2	2	**A**
32	¿Existe un software que detecte e inicie una acción correctiva sobre los errores de la información en el procesamiento?	La entidad no posee un software que permita detectar los errores en el procesamiento de la información	Integridad de la información	2	3	6	**B**
33	¿Existe una metodología para autorizar, priorizar y rastrear los requerimientos de cambios en los sistemas?	No existe procedimientos para autorizar, priorizar o rastrear los cambios de requerimientos del sistema	Integridad de la información	3	3	9	**B**
34	Aplicación de planes de capacitación para el uso de los sistemas de información contable	Erros el uso de los equipos informáticos, con lleva al registro de información errónea	Errores humanos	2	2	4	**B**
35	¿El software contable realiza búsqueda de registros duplicados?	No existe controles para detectar la duplicación de registros	Duplicidad de la información	2	3	6	**C**
36	¿Se utiliza la firma electrónica para la transmisión de datos que aseguren el origen y destino de la información ¿	Para realizar pedidos de equipos médicos, debe contener la firma respectiva como medio de autorización	Integridad de la información	2	1	2	**A**
37	¿El sistema de información permite la existencia de campos vacíos o espacios en blanco?	El software contable no limita que algunos cambios queden vacíos al momento de ingresar información	Integridad de la información	2	3	6	**B**
38	Se aplican controles antes de registrar las transacciones para evitar la existencia de errores	El departamento de contabilidad no posee controles para verificar la información antes de ser procesada	Integridad de la información	3	3	9	**B**
39	El departamento de contabilidad comunica los fallos en el software contable que pueden perjudicar el ingreso de la información	En ocasiones por la saturación de la red el sistema no permite ingresar la información de manera oportuna	Fallas técnicas	2	2	4	**B**
40	El sistema controla las redundancias de información	Los módulos notifican cuando existen datos o registros repetidos	Integridad de la información	1	3	3	**D**
41	Se aplican controles al momentos de trasladar los asientos diarios al libro mayor del software contable	Cuando se migra la información a la nube no se cerciora que exista información duplicada	Pérdida de información	2	3	6	**B**

42	Se informa a los empleados la existencia de planes de contingencia en caso de fallos en los sistemas	Cuando los sistemas presenta fallas los usuarios notifican al área de tecnologías para realizar los procedimientos adecuados	Disponibilidad de la información	1	3	3	**A**
43	Se comunica a los empleados que no se deben divulgar sus claves de acceso a los sistemas	El departamento de informática concientiza al personal sobre los riesgos que inciden al divulgar las contraseñas de acceso	Divulgación de la información	1	2	2	**A**
44	¿Existe una adecuada segregación de funciones en cuanto a la autorización y verificación de los registros?	Existe segregación de funciones pero no se poseen controles para el acceso del personal eventual	Manipulación o alteración de la información	2	2	4	**C**
45	Los reportes generados por el sistema está conforme a los requerimientos de la normativa vigente	El sistema de la entidad en el caso de los libros de IVA, se realizan por medio Microsoft Excel, ya que los campos no son adecuados a la normativa legal	Manipulación o alteración de la información	2	2	4	**B**
46	¿Existe controles en el ingreso de la información así como las salidas de los datos?	Se controla la salida de la información mediante las impresoras ya que guarda en su memoria los archivos que de información sensible	Manipulación o alteración de la información	3	1	3	**B**
47	Se le da seguimiento a los errores reportados o encontrados en el procesamiento de la información	Se lleva una bitácora de los errores reportados en los sistemas para realizar las modificaciones respectivas	Pérdida de información	1	3	3	**C**
48	Se verifica la documentación antes de ser ingresada al módulo de compras	Antes de ingresar la documentación se verifica que los datos sean del periodo correspondiente	Integridad de la información	1	2	2	**D**
49	Elaboración de seguimiento sobre los principales errores cometidos en los módulos contables	Se elabora una bitácora de los principales errores cometidos por los usuarios en los módulos contables	Integridad de la información	2	3	6	**B**
50	Utilización de software de recuperación en caso de borrar información de manera accidental	No se posee software de recuperación de información	Errores humanos	3	3	9	**C**
51	Se lleva un registro del historial de los cambios realizados por los usuarios en los registros contables	Se realiza un reporte del historial de las actividades de los empleados	Accesos no autorizados	2	2	4	**A**
52	Se controla la salida de información a través de las impresoras de la entidad	Se registra y controla los documentos impresos por parte de los usuarios	Robo o fuga de información	1	2	2	**A**

53	Los reportes realizados en el software contable registra, fecha, hora, usuario, para controlar quien genero la información	Los sistemas informáticos registras la fecha, hora, nombre de usuario, cuando se realiza el ingreso de información	Accesos no autorizados	2	2	4	**B**
54	Existen controles en cuanto a la migración de información financiera	Se verifica que la información trasladada a la nube sea completa	Integridad de la información	1	2	2	**D**

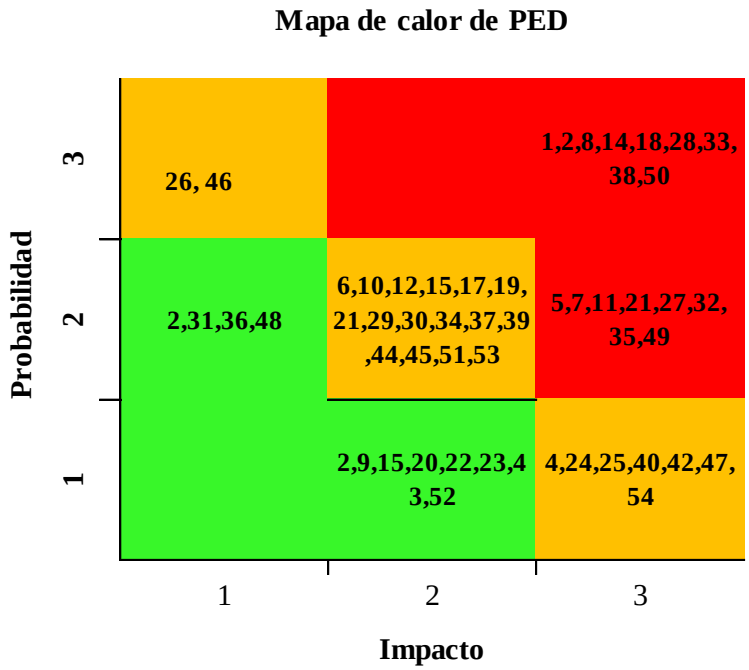


Figura 12: Mapa de calor del procesamiento electrónico de datos.

Diagnóstico de la evaluación: Es importante tomar en consideración los riesgos que se encuentran presentes en la captura, procesamiento, almacenamiento y salida de la información, ya que el resultado de los datos contables sirven para generar la información financiera y es útil para la toma de decisiones, según el resultado de la evaluación se debe prestar atención a los numerales 1,8, 18 y 28, en el cual los riesgos presentes son relacionados a los errores humanos y a la alteración o manipulación de los registros por parte de los usuarios, cuando no se aplican controles rígidos para preservar la confidencialidad, integridad y disponibilidad.

Se recomienda a la entidad considerar los diferentes marcos de referencia aplicables a las tecnologías de la información como lo es NTS ISO 27001:2013, en la cual contiene una lista de controles en el anexo A para implementar medidas de seguridad en los sistemas de información y así gestionar los riesgos. También NTS ISO 31000:2018 contiene directrices aplicables para evaluar e identificar las principales amenazas o vulnerabilidades provenientes de fuentes tangibles e intangibles.

CONCLUSIONES

Al finalizar el trabajo de investigación realizado para las empresas que comercializan equipos médicos; así mismo a los gerentes o encargados de tecnología de la información y contadores públicos autorizados sobre la evaluación de riesgos informáticos en la generación de la información financiera contable, se logró obtener información que ha permitido determinar las siguientes conclusiones.

- Se determinó en la investigación que no todos los encargados del área de informática y contadores públicos tienen los conocimientos ni la experiencia sobre los marcos normativos y técnicos esto debido a la falta de capacitación en el área de tecnología.
- La participación de la gerencia en la implementación y mejora de los controles en el procesamiento electrónico de datos contribuye a que el personal desarrolle de mejor manera las actividades asignadas, sin embargo en la investigación realizada se determinó que la gerencia no cuenta con un modelo de evaluación de riesgos informáticos en la captura, almacenamiento, procesamiento y salida de la información que garantice la integridad y confidencialidad en la generación de la información financiera contable.
- Las directrices sobre la seguridad de la información están orientadas a proteger los activos en los que se genera la información financiera contable, por lo tanto, a evitar que las amenazas a estas categorías puedan afectar los objetivos de las organizaciones. Sin embargo, no hay ninguna medida que pueda garantizar un ambiente libre de amenazas o vulnerabilidades en los riesgos informáticos. Por esta razón es que se hace necesario adoptar modelos adecuados de gestión de la seguridad de la información que permitan logar niveles efectivos de protección, basados en la relación coordinada de los diferentes

mecanismos, especialmente, en hardware, software, políticas y procedimientos, recursos humanos que administra, opera y utiliza los activos de información.

- La debilidad que existe en la definición de políticas en los recursos de información sobre el tiempo para realizar el cambio de contraseñas, esto debido a que los encargados del área de informática no tiene tiempo para efectuar los cambios, ya que son ellos los responsables de ejecutarlos, la falta de conocimiento sobre las buenas prácticas y desconocimientos de otros marcos de referencia, no le dan a estos recursos la importancia que tiene para que la información tenga altos los parámetros de seguridad, para el ingreso de usuarios a los activos en los cuales se respalda y guarda la información sensible de la organización.
- Más que un problema de tecnología, la seguridad en la transmisión de la información por la red se debe a la falta de cultura de las organizaciones y de los usuarios que la integran. El eslabón más débil de esta cadena de la constituye el factor humano y no el tecnológico, por lo cual se destaca la importancia de tener una cultura de seguridad en la generación de la información
- Las empresas que comercializan equipos médicos cuentan con sistemas integrados tanto a la medida como ERP, ya que es una herramienta importante para la automatización de procesos, que contribuye a la reducción de tiempos con la integración de los módulos, sin embargo, no todos están adquiridos por la entidad, estableciendo así una deficiencia en la en la generación de la información financiera contable.

RECOMENDACIONES

Partiendo de las conclusiones sobre el trabajo realizado, se enumeran las recomendaciones que pueden ayudar a la solución de la problemática identificada, las cuales se mencionan a continuación:

- Se recomienda a la gerencia de las empresas que comercializan equipos médicos implementar planes de capacitación en el área de tecnologías de la información, así como en modelos de gestión de riesgos tecnológicos como COBIT 5, ITIL e ISO 31000:2018 que establecen directrices para una adecuada creación y protección de valor en todos los niveles de la organización, garantizando una administración adecuada de los eventos en las operaciones de cada departamento.
- Para evitar que la dirección implemente controles en el procesamiento electrónico de datos sin una adecuada gestión de sus activos de información, se recomienda implementar una evaluación de riesgos informáticos basado en la NTS ISO 31000:2018, que se adecue a las necesidades de las empresas de comercializan equipos médicos, el cual contenga los procedimientos necesarios y adecuados para la oportuna evaluación, identificación, análisis, valoración y tratamiento de eventualidades en las operaciones financieras contables a fin de asegurar su integridad y confidencialidad.
- A las entidades del sector en estudio se les recomienda que identifiquen en forma clara y documental sus activos de información, especialmente los relacionados a datos financieros contables, estableciendo clasificaciones en función de su importancia para así minimizar los riesgos y establecer controles adecuados, idóneos y eficaces.
- A los encargados en el área de informática mantenerse en constante capacitación en temas relacionados a la gestión de riesgos, que le permita optimizar sus conocimientos

para continuar apoyando a la administración en la labor de mitigar los riesgos existentes y que pueden surgir con el tiempo. De este modo, contribuir al cumplimiento de los objetivos estratégicos y metas planteadas por la organización.

- A la gerencia se recomienda capacitar dos veces al año, a los usuarios creando una conciencia sobre la seguridad de los datos y cuánto valen estos para la entidad. Estableciendo políticas sobre los controles de autenticación de la información en los cuales se les dé seguimiento para la protección de estos.
- Los encargados del área de tecnología de la información capacitar a los usuarios involucrados en la captura, procesamiento y salida de la información del sistema contable, acerca de los aspectos importantes para las evaluaciones, en el contexto tecnológico y que conozcan su importancia.

BIBLIOGRAFÍA

Baca Urbina, G. (2016). *Introduccion a la seguridad informatica.* Mexico: Grupo Editorial Patria.

Cohen Karen, D. (2009). *Tecnologías de información en los negocios (5a. ed.).* McGRaw-Hill Interamericana.

Asamblea Legislativa de El Salvador. (31/07/1970), Código de Comercio. Obtenido de Código de Comercio:

https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_072920482_archivo_documento_legislativo.pdf

Asamblea Legislativa de El Salvador, (22/12/2000), *Código Tributario.* Obtenido de Código Tributario: https://www.asamblea.gob.sv/sites/default/files/documents/decretos/4600CE01-0E0D-4DBA-AB80-84EADBFA13FE.pdf

Asamblea Legislativa de El Salvado, (11/12/2001), *Reglamento de aplicación al Código Tributario.* Obtenido de Reglamento de aplicación al Código Tributario: http://www.transparenciafiscal.gob.sv/downloads/pdf/DC5854_Reglamento%20aplicacion%20Codigo%20Tributario.pdf

Consejo de Ministros de Integración Económica, (25/08/2008), *Código Aduanero Uniforme Centroamericano Arancelario.* Obtenido de Código Aduanero Uniforme Centroamericano Arancelario:http://www.transparenciafiscal.gob.sv/downloads/pdf/DC5085_2_Codigo_Aduanero_Uniforme_Centroamericano_(CAUCA).pdf

Consejo de Ministros de Integración Económica, (25/08/2008), *Reglamento del Código Aduanero Uniforme Centroamericano Arancelario.* Obtenido de Reglamento del Código Aduanero Uniforme Centroamericano Arancelario: http://www.transparenciafiscal.gob.sv/downloads/pdf/DC5137_1_Reglamento_del_Codigo_Aduanero_Uniforme_Centroamericano.pdf

Asamblea Legislativa de El Salvador, (02/03/2012), *Ley de Medicamentos.* Obtenido de Ley de Medicamentos: https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_073104135_archivo_documento_legislativo.pdfCondori Rivera, M. D. (2017). Modelización de un proceso de clasificación de activos de información mediante la implementación de una solución informática para una entidad financiera. En M. Maggiore. Buenos Aires, Argentina: Universidad de Buenos Aires. Facultad de Ciencias Económicas. Obtenido de http://bibliotecadigital.econ.uba.ar/?c=tpos&a=d&d=1502-1101_CondoriRiveraMD

elsalvador.com. (1 de Diciembre de 2017). Obtenido de Troll Center en El Salvador: http://www.elsalvador.com/noticias/nacional/425027/absuelven-de-tres-delitos-a-acusados-de-caso-troll-center/

Freitas, D. (2009). Analisis y evaluación de riesgos de la información. Casa de estudio Universidad Simon Bolivar.

Gomez Vieites, A. (2011). *Enciclopedia de la Seguridad Informatica.* Mexico: Alfaomega Ra-Ma.

ISACA. (2012). *COBIT 5 para Seguridad de la Infomacion.* Chicago: ISACA.

ISACA. (2013). *COBIT 5 para Riesgos.* Chicago: ISACA.

ISO, N. (31000:2018). *Gestión del riesgo. Directrices.*

Knight, J. A. (2017). *Azzets : definición de sistema de gestión de activos de información.* Obtenido de http://bibliotecadigital.econ.uba.ar/?c=tpos&a=d&d=1502-0821_KnightJA

Perla D. Lezanski, A. O. (2016). *Sistemas de información contable II.* Editorial Maipue.

Piattini, M. G. (2011). Auditoria informatica un enfoque practico. En M. G. Piattini. Alfaomega Grupo Editor, S.A. de C.V. .

Publishing, J. A. (2011). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. En J. A. Publishing. Obtenido de https://qanewsblog.com/2013/04/16/evaluacion-de-la-seguridad-de-los-sistemas-informaticos-politicas-estandares-y-analisis-de-riesgos/

Reyes, D. N. (2017). Control Interno Informático Sistemas Contables Computarizados. *Control Interno Informático Sistemas Contables Computarizados*.

Roca, C. M. (2016). *Contabilidad financiera para contaduría y administración.* Barranquilla, Colombia: Universidad del norte.

Soy i Aumatelli, C. (2013). *Auditoría de la información: identificar y explotar la información en las organizaciones.* Barcelona: Editorial UOC.

ANEXOS

Anexo No. 1

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

CUESTIONARIO SOBRE EL TEMA DE INVESTIGACIÓN DENOMINADO "EVALUACIÓN DE RIESGOS RELACIONADOS A LA GENERACIÓN DE INFORMACIÓN FINANCIERA CONTABLE EN LAS EMPRESAS QUE COMERCIALIZAN EQUIPO MÉDICO EN EL ÁREA METROPOLITANA DE SAN SALVADOR"

DIRIGIDO A: Los encargados o administradores del departamento de tecnologías de información o departamento informático de las empresas que comercializan equipos médicos del área metropolitana de San Salvador.

OBJETIVO: Obtener información que facilite la elaboración de un modelo de evaluación de riesgos informáticos relacionados a la generación de información financiera contable en las empresas que brindan servicios de salud, para facilitar la identificación de las vulnerabilidades y amenazas a las que se encuentran expuestas e implementar los controles adecuados para minimizar los riesgos.

INDICACIONES: Por favor marque con una "x" la(s) respuesta(s) que usted considere más convenientes.

1. **¿Cuál es su grado académico?**

a) Técnico ☐

b) Licenciado/a ☐

c) Ingeniero/a ☐

d) Máster ☐

e) Otros ☐

Especifique: _____

2. **De acuerdo con la pregunta anterior ¿Cuántos años de experiencia tiene en su campo profesional?**

   a) Uno a menos de tres años ☐

   b) Tres a menos de seis años ☐

   c) Seis a menos de diez años ☐

   d) Más de diez años ☐

3. **¿Tiene conocimiento sobre los riesgos informáticos y su incidencia relacionados con el procesamiento electrónico de datos en la generación de información financiera contable?**

   a) SI ☐ b) NO ☐

4. **¿Se capacita al personal encargado de los sistemas de información?**

   a) SI ☐ b) NO ☐

5. **¿En qué áreas se capacita a los encargados o administradores de los sistemas de información?**

   a) Gestión de riesgos informáticos ☐

   b) Auditoría de sistemas ☐

   c) Modelo de gestión de TI (COBIT 5, ISO, ITIL, otros) ☐

   d) Ninguno de los anteriores ☐

6. **¿Conoce usted qué son los activos de información?**

   a) SI ☐ b) NO ☐

7. **¿La entidad lleva un reporte en el cual se detallen los activos información?**

   a) SI ☐ b) NO ☐

8. **¿La entidad posee una clasificación de su información de acuerdo con el valor que esta representa?**

   a) SI ☐ b) NO ☐

9. **Si su respuesta a la pregunta anterior fue si ¿Con que frecuencia se realiza una evaluación de controles preventivos en el área de tecnologías de la información?**

   a) Semanal ☐

   b) Mensual ☐

c) Anual ☐

d) Nunca ☐

10. ¿Existe en la entidad un modelo de evaluación de riesgos informáticos en la captura, almacenamiento, procesamiento y salida de información, para garantizar la integridad y confidencialidad en la generación de información financiera contable?

a) SI ☐ b) NO ☐

11. Según su experiencia ¿Sería útil para la entidad una evaluación de riesgos informáticos relacionados en la generación de información financiera contable, para mejorar su integridad y confidencialidad?

a) SI ☐ b) NO ☐

12. ¿Existe una política de cambio de contraseña para el acceso a los ordenadores de la entidad?

a) SI ☐ b) NO ☐

13. ¿Cuál es la periodicidad en que se realizan cambios de las contraseñas para el acceso a los sistemas?

a) Mensualmente ☐

b) Trimestralmente ☐

c) Semestralmente ☐

d) Anualmente ☐

e) Nunca ☐

14. ¿Quiénes están autorizados por la entidad para realizar un cambio de contraseña?

a) Gerente General ☐

b) Encargado de TI ☐

c) Otros ☐

Especifique_____

15. ¿Qué programa se utiliza para la generación de la información financiera contable?

a) Software a la medida ☐

b) Software ERP ☐

c) Otros ☐

16. **¿Cuáles de los siguientes módulos tiene integrados el sistema utilizado por la entidad?**

    a) Ventas ☐

    b) Inventarios ☐

    c) Activos Fijos ☐

    d) Presupuesto ☐

    e) Bancos ☐

    f) Todos los anteriores ☐

17. **¿El personal de la empresa tiene los accesos restringidos a la información de acuerdo con la segregación de sus funciones?**

    a) SI ☐ b) NO ☐

18. **¿Qué tipo de controles internos utiliza para efectuar la autenticación de los usuarios al sistema?**

    a) Encriptación ☐

    b) Listas de control de acceso ☐

    c) Contraseñas ☐

    d) Ninguno ☐

19. **¿Existen manuales o instructivos escritos para el personal en los que se describa el manejo de los datos en los sistemas de información?**

    a) SI ☐ b) NO ☐

20. **¿En caso de fallo en los sistemas informáticos y servicios conexos se aplica planes de contingencia para resguardar los recursos informáticos?**

    a) SI ☐ b) NO ☐

Anexo No. 2

TABULACIÓN Y ANALISIS DE RESULTADOS

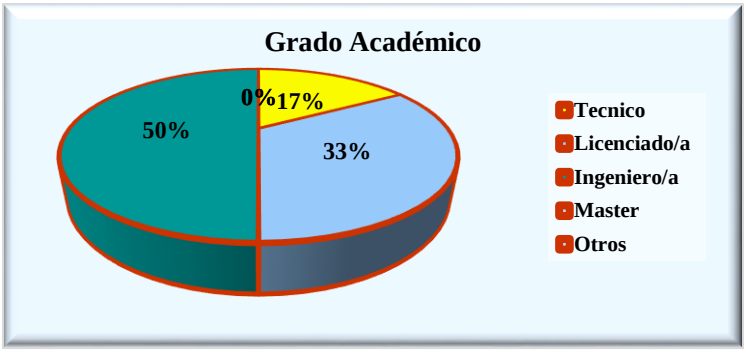
Pregunta 1 ¿Cuál es su grado académico?

Objetivo: Investigar el grado académico que poseen los encargados y/o administradores del área de informática, ayudará a conocer la importancia que les brinda a los diferentes marcos técnicos relacionados a la gestión de riesgos.

Cuadro N° 1
Título: Grado Académico

Grado académico	Frecuencia absoluta	Frecuencia relativa
Técnico	2	17%
Licenciado/a	4	33%
Ingeniero/a	6	50%
Master	0	0%
Otros	0	0%
Total	**12**	**100%**

Grafico No.1



Análisis e interpretación: De la población encuestada el 50% de los encargados del área de informática son ingenieros, por lo tanto, conocen y se apoyan en los marcos normativos y técnicos para identificar los parámetros en los sistemas y reducir el riesgo al momento que se genere la información. El 33% son Licenciados y el otro 17% son técnicos cubriendo de manera más general los riesgos.

Pregunta 2 De acuerdo con la pregunta anterior ¿Cuántos años de experiencia tiene en su campo profesional?

Objetivo: Evaluar el nivel de experiencia que tiene el personal encargado de los recursos informáticos, que permita comprender el buen manejo de los sistemas de información.

Cuadro N° 2
Título: Años de experiencia

Años de experiencia	Frecuencia absoluta	Frecuencia relativa
Uno a menos de tres años	2	17%
Tres a menos de seis años	2	17%
Seis a menos de diez años	2	17%
Más de diez años	6	50%
Total	**12**	**100%**

Gráfico No. 2

Análisis e interpretación: La experiencia laboral es importante para el buen funcionamiento de las empresas, el tiempo les proporciona la experiencia necesaria para identificar cuáles son las áreas críticas en las que tienen que prestar atención para lograr los objetivos de la administración. De la población encuestada el 50% tiene más de 10 años de experiencia en el manejo de los recursos informáticos, el 17% de seis a menos de un año.

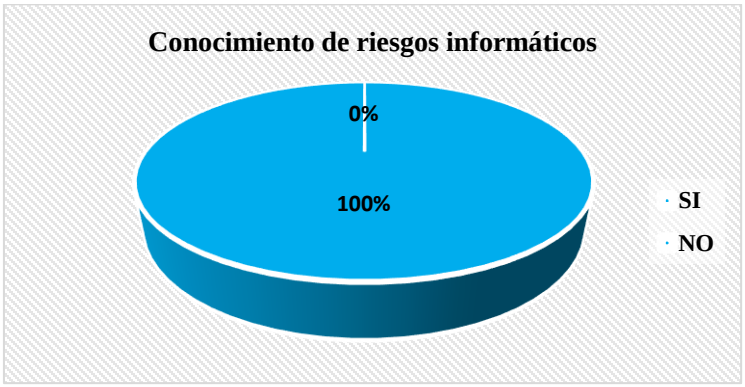
Pegunta 3 ¿Tiene conocimiento sobre los riesgos informáticos relacionados con el procesamiento electrónico de datos en la generación de información financiera contable?

Objetivo: Comprender si el personal informático conoce sobre los riesgos y su incidencia asociados con la captura, procesamiento y salida de información que podrían poner en peligro los objetivos de la entidad.

Cuadro N° 3
Título: Conocimiento de riesgos informáticos

Conocimiento de los riesgos	Frecuencia absoluta	Frecuencia relativa
SI	12	100%
NO	0	0%
Total	**12**	**100%**

Gráfico No. 3



Análisis e interpretación: El 100% de la población encuestada conoce los riesgos en el procesamiento electrónico de datos y considera que se está en una era de tecnología y sistematización, en donde la generación de la información financiera contable se realiza por medios electrónicos, en los cuales se llevan los registros y transacciones diarias que son desarrolladas por los sistemas contables en los que radica la utilización y seguridad que se brinda desde la captura, procesamiento y salida de esta, para contribuir al cumplimiento de los objetivos de la dirección.

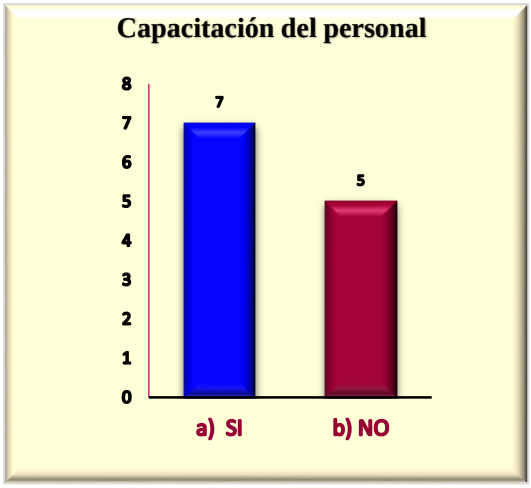
Pregunta 4 ¿Se capacita al personal encargado de los sistemas de información?

Objetivo: Determinar la importancia que tiene la entidad al capacitar a los empleados para enfrentar los nuevos avances tecnológicos.

Cuadro N° 4
Título: Capacitación del personal

Capacitación del personal	Frecuencia absoluta	Frecuencia relativa
Si	7	58%
No	5	42%
Total	**12**	**100%**

Gráfico No. 4



Análisis e interpretación: El 42% de la población encuestadas respondieron que el personal del departamento de informática no se capacita. Debido a que las empresas no le dan la importancia necesaria a los riesgos relacionados con la integridad y confidencialidad de la información; ya que a medida que la tecnología avanza nace la importancia de la participación de los encargados del área de tecnología de la información en la gestión estratégica de las operaciones.

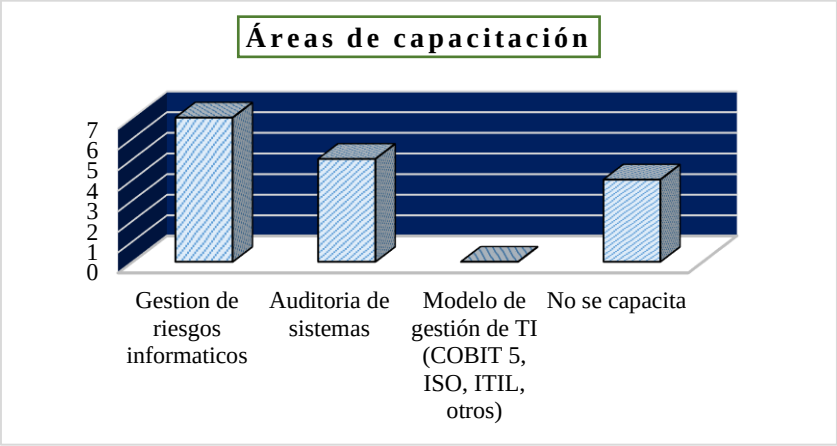
Pregunta 5 ¿En qué áreas se capacita a los encargados o administradores de los sistemas de información?

Objetivo: Conocer cuáles son las principales áreas en las que se capacita al personal de informática a fin de ser competentes en el desarrollo de sus actividades.

Cuadro N° 5
Título: Áreas de capacitación

Áreas de capacitación	Frecuencia absoluta	Frecuencia relativa
Gestión de riesgos informáticos	7	58%
Auditoria de sistemas	5	42%
Modelo de gestión de TI (COBIT 5, ISO, ITIL, otros)	0	0%
No se capacita	4	33%

Gráfico No. 5



Análisis e interpretación: El resultado de esta pregunta relacionada a las principales áreas en las que se capacita el personal encargado del área tecnologías de información se puede mencionar que el 58% se capacita en la gestión de riesgos informáticos, mientras el 42% en auditora de sistemas y el 33% no se capacita. Las empresas necesitan contar con personal que conozca sobre los riesgos informáticos en el procesamiento electrónico de datos, las buenas prácticas en la gestión de riesgos, las normativas aplicables y los estándares internacionales, esto con el fin de resguardar la información y cumplir con los objetivos de la entidad.

Pregunta 6 ¿Conoce usted qué son los activos de información?

Objetivo: Averiguar si los encargados del área de informática entienden el concepto de activos de información.

Cuadro N° 6

Título: Conocimiento activo de información

Conocimiento activo de información	Frecuencia absoluta	Frecuencia relativa
Si	12	100%
No	0	0%
Total	**12**	**100%**

Gráfico No. 6

Análisis e interpretación: Se ha determinado que el 100% de la población entiende el concepto de que son los activos de información. Por lo cual se puede identificar que los encargados de tecnología de información se capacitan en las diferentes áreas como gestión de riesgos y auditoria de sistemas, para proteger, mantener y resguardar estos activos en los cuales las empresas capturan, procesan y almacenan su información más valiosa, los encargados del área de informática son los responsables de establecer los lineamientos para una adecuada gestión de todos los recursos tecnológicos.

Pregunta 7 ¿La entidad lleva un reporte en el cual se detallen los activos información?

Objetivo: Identificar si en el departamento de informática se lleva un reporte en el cual se detalla el inventario de los activos de información.

Cuadro N° 7
Título: Seguridad de los activos

Seguridad de los activos	Frecuencia absoluta	Frecuencia relativa
SI	7	58%
NO	5	42%
Total	**12**	**100%**

Gráfico No. 7

Análisis e interpretación: Según los encuestados en el área de informática el 42% expresaron que no llevan reportes en el cual se detallan los activos de información, considerando que si conocen el concepto; estableciendo los parámetros según los estándares internacionales de las ISO en la cual manifiesta que los activos de información tienen que estar identificados de una forma clara y documentados en función de su importancia y así minimizar los riesgos garantizando que los inventarios de los activos tengan una protección eficiente ante cualquier desastre.

Pregunta 8 ¿La entidad posee una clasificación de su información de acuerdo con el valor que esta representa?

Objetivo: Comprender si la compañía le da el valor significativo a la información con la que cuenta.

Cuadro N° 8
Título: Valoración de la Información

Respuesta	Frecuencia absoluta	Frecuencia relativa
Si	7	58%
No	5	42%
Total	**12**	**100%**

Gráfico No. 8

Análisis e interpretación: Del total de la población el 42% no posee una clasificación de la información según el grado de importancia que representa lo que ocasionaría que tal información podría estar susceptible o vulnerable a posibles pérdidas o robo de la misma, careciendo en muchos casos de ser oportuna y confidencial, además de no asegurar un nivel adecuado de protección para este activo de información permitiendo indicar el grado de necesidad, de prioridad y de protección de los datos, clasificando la información según su valor, requisitos legales, la sensibilidad y la criticidad de la misma.

Pregunta 9 Si su respuesta a la pregunta anterior fue si ¿Con que frecuencia se realiza una evaluación de controles preventivos en el área de tecnologías de la información?

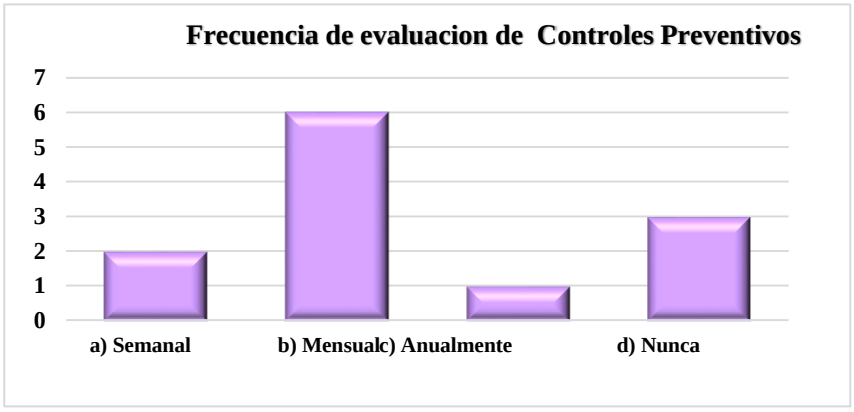
Objetivo: Verificar la frecuencia en que la empresa realiza controles preventivos en las tecnologías de la información para identificar las principales amenazas a las que se encuentran expuestas.

Cuadro N° 9

Título: Frecuencia de Controles Preventivos

Periodo	Frecuencia absoluta	Frecuencia relativa
Semanal	2	17%
Mensual	6	50%
Anualmente	1	8%
Nunca	3	25%
Total	**12**	**100%**

Gráfico No. 9



Análisis e interpretación: El 50% de las empresas encuestadas afirma que mensualmente realiza una evaluación de los controles preventivos, para tratar de evitar incidentes antes de que estos aparezcan, efectuando un monitoreo de las operaciones, así como del ingreso de datos a los sistemas de información, su procesamiento y salida, no obstante, un 17% de las empresas asegura que realiza este proceso más frecuentemente es decir cada semana y un 25% nunca efectúa una evaluación de sus controles preventivos por lo que están expuestos a riesgos que aún

no han considerado ni valorado y no le dan la importancia debida a su información, como resultado de la falta de capacitación en el área de tecnologías de la información y en la gestión efectiva de riesgos.

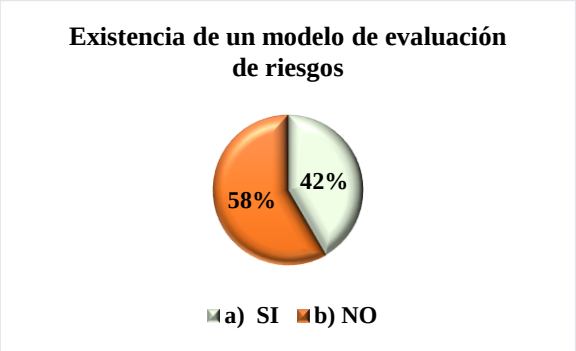
Pregunta 10 ¿Existe en la entidad un modelo de evaluación de riesgos informáticos en la captura, almacenamiento, procesamiento y salida de información, para garantizar la integridad y confidencialidad en la generación de información financiera contable?

Objetivo: Investigar si la entidad ha desarrollado un modelo de evaluación de riesgos informáticos en la generación de información financiera contable.

Cuadro N° 10
Título: Existencia de un modelo de evaluación de riesgos

Respuesta	Frecuencia absoluta	Frecuencia relativa
Si	5	42%
No	7	58%
Total	**12**	**100%**

Gráfico No. 10



Análisis e interpretación: De acuerdo a la información obtenida alrededor del 58% de empresas que comercializa equipo médico no cuenta con un modelo de evaluación de riesgos informáticos por lo que se encuentran en riesgo sus procesos de captura, almacenamiento, procesamiento y salida de información comprometiendo la integridad y confidencialidad en la generación de información financiera contable, ocasionado en parte por la falta de capacitación en modelos de gestión de riesgos de tecnologías como COBIT 5, ISO, ITIL y otros, la otra parte de empresas es decir el 42% de ellas afirma que si cuentan con tal modelo para proteger su información aunque no se encuentre escrito o no está desarrollado según los parámetros de la

norma ISO 31000:2018 que establece una gestión del riesgo en todos los niveles de la organización.

Pregunta 11 Según su experiencia ¿Sería útil para la entidad una evaluación de riesgos informáticos relacionados en la generación de información financiera contable, para mejorar su integridad y confidencialidad?

Objetivo: Confirmar si el desarrollo de un modelo para evaluar riesgos informáticos beneficiaria a la entidad a generar información integra y confiable para la toma de decisiones.

Cuadro N° 11
Título: Utilidad de una evaluación de riesgos

Respuesta	Frecuencia absoluta	Frecuencia relativa
Si	12	100%
No	0	0%
Total	**12**	**100%**

Gráfico No. 11

Análisis e interpretación: Del personal encuestado en las empresas que comercializa equipo médico el 100% manifiesta que sería de utilidad contar con una evaluación de riesgos informáticos que asegure la integridad y confiabilidad de la información financiera contable, es decir que todas las entidades de este sector poseen riesgos que deben considerar los encargados de TI y ya que la mitad de ellos poseen considerable experiencia en su ámbito, reconocen que tal evaluación les ayudaría agregando valor y calidad a sus procesos de entrada, procesamiento y

salida de datos en los sistemas, robusteciendo su administración y así se refleje en sus resultados financieros y rendimiento económico.

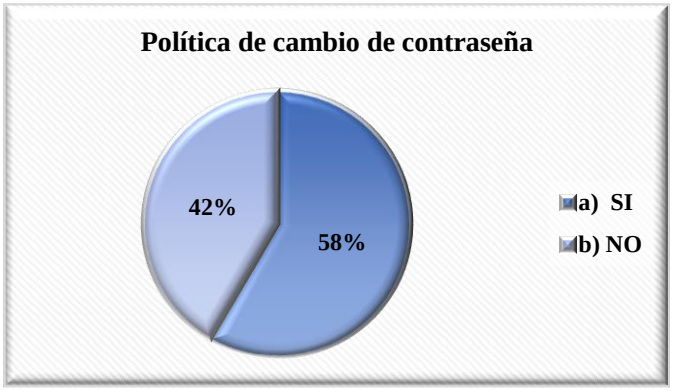
Pregunta 12 ¿Existe una política de cambio de contraseña para el acceso a los ordenadores de la entidad?

Objetivo: Cerciorarse que la empresa aplica controles generales en cuanto al acceso sus sistemas de información, con la finalidad que solo el personal autorizado pueda hacer uso de los reportes e informes.

Cuadro N° 12
Título: Política de cambio de contraseña

Respuesta	Frecuencia absoluta	Frecuencia relativa
Si	7	58%
No	5	42%
Total	**12**	**100%**

Gráfico No. 12



Análisis e interpretación: El 42 % de los encuestados afirma que no aplica política alguna para el cambio de contraseñas lo que representa una amenaza que puede traer como consecuencia la sustracción o revelación de las mismas, ocasionando pérdidas de información que provoca perjuicios económicos u otras consecuencias, por lo que existe deficiencias en la clasificación de la información según el grado de importancia que representa ocasionando que sea susceptible o vulnerable, por tanto se deben implementar practicas encaminadas a mejorar la seguridad y

autenticar al usuario al momento de realizar procesos u operaciones que involucran información sensible o confidencial.

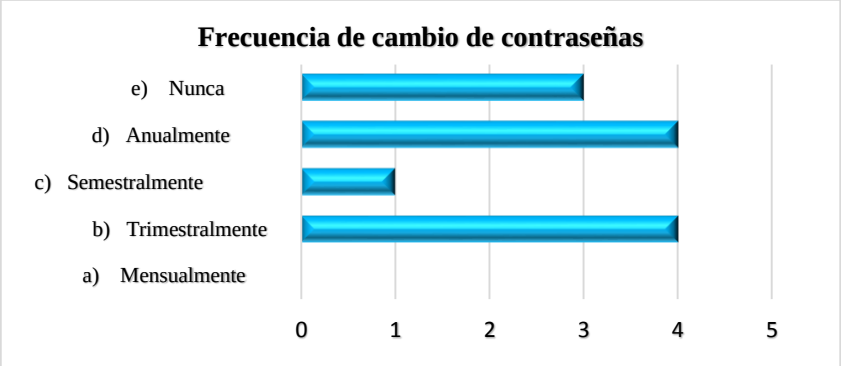
Pregunta 13 ¿Cuál es la periodicidad en que se realizan cambios de las contraseñas para el acceso a los sistemas?

Objetivo: Evaluar con que regularidad se hacen cambios de contraseñas y si la entidad posee una política en la cual la persona o administrador de los sistemas debe cumplir.

Cuadro N° 13
Título: Frecuencia de cambio de contraseñas

Periodo	Frecuencia absoluta	Frecuencia relativa
Mensualmente	0	0%
Trimestralmente	4	33%
Semestralmente	1	8%
Anualmente	4	33%
Nunca	3	25%
Total	**12**	**100%**

Gráfico No. 13



Análisis e interpretación: Los resultados indican que el 25% de la población asegura nunca realizar un cambio de contraseñas de ingreso a los sistemas lo que ocasiona que se generen riesgos como que personal no autorizado tenga acceso a todo tipo de información sensible relacionada a la entidad, un 33% afirma realizar el cambio trimestralmente y anualmente buscando en estos casos una clave que cumpla con criterios de seguridad lógica, esto debido a que un cambio de contraseña cada poco tiempo provoca que se pierda la efectividad de la misma

y son políticas ya establecidas por la entidad, razón por la que ninguna empresa cambia las contraseñas mensualmente.

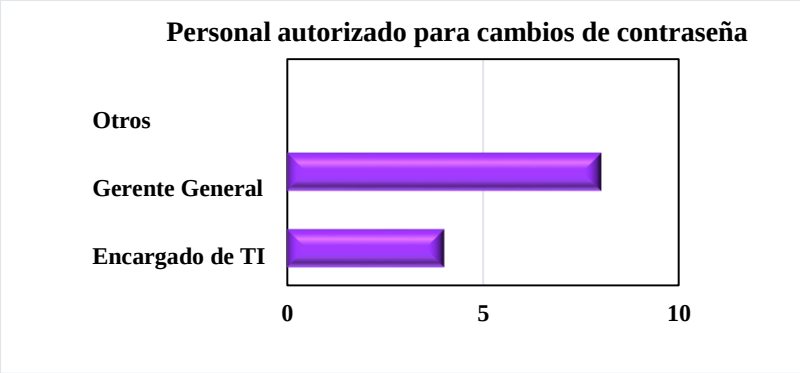
Pregunta 14 ¿Quiénes están autorizados por la entidad para realizar un cambio de contraseña?

Objetivo: Conocer el rol que desempeña dentro de la entidad la persona que administra el equipo de cómputo en el que se almacena la información de la empresa.

Cuadro N° 14
Título: Personal autorizado para cambios de contraseña

Periodo	Frecuencia absoluta	Frecuencia relativa
Gerente General	5	38%
Encargado de TI	8	62%
Otros	0	0%
Total	**12**	**100%**

Gráfico No. 14



Análisis e interpretación: Para las empresas que comercializan equipo médico el encargado de tecnologías de la información es en su mayoría la persona responsable de administrar y de otorgar privilegios en los niveles de la organización para gestionar el equipo informático y ordenadores con alrededor del 62% de los resultados, ya que puede realizar los cambios de contraseña necesarios y además por su experiencia está capacitado para realizar o autorizar tal cambio, alrededor de 38% de las entidades encuestadas sostiene que el gerente general también

está autorizado para efectuar cambios en las claves de acceso de acuerdo a las funciones que se le han otorgado y la cantidad de información confidencial que administra.

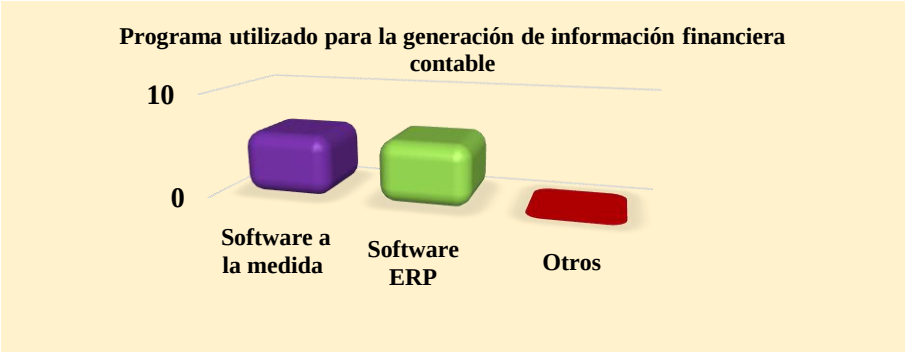
Pregunta 15 ¿Qué programa se utiliza para la generación de la información financiera contable?

Objetivo: Conocer el tipo de software que se utiliza para la entrada, procesamiento y almacenamiento de la información, además tomar en consideración que la facturación se desarrolle en algún software de ofimática o uno en específico de acuerdo con el sector que pertenezca la entidad.

Cuadro N° 15
Título: Programa utilizado para la generación de información financiera contable

Áreas de capacitación	Frecuencia absoluta	Frecuencia relativa
Software a la medida	6	50%
Software ERP	6	50%
Otros	0	0%
Total	**12**	**100%**

Gráfico No. 15



Análisis e interpretación: De las 12 empresas el 50% de la población utiliza un software a la medida debido a que las entidades al poseer un profesional en el área de informática desarrollan softwares o aplicaciones de acuerdo a las necesidades del sector al que pertenece. El 50% restante posee un software ERP estándar el cual los procesos deben adaptarse a los sistemas,

ocasionando una desventaja para la organización ya que no se tiene acceso a todos los módulos que conforman el sistema por el alto costo de adquisición, originando a que la entidad se auxilie de programas adicionales para agilizar sus procesos y presentar reportes de acuerdo a las necesidades de la entidad.

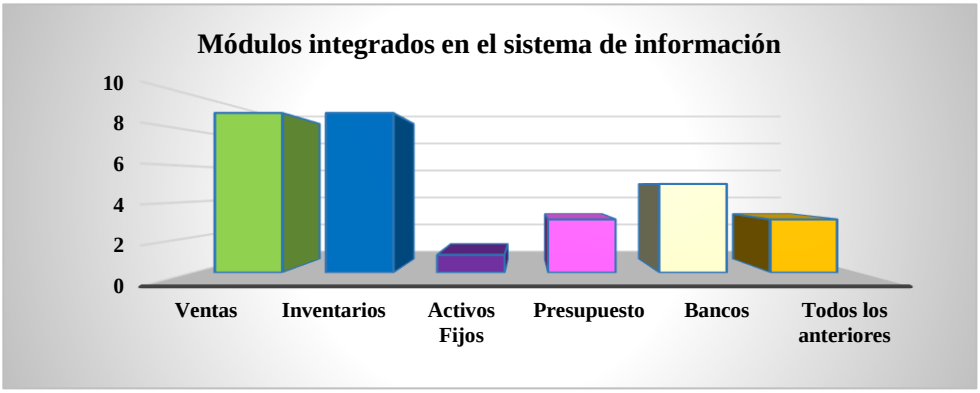
Pregunta 16 ¿Cuáles de los siguientes módulos tiene integrados el sistema utilizado por la entidad?

Objetivo: Averiguar el sistema contable se encuentra integrado a otros módulos o es independiente.

Cuadro N° 16
Título: Módulos integrados en el sistema de información

Módulos integrados	Frecuencia absoluta	Frecuencia relativa
Ventas	9	75%
Inventarios	9	75%
Activos Fijos	1	8%
Presupuesto	3	25%
Bancos	5	42%
Todos los anteriores	3	25%

Gráfico No. 16



Análisis e interpretación: Las empresas del sector de equipos médicos respondieron en un 75% que los principales módulos que se encuentran integrados en sus sistemas de informáticos son el de ventas e inventario, ya que se puede obtener un control de los productos existentes de la entidad, así mismo al integrarse con el módulo de ventas se manejan las salidas de la bodega y la facturación. Además el 42% respondió que es necesario incluir en el sistema el módulo de

bancos para llevar el control de los ingresos y egresos de los flujos de efectivo, sin embargo es importante para las empresas de este sector contar con un sistema ERP en el cual permita agilizar las operaciones de la entidad.

Pregunta 17 ¿El personal de la empresa tiene los accesos restringidos a la información de acuerdo con la segregación de sus funciones?

Objetivo: Indagar si la entidad aplica controles de acceso para el ingreso de datos según las funciones que desempeña el personal.

Cuadro N° 17
Título: El personal posee accesos restringidos de acuerdo de la segregación de funciones

Se poseen accesos restringidos	Frecuencia absoluta	Frecuencia relativa
Si	11	92%
No	1	8%
Total	**12**	**100%**

Gráfico No. 17

Análisis e interpretación: Según los datos recopilados 11 empresas que representa el 92%, indican poseer controles de acuerdo a las funciones de cada empleado, ya que la información se ha convertido en un activo valioso, y para asegurar que sea integra, confiable la mayoría de empresas encuestadas cuenta con una a clasificación de su información de acuerdo a la importancia que tiene para la entidad para minimizar los riesgos asociados como la

manipulación, alteración de la información financiera contable que pueda perjudicar los objetivos estratégicos de la organización, sin embargo es necesario que el personal se capacite en estándares y buenas prácticas para la implementación de una cultura de gestión de riesgos.

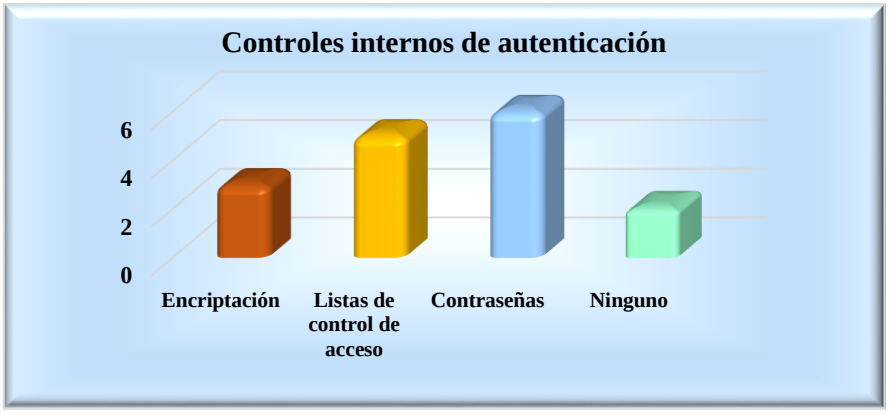
Pregunta 18 ¿Qué tipo de controles internos utiliza para efectuar la autenticación de los usuarios al sistema?

Objetivo: Identificar los tipos de controles implementados para autenticar los accesos a los sistemas que procesan información confidencial para la empresa.

Cuadro N° 18
Título: Controles internos de autenticación

Controles internos de autenticación	Frecuencia absoluta	Frecuencia relativa
Encriptación	3	25%
Listas de control de acceso	5	42%
Contraseñas	6	50%
Ninguno	2	17%

Gráfico No. 18



Análisis e interpretación: El 50% de la población utilizan controles de autenticación como las contraseñas para resguardar que la información sea mal utilizada por personal no autorizado o personas externas a la entidad, en la cual pueda perjudicar su reputación, sin embargo el 42% respondió que posee un listado de controles de acceso en donde solo personas especificas tienen

accesos a los datos de acuerdo a las funciones o áreas a los que pertenecen, en todo caso es necesario evaluar con regularidad la aplicación de estos controles para disminuir los riesgos.

Pregunta 19 ¿Existen manuales o instructivos para el personal en los que se describa el manejo de los datos en los sistemas de información?

Objetivo: Investigar si existen manuales de apoyo para facilitarle al personal los procedimientos a seguir para el ingreso, procesamiento y salida de la información, con la finalidad de garantizar que la información se valida.

Cuadro N° 19
Título: Existen manuales o instructivos escritos

Existencia de manuales o instructivos para el personal	Frecuencia absoluta	Frecuencia relativa
Si	6	50%
No	6	50%
Total	**12**	**100%**

Gráfico No. 19

Análisis e interpretación: El 50% de las empresas manifestaron contar con procedimientos específicos para el procesamiento electrónico de datos; sin embargo el 50% restante manifestó que no cuentan con manuales o instructivos escritos en el que se detallen los procedimientos a seguir para el ingreso de la información en los sistemas informáticos. Por lo tanto las empresas al capacitar a los encargados o administradores de tecnologías de la información en cuanto a la gestión de riesgos deben aplicar controles, así como llevar un registro detallado los activos de

información de la entidad donde se almacena información sensible para identificar al personal responsable del manejo de los sistemas.

Pregunta 20 ¿En caso de fallo en los sistemas informáticos y servicios conexos se aplica planes de contingencia para resguardar los recursos informáticos?

Objetivo: Conocer si la empresa cuenta con planes de contingencia, para el resguardo de la información digital.

Cuadro N° 20
Título: Se aplican planes de contingencia en caso de fallo en los sistemas de información

Aplicación de planes de contingencia	Frecuencia absoluta	Frecuencia relativa
Si	9	75%
No	3	25%
Total	**12**	**100%**

Gráfico No. 20

Análisis e interpretación: Con el avance de la tecnología las empresas que comercializan equipos médicos se han visto en la necesidad de mejorar sus procesos adoptando sistemas informáticos para agilizar el ingreso de la información y que esta se encuentre disponible en el momento que sea necesario; según los resultados de la encuesta el 75% de las empresas aplican planes de contingencia ya que son una herramienta que permiten afrontar de manera oportuna adecuada y efectiva, la eventualidad de incidentes o accidentes que podrían generar pérdidas económicas.

Anexo No. 3

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

CUESTIONARIO SOBRE EL TEMA DE INVESTIGACIÓN DENOMINADO "EVALUACIÓN DE RIESGOS INFORMÁTICOS RELACIONADOS A LA GENERACIÓN DE INFORMACIÓN FINANCIERA CONTABLE EN LAS EMPRESAS QUE COMERCIALIZAN EQUIPOS MÉDICOS DEL ÁREA METROPOLITANA DE SAN SALVADOR"

DIRIGIDO A: Los Profesionales de Contaduría Pública inscritos en el Consejo de Vigilancia de la Profesión de la Contaduría Pública y Auditoria.

OBJETIVO: Obtener información que sustente la problemática objeto de estudio.

PROPÒSITO: El presente cuestionario ha sido elaborado por estudiantes de la carrera de Licenciatura en Contaduría Pública, con el propósito de recopilar información y fortalecer el trabajo de investigación con la problemática objeto de estudio antes mencionado.

INDICACIONES: Por favor marque con una "x" la(s) respuesta(s) que usted considere más convenientes.

1. **¿En cuáles de las siguientes áreas ha recibido o recibe actualmente formación profesional? Puede seleccionar más de una opción.**

a) Informática	☐	e) Auditoría interna	☐
b) Contabilidad	☐	f) Auditoría forense	☐
c) Finanzas	☐	g) Administración de riesgos	☐
d) Auditoría externa	☐	h) Impuestos	☐

2. **¿Con que frecuencia se capacita en el área de tecnologías de la información?**

a) Mensualmente	☐	d) Anualmente	☐

b) Trimestralmente ☐ e) Pocas veces ☐

c) Semestralmente ☐ f) No se capacita ☐

3. Según su experiencia ¿Cómo evalúa la oferta de capacitaciones en el área de tecnologías de información para Contadores Públicos por parte de los gremios, asociaciones y demás consultores en la materia?

a) Excelente ☐ d) Regular ☐

b) Muy buena ☐ e) Mala ☐

c) Buena ☐ f) Escasa ☐

4. ¿Cuándo realiza una evaluación de riesgos bajo qué enfoque basan la consideración de aspectos relativos a tecnologías de información? Puede seleccionar más de una opción.

a) COBIT 5 ☐

b) ISO 27001/27002 ☐

c) ISO 31000/2018 (Gestión del Riesgo. Directrices) ☐

d) COSO ERM ☐

e) Otros ☐

Especifique _____

5. Según su criterio ¿Cuál de las siguientes áreas se consideran más vulnerables al momento de realizar una evaluación de riesgos informáticos? Puede seleccionar más de una opción.

a) Seguridad lógica ☐ d) Hardware ☐

b) Seguridad física ☐ e) Recursos humanos ☐

c) Software ☐

6. Según su experiencia ¿Es necesario que existan controles internos para la gestión de riesgos en las entidades?

a) SI ☐ b) NO ☐

7. Según su criterio ¿Con que frecuencia las entidades deben realizar una evaluación efectiva de riesgos informáticos?

a) Mensualmente ☐ d) Anualmente ☐

b) Trimestralmente ☐ e) Siempre ☐

c) Semestralmente ☐

8. **Según su criterio ¿Es necesario auxiliarse de expertos en tecnología de la información para realizar una evaluación del riesgo informático?**

   a) SI ☐ b) NO ☐

9. **¿Se toman en cuenta los principios del procesamiento electrónico de datos para evaluar la confidencialidad e integridad de la información?**

   a) SI ☐ b) NO ☐

10. **Según su criterio ¿Es necesario y útil para realizar una auditoría que las entidades cuenten con un modelo de evaluación para la identificación y medición de riesgos de tecnologías de información especialmente en el procesamiento electrónico de datos?**

    a) SI ☐ b) NO ☐

Anexo No. 4

TABULACIÓN Y ÁNALISIS A CONTADORES PÚBLICOS

Pregunta 1 ¿En cuáles de las siguientes áreas ha recibido o recibe actualmente formación profesional? Puede seleccionar más de una opción.

Objetivo: Conocer las principales áreas de interés profesional de los contadores públicos.

Cuadro N° 1
Título: Áreas de formación profesional

Áreas de capacitación	Frecuencia absoluta	Frecuencia relativa
Informática	8	30%
Contabilidad	13	48%
Finanzas	12	44%
Auditoria Externa	18	67%
Auditoría Interna	14	52%
Auditoría Forense	4	15%
Administración de riesgos	9	33%
Impuestos	23	85%

Grafico No. 1

Análisis: La Norma de Educación Continuada obliga a los profesionales en contaduría pública, a capacitarse principalmente en las áreas de auditoría, contabilidad e impuestos, según los resultados obtenidos por los encuestados, se puede corroborar que las áreas de mayor interés para los profesionales son: los impuestos con un porcentaje del 85%, seguido de auditoría externa con un 67% y auditoria interna el 52% y solo el 30% se capacita en el área de informática. Por lo cual se considera que los profesionales no le dan la importancia que requiere al área de informática que es parte integral para el desarrollo de su trabajo.

Pregunta 2 ¿Con que frecuencia se capacita en el área de tecnologías de la información?

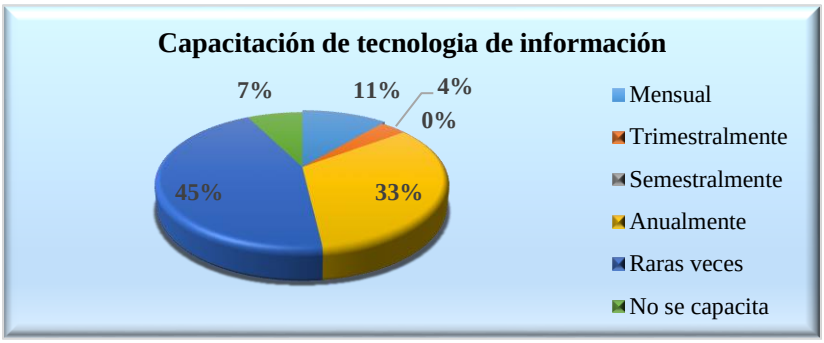
Objetivo: Confirmar si los profesionales en contaduría reciben capacitaciones constantemente que les permita estar actualizados en el área de las tecnologías de información.

Cuadro N° 2

Título: Capacitación de Tecnología de información

Capacitación en tecnología de información	Frecuencia absoluta	Frecuencia relativa
Mensual	3	11%
Trimestralmente	1	4%
Semestralmente	0	0%
Anualmente	9	33%
Pocas veces	12	44%
No se capacita	2	7%
Total	**27**	**100%**

Grafico No. 2



Análisis e interpretación: Con base a esta pregunta se concluye que el contador público debe capacitarse más y de manera constante en el área en informática, para poder evaluar los riesgos tecnológicos en el momento que se generan los reportes, así mismo realizar auditorías de calidad, dominando técnicas que faciliten el análisis técnico y sustantivo de las mismas. De los 27 encuestados, el 44% rara vez se capacita, siendo esta una deficiencia ya que es necesario evaluar los sistemas para poder realizar los trabajos de auditoría.

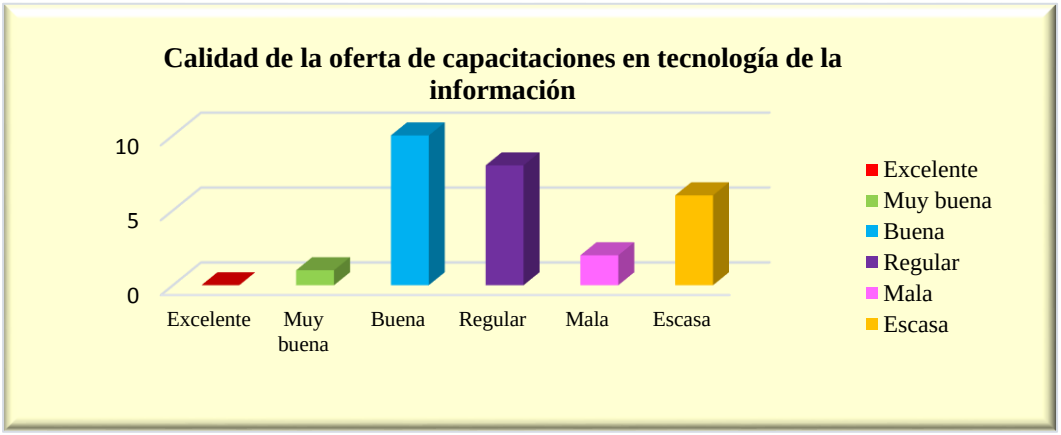
Pregunta 3 Según su experiencia: ¿Cómo evalúa la oferta de capacitaciones en el área de tecnologías de información para contadores públicos por parte de los gremios, asociaciones y demás consultores en la materia?

Objetivo: Valorar por parte de los profesionales en contaduría el servicio de capacitaciones en el área de informática por parte de los gremios, asociaciones y consultores en la materia.

Cuadro N° 3
Título: Calidad de la oferta de capacitaciones en tecnología de la información

Calificación	Frecuencia absoluta	Frecuencia relativa
Excelente	0	0%
Muy buena	1	4%
Buena	10	37%
Regular	8	30%
Mala	2	7%
Escasa	6	22%
Total	**27**	**100%**

Grafico No. 3



Análisis e interpretación: Los profesionales de la contaduría pública no son capacitados de forma constante ya que el 37% de los encuestados, califican a las diferentes instituciones que brindan el servicio como “bueno”, mientras que el 22% indicó que las ofertas son “escasas” puesto que no consideran impartir aspectos de suma importancia para el auditor.

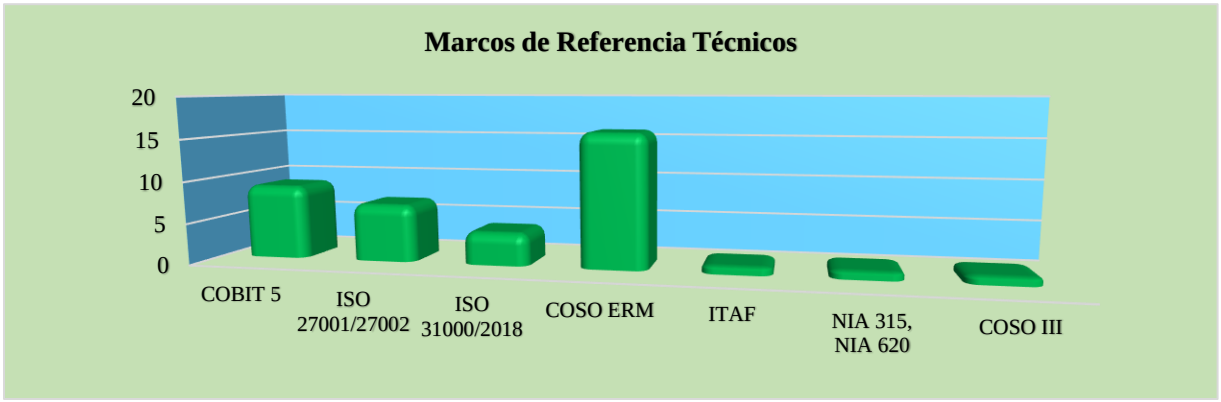
Pregunta 4 ¿Cuándo realiza una evaluación de riesgos bajo qué enfoque basan la consideración de aspectos relativos a tecnologías de información?

Objetivo: Determinar cuál(es) son los marcos de referencia técnico más utilizado por los profesionales en contaduría para la evaluación de riesgos informáticos.

Cuadro N° 4
Título: Marcos de referencia técnicos

Principales marcos de referencia	Frecuencia absoluta	Frecuencia relativa
COBIT 5 (Objetivos de control para la información y tecnologías relacionadas)	9	33%
ISO 27001/27002 (Sistema de gestión para la seguridad de la información)	7	26%
ISO 31000/2018 (Gestión del Riesgo. Directrices)	4	15%
COSO ERM	16	59%
ITAF	1	4%
NIA 315, NIA 620	1	4%
COSO III	1	4%

Grafico No. 4



Análisis e interpretación: Los marcos de referencia técnicos más utilizados por los encuestados son el Modelo de COSO ERM con el 59%, ya que este marco técnico forma parte de las buenas prácticas de gestión empresarial más conocidas, difundidas y de mayor aceptación general, en segundo lugar se encuentra COBIT 5 con 33% que integra el gobierno de la entidad con la gestión de tecnologías de la información, la norma ISO 31000:2018 por ser de reciente

presentación y ante la falta de capacitación en tecnologías de la información aún no se aplica ampliamente en todas las entidades.

Pregunta 5 Según su criterio ¿Cuál de las siguientes áreas se consideran más vulnerables al momento de realizar una evaluación de riesgos informáticos?

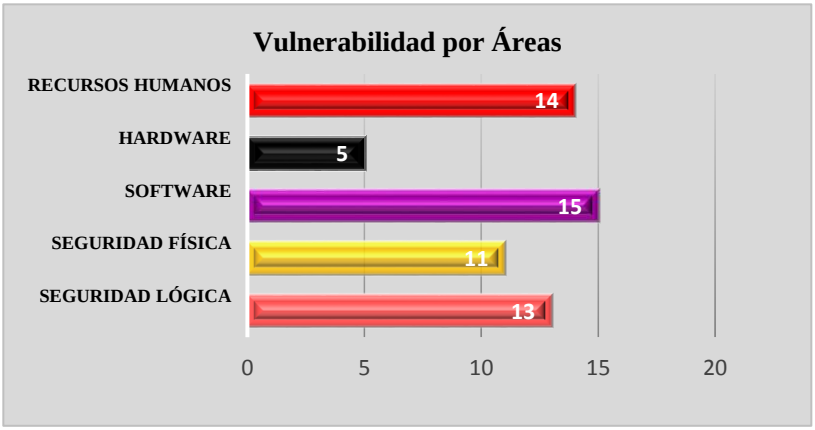
Objetivo: Identificar las principales áreas en las cuales existen riesgos tecnológicos según su relevancia dentro de la organización tomando en cuenta la percepción de vulnerabilidad de que tenga el profesional de la contaduría.

Cuadro N° 5

Título: Percepción de vulnerabilidad por áreas

Principales áreas	Frecuencia absoluta	Frecuencia relativa
Seguridad Lógica	13	48%
Seguridad Física	11	41%
Software	15	56%
Hardware	5	19%
Recursos Humanos	14	52%

Grafico No. 5



Análisis e interpretación: Los Profesionales de Contaduría Pública encuestados afirman con el 56 % que el área más vulnerable al realizar una evaluación de riesgos informáticos es la de software debido a los continuos avances y cambios en este ámbito que obligan a capacitarse frecuentemente, además el 52% de profesionales considera como segunda área más susceptible

la de recursos humanos tomando en cuenta el acceso a información sensible que estos poseen y el 19% por el contrario considera que el área más fuerte es la de hardware.

Pregunta 6: Según su experiencia ¿Es necesario que existan controles internos para la gestión de riesgos en las entidades?

Objetivo: Precisar la importancia que amerita para el profesional de la contaduría el establecimiento de directrices que orienten a la entidad para salvaguardar sus activos de información.

Cuadro N° 6
Título: Controles en la gestión de riesgos

Controles en la gestión de riesgos	Frecuencia absoluta	Frecuencia relativa
Si	27	100%
No	0	0%
Total	**27**	**100%**

Grafico No. 6

Análisis e interpretación: Una de las tareas claves de la administración es la gestión del riesgo, normalmente estos controles no se encuentran escritos en la entidad, sino que los usuarios los conocen de manera empírica, los problemas se van solucionando a medida van apareciendo, en resumen, el 100% de los profesionales encuestados están de acuerdo con que deben de existir controles internos.

Pregunta 7: Según su criterio ¿Cada cuánto tiempo las entidades deben realizar una evaluación efectiva de riesgos informáticos?

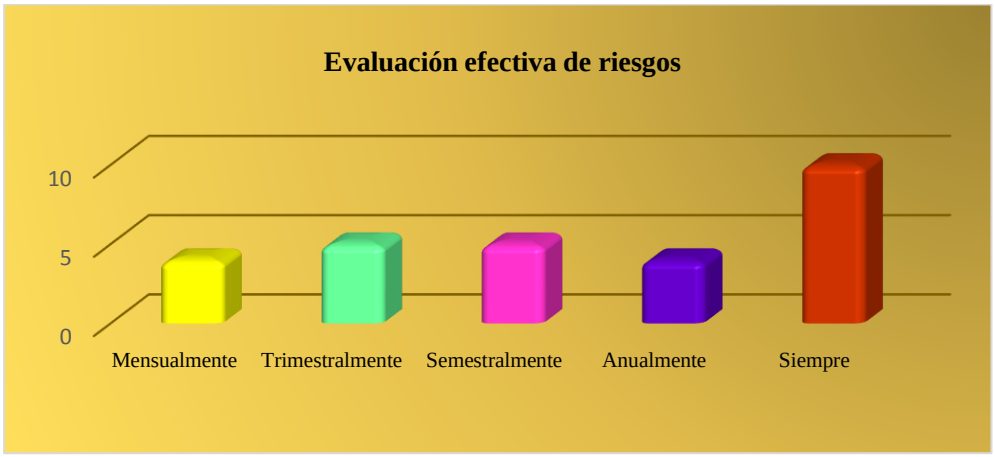
Objetivo: Verificar con que regularidad se realiza una evaluación de riesgos informáticos, que contribuya a mitigar las amenazas a los cuales se encuentran expuestos los activos de información.

Cuadro N° 7

Título: Evaluación efectiva de riesgos

Evaluación efectiva de riesgos	Frecuencia absoluta	Frecuencia relativa
Mensualmente	4	15%
Trimestralmente	5	19%
Semestralmente	5	19%
Anualmente	4	15%
Siempre	10	37%

Grafico No. 7



Análisis e interpretación: Según el análisis de las respuestas el 37% de los encuestados contestaron que las empresas deben estar en constante evaluación, el 19% consideran que se debe realizar trimestral o semestral con el fin de mitigar y prevenir los riesgos a los que se encuentran expuestos los activos informáticos, así mismo, es necesario un modelo de evaluación para la identificación de riesgos en el procesamiento electrónico de datos.

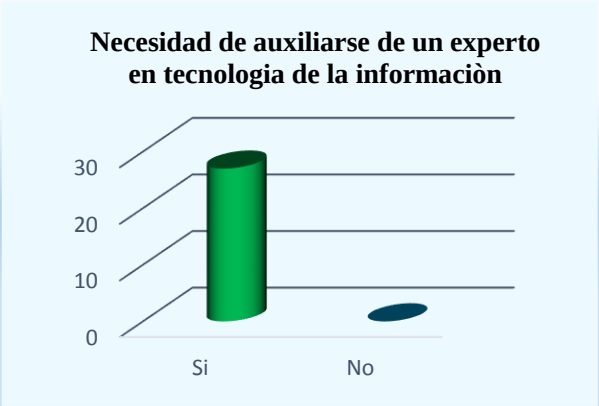
Pregunta 8 Según su criterio ¿Es necesario auxiliarse de expertos en tecnología de la información para realizar una evaluación del riesgo informático?

Objetivo: Conocer la necesidad de emplear la ayuda de un experto de tecnologías de la información que puedan auxiliar al profesional de la contaduría cuando se necesite realizar un diagnóstico de la vulnerabilidad en los activos de información de la organización.

Cuadro N° 8
Título: Necesidad de auxiliarse de un experto en tecnología de la información

Respuesta	Frecuencia absoluta	Frecuencia relativa
Si	27	100%
No	0	0%
Total	**27**	**100%**

Gráfico No. 8



Análisis e interpretación: El 100% de los contadores públicos encuestados consideran que es importante la intervención de un profesional para garantizar que la información financiera contable facilite a la toma de decisiones a los usuarios internos y externos, a su vez que tome en cuenta la necesidad de contar con una evaluación de riesgos que permita identificar las principales amenazas que puedan afectar a los activos de información en el procesamiento electrónico de datos, evaluando la efectividad de los controles generales y específicos en cuanto

al uso de la tecnología para garantizar que los datos procesados por los sistemas informáticos generen información integra.

Pregunta 9 ¿Se toman en cuenta los principios del procesamiento electrónico de datos para evaluar la confidencialidad e integridad de la información?

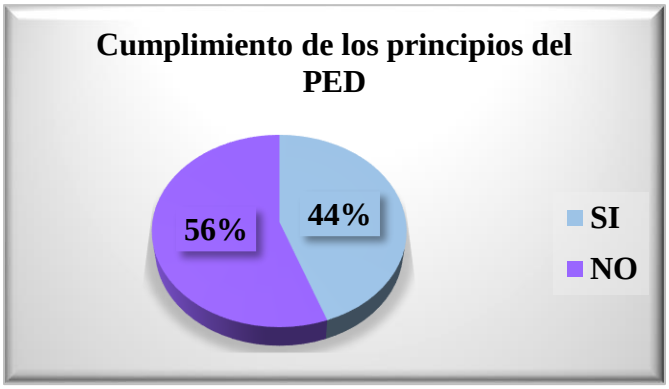
Objetivo: Verificar si la información procesada es analizada por el profesional de la contaduría en cuanto a que cumple los principios del procesamiento electrónico de datos y de esa manera asegurando a las entidades la buena toma de decisiones.

Cuadro N° 9

Título: Cumplimiento de los principios del PED

Áreas	Frecuencia absoluta	Frecuencia relativa
SI	12	44 %
NO	15	56 %
Total	**27**	**100%**

Grafico No. 9



Análisis e interpretación: El 56% de los encuestados asegura que no toma medidas para evaluar y ordenar desde la recolección de los datos primarios de entrada, su procesamiento y salida probablemente por la falta de capacitación en tecnologías de la información., un 44% de los profesionales afirma que aplican los principios del PED para obtener información útil, aunque no cuenten con un modelo que le permita tomar las decisiones más convenientes por el

usuario final y así se asegure la confidencialidad e integridad en la generación de la información financiera contable

Pregunta 10 Según su criterio ¿Es necesario y útil en las entidades contar con un modelo de evaluación para la identificación y medición de riesgos de tecnologías de información especialmente en el procesamiento electrónico de datos?

Objetivo: Conocer la necesidad de un modelo de evaluación de riesgos en la captura, procesamiento, almacenamiento y salida de información cuando se encuentra en un ambiente computarizado

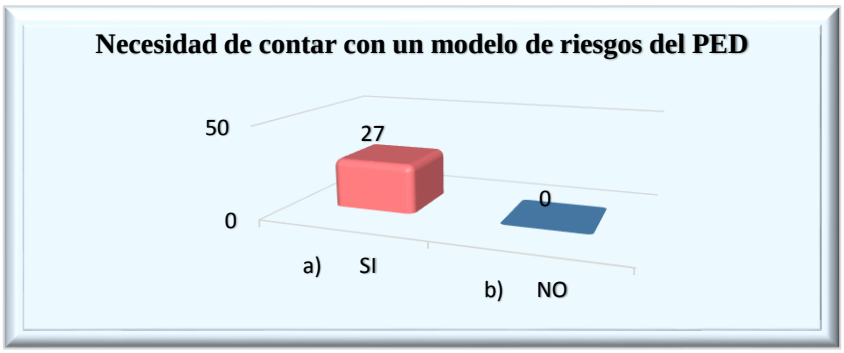
Cuadro N° 10

Título: Necesidad de contar con un modelo de riesgos del PED

.

Áreas	Frecuencia absoluta	Frecuencia relativa
SI	27	100%
NO	0	0%
Total	**27**	**100%**

Grafico No. 10



Análisis e interpretación: De acuerdo con los datos obtenidos el 100% de los profesionales en contaduría pública considera útil y necesario contar con controles internos para la gestión de riesgos informáticos mediante una evaluación de riesgos en la generación de información financiera contable y ante los continuos cambios y actualizaciones en los sistemas de información, para agregar valor a las operaciones del negocio junto a la toma de decisiones de la administración.

Anexo No. 5

Glosario de términos

Activo: es un recurso del sistema de información, necesario para garantizar el correcto funcionamiento de los procesos de la organización (Tejada, 2014)

Amenazas: se entiende por amenaza una condición del entorno de los sistemas, áreas o dispositivos que contienen información importante (persona, equipo, suceso o idea) que ante determinada circunstancia podría dar lugar a que se produjese una violación de seguridad, afectando parte de la información y de la TI de la organización. (Urbina, 2016)

Análisis de riesgos: proceso y metodología utilizados para estimar magnitud de los riesgos a los que se expone la organización. (Tejada, 2014)

Auditoria informática: identifica el nivel de exposición por falta de controles.

Bases de datos: conjunto de información útil organizada de una forma específica y almacenada en una computadora que permite el acceso, ordenamiento, análisis y salida de los datos. (Amaya, 2009)

Centros de procesamientos de datos: es la ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización. (Santos, 2014)

COBIT: objetivos de control para la información y tecnologías relacionadas. Es un conjunto de completo que contiene la información de que las empresas necesitan para adoptar un marco de trabajo, el cual proporciona un modelo de procesos de referencia y un lenguaje común para que todas las organizaciones visualicen sus actividades en base a las TI.

Confidencialidad: se refiere a que todas las etapas del procesamiento de la información, esta se encuentre protegida contra accesos no autorizados los cuales pueden derivar en la alteración o robo de información confidencial. (Urbina, 2016)

Control interno informático: son actividades o acciones realizadas de forma manual o automática para prevenir, corregir errores o irregularidades que puedan afectar el funcionamiento de un sistema para lograr sus objetivos.

Control interno: contempla una seguridad razonable, pero no absoluta, de que los objetivos del sistema se cumplirán. (Estupiñán, 2015)

Dato: puede ser un número, una palabra o una imagen. (Karen & Lares, 2009)

Efectividad: se trata de lograr que la información sea en realidad la necesaria para desarrollar cualquiera de las tareas que se desarrollan en la empresa u organización y sea adecuada para realizar los procesos del negocio. (Urbina, 2016)

Eficiencia: la información debe ser generada y procesada utilizando de manera óptima los recursos que tiene la empresa para este fin. (Urbina, 2016)

Fuente de riesgo: elemento que, por si solo o en combinación con otros, tiene el potencial de generar riesgo. (ISO, 31000:2018)

Gestión de la seguridad de la información: es la parte de la gestión de tecnología de la información encargada de la protección y la seguridad de los activos informativos de una organización.

Gestión del riesgo: es el conjunto de procesos desarrollados por una organización con el fin de disminuir la probabilidad y ocurrencia de amenazas y aumentar la probabilidad de ocurrencia de oportunidades con efectos negativos. (Tejada, 2014)

Hardware: incluye todos los componentes electrónicos, eléctricos y mecánicos que componen una computadora. (Amaya, 2009)

Impacto: es la medición y valoración del daño que podría producir a la organización un incidente de seguridad. (Gomez Vieites, 2011)

Incidente de seguridad: es cualquier evento que tenga o pueda tener como resultado la interrupción de los servicios suministrados por un sistema informático y/o posibles pérdidas físicas, de activos o financieras. Es decir, se considera que un incidente es la materialización de una amenaza. (Gomez Vieites, 2011)

Informe de evaluación de riesgos: son las acciones ejecutadas en el proceso de gestión de riesgos documentarse debidamente para poder elaborar un informe de valoración de riesgos con los resultados obtenidos en el análisis. (Tejada, 2014)

Integridad: significa que la información que se recibe sea precisa y este completa (su contenido es el necesario) para los fines que se persiguen con su procesamiento así como su validez. (Urbina, 2016)

Matriz de riesgos: es una representación gráfica de la probabilidad e impacto de uno o más de la probabilidad e impacto de uno o más riesgos.

Procesamiento de electrónico de datos (PED): es la técnica que consiste en la recolección de datos primarios de entrada que son evaluados y ordenados con la finalidad de que se obtenga información útil, en la que pueda el usuario final tomar decisiones o realizar acciones.

Red: en informática, interconexión de computadoras mediante cales, ondas radiales o telefónicas. (Amaya, 2009)

Riesgo: es definido generalmente como una combinación de la probabilidad de un evento y sus consecuencias. Las consecuencias se reflejan en que no se logren los objetivos de la empresa. (Santillán, 2015)

Riesgo: es una combinación de la probabilidad de un evento y sus consecuencias. Las consecuencias se reflejan en que no se logren los objetivos de la empresa. (ISACA, 2013)

Riesgos tecnológicos: suelen ser cometidos por usuarios con muy poca experiencia, quienes no miden la magnitud de las consecuencias. (Urbina, 2016)

Seguridad de la Información: es la disciplina que con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que están expuestos. (Baca Urbina, 2016)

Seguridad física: trata de proteger el hardware, teniendo en cuenta entre otros aspectos la ubicación y las amenazas de tipo físico: robos, catástrofes naturales o artificiales, etc. Algunas medidas son el estudio de la ubicación correcta, medidas preventivas contra incidentes. (Santos, 2014)

Seguridad informática: es la disciplina que con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenaza, minimizando los riesgos tanto físicos como lógicos , a los que están expuesta. (Urbina, 2016)

Seguridad lógica: protege el software tanto a nivel de sistema operativo como de aplicación, sin perder nunca de vista el elemento fundamental a proteger, la información o datos del usuario. (Santos, 2014)

Sistemas operativos: software de base instalado en un sistema informático que interactúa con el hardware y permite la ejecución de las aplicaciones instaladas en el.

Software: programas y lenguajes de programación. (Amaya, 2009)

Tecnología de la información: es el conjunto de dispositivos, servicios y actividades apoyadas por equipo de cómputo, y que se basan en la transformación de información numérica, también llamada digital. (Santillán, 2015) México D.F Pág. 2

Tratamiento del riesgo: procesos realizados para modificar los riesgos de una organización. (Tejada, 2014)

Virus: son un tipo de software malicioso que se diseñan para dañar el equipo al que acceden, pasando desapercibidos por el usuario. Su funcionamiento también varía según el tipo de virus. (Tejada, 2014)

Vulnerabilidad: constituye un hecho o una actividad que permite concretar una amenaza. Se es vulnerable en la medida que no hay suficiente protección como para evitar que llegue a suceder una amenaza. (Urbina, 2016)

AnexoNo. 6

Universo y Muestra

Departamento	Municipio	Actividad	Nombre Comercial
SAN SALVADOR	SAN MARCOS	VENTA AL POR MAYOR DE REACTIVOS PARA LABORATORIO	RGH DE EL SALVADOR , S.A. DE C.V.
SAN SALVADOR	SAN MARCOS	VENTA AL POR MAYOR DE REACTIVOS PARA LABORATORIO	PRODYLAB
SAN SALVADOR	SAN SALVADOR	VENTA AL POR MAYOR DE REACTIVOS PARA LABORATORIO	PROMED, S. A. DE C. V.
SAN SALVADOR	SAN MARCOS	VENTA AL POR MAYOR DE REACTIVOS PARA LABORATORIO	ALFA, S. A. DE C. V.
SAN SALVADOR	SAN MARCOS	VENTA AL POR MAYOR DE REACTIVOS PARA LABORATORIO	LABTRONIC, S. A DE C. V
SAN SALVADOR	SAN MARCOS	Venta al por mayor de reactivos para laboratorio	DIAGNOSAL..
SAN SALVADOR	SAN SALVADOR	VENTA AL POR MAYOR DE REACTIVOS PARA LABORATORIO	IMPOLAB, S.A DE C.V
LA LIBERTAD	NUEVO CUSCATLAN	VENTA AL POR MAYOR DE REACTIVOS PARA LABORATORIO	DROGUERIA F.G. DE DIOS, S.A DE C.V.
LA LIBERTAD	SANTA TECLA	VENTA AL POR MAYOR DE REACTIVOS PARA LABORATORIO	DISTRIBUIDORA DE PRODUCTOS MERCK
SAN SALVADOR	SAN MARCOS	VENTA AL POR MAYOR DE REACTIVOS PARA LABORATORIO	PROVEEDORES DE INSUMOS DIVERSOS
SAN SALVADOR	SAN MARCOS	VENTA AL POR MAYOR DE REACTIVOS PARA LABORATORIO	AGROBIOTEK EL SALVADOR, S.A. DE C.V.
SAN SALVADOR	SAN MARCOS	VENTA AL POR MAYOR DE REACTIVOS PARA LABORATORIO	HIGH - TECH MEDICAL SYSTEMS , S. A. DE C. V.

Directorio Económico 2016 según la base de datos de la Dirección General de Estadísticas y Censo

No	Departamento	Municipio	Actividad
1	LA LIBERTAD	SANTA TECLA	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
2	LA LIBERTAD	SANTA TECLA	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
3	LA LIBERTAD	SANTA TECLA	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
4	SAN SALVADOR	AYUTUXTEPEQUE	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
5	SAN SALVADOR	SAN MARCOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
6	LA LIBERTAD	SANTA TECLA	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
7	LA LIBERTAD	SANTA TECLA	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
8	LA LIBERTAD	SANTA TECLA	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
9	LA LIBERTAD	SANTA TECLA	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
10	LA LIBERTAD	SANTA TECLA	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
11	LA LIBERTAD	SANTA TECLA	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
12	LA LIBERTAD	SANTA TECLA	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
13	SAN SALVADOR	MEJICANOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
14	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
15	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
16	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
17	SAN SALVADOR	SOYAPANGO	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
18	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
19	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
20	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
21	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
22	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
23	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
24	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
25	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
26	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
27	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
28	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
29	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
30	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
31	SAN	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)

	SALVADOR		
32	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
33	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
34	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
35	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
36	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
37	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
38	SAN SALVADOR	SOYAPANGO	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
39	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
40	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
41	SAN SALVADOR	MEJICANOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
42	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
43	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
44	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
45	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
46	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
47	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
48	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
49	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
50	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
51	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
52	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
53	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
54	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
55	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
56	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
57	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
58	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)

59	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
60	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
61	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
62	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
63	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
64	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
65	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
66	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
67	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
68	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
69	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
70	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
71	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
72	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
73	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
74	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
75	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
76	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
77	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
78	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
79	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
80	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
81	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
82	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
83	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
84	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
85	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
86	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)

87	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
88	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
89	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
90	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
91	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
92	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
93	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
94	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
95	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
96	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
97	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
98	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
99	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
100	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
101	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
102	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
103	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
104	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
105	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
106	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
107	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
108	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
109	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
110	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
111	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
112	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
113	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
114	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)

115	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
116	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
117	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
118	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
119	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
120	SAN SALVADOR	SOYAPANGO	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
121	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
122	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
123	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
124	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
125	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
126	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
127	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
128	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
129	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
130	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
131	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
132	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
133	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
134	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
135	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
136	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
137	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
138	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
139	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
140	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
141	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
142	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)

143	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
144	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
145	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
146	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
147	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
148	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
149	SAN SALVADOR	MEJICANOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
150	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
151	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
152	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
153	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
154	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
155	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
156	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
157	SAN SALVADOR	SAN MARTIN	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
158	LA LIBERTAD	ANTIGUO CUSCATLAN	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
159	LA LIBERTAD	ANTIGUO CUSCATLAN	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
160	LA LIBERTAD	ANTIGUO CUSCATLAN	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
161	LA LIBERTAD	ANTIGUO CUSCATLAN	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
162	SAN SALVADOR	APOPA	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
163	LA LIBERTAD	ANTIGUO CUSCATLAN	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
164	LA LIBERTAD	ANTIGUO CUSCATLAN	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
165	LA LIBERTAD	ANTIGUO CUSCATLAN	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
166	LA LIBERTAD	ANTIGUO CUSCATLAN	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
167	LA LIBERTAD	ANTIGUO CUSCATLAN	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
168	LA LIBERTAD	ANTIGUO CUSCATLAN	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
169	SAN SALVADOR	SAN MARTIN	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
170	SAN SALVADOR	MEJICANOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)

171	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
172	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
173	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
174	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
175	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
176	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
177	LA LIBERTAD	ANTIGUO CUSCATLAN	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
178	LA LIBERTAD	ANTIGUO CUSCATLAN	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
179	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
180	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
181	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
182	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
183	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
184	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
185	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
186	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
187	SAN SALVADOR	MEJICANOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
188	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
189	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
190	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
191	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
192	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
193	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
194	LA LIBERTAD	ANTIGUO CUSCATLAN	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
195	LA LIBERTAD	ANTIGUO CUSCATLAN	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
196	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
197	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
198	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)

199	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
200	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
201	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
202	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
203	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
204	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
205	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
206	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
207	LA LIBERTAD	ANTIGUO CUSCATLAN	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
208	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
209	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
210	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
211	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
212	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
213	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
214	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
215	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
216	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
217	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
218	SAN SALVADOR	SAN SALVADOR	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)

Directorio Económico 2016 según la base de datos de la Dirección General de Estadísticas y Censo