UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

"METODOLOGÍA DE GESTIÓN DE RIESGOS PARA LA PROTECCIÓN DE DATOS DE UN DESPACHO CONTABLE Y DE SUS CLIENTES, UBICADO EN EL DEPARTAMENTO DE SAN SALVADOR".

TRABAJO DE INVESTIGACIÓN PRESENTADO POR:

BATRES MELGAR, KATERIN LISSETH.

BERNAL RAMÍREZ, SANDY MAYARETH.

RODRÍGUEZ LÓPEZ, KATHERINE ESMERALDA.

PARA OPTAR AL GRADO DE:

LICENCIATURA EN CONTADURÍA PÚBLICA.

OCTUBRE, 2023

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES

RECTOR	**:**	Ing. Juan Rosa Quintanilla
VICERRECTORA ACADÉMICA	**:**	Dra. Evelyn Beatriz Farfán Mata
SECRETARIO GENERAL	**:**	Lic. Pedro Rosalío Escobar Castaneda
DECANA DE LA FACULTAD DE CIENCIAS ECONÓMICAS	**:**	Licda. Celina Amaya de Calderón
SECRETARIO DE LA FACULTAD DE CIENCIAS ECONÓMICAS	**:**	Lic. Pedro Javier Rivas Mejía
DIRECTOR DE LA ESCUELA DE CONTADURÍA PÚBLICA	**:**	Msc. Mauricio Ernesto Magaña Menéndez
COORDINADOR GENERAL DE PROCESOS DE GRADO	**:**	Msc. Ronald Edgardo Gálvez Rivera
COORDINADOR DE PROCESOS DE GRADUACIÓN DE LA ESCUELA DE CONTADURÍA PÚBLICA	**:**	Lic. Daniel Nehemías Reyes López
DOCENTE ASESOR	**:**	Msc. Wilmer Edmundo Pérez Díaz
TRIBUNAL EVALUADOR	**:**	Msc. Wilmer Edmundo Pérez Díaz
		Msc. Jorge Luis Martínez Bonilla
		Lic. Ernaldo de Jesús Ramos de la Cruz

AGRADECIMIENTOS

Primeramente, le agradezco a Jehová Dios por darme sabiduría durante todo este proceso, a mis padres Noé Batres y Yanira Melgar, a mis hermanos y hermanas, por brindarme su apoyo incondicional, amor e inspirarme a seguir adelante y a mi amiga Ethel, por su apoyo y motivación para continuar a pesar de las dificultades que surgen en el camino, y a mis compañeras y amigas que forman parte de este trabajo de graduación, por su esfuerzo, dedicación y no darse por vencidas ante ningún obstáculo.

Katerin Lisseth Batres Melgar.

Agradezco primeramente a Dios por el respaldo y la sabiduría brindada durante todo este proceso y sobre todo por ser el pilar de mi vida, asimismo, agradezco a mis padres Aida Esmeralda López Arévalo y a Jorge Alberto Rodríguez por su amor y apoyo incondicional a lo largo de todo este proceso, a mis hermanos y sobrino porque siempre me animaron con sus palabras de aliento en este proceso. Agradezco a un amigo muy especial por su cariño, apoyo y sobre todo por estar siempre a mi lado, además, agradezco a mi compañeras y amigas por su esfuerzo y apoyo a lo largo de esta dura y gran experiencia.

Katherine Esmeralda Rodríguez López.

Primeramente, agradecer a Dios por darme la sabiduría, entendimiento y fortaleza para culminar con mi carrera, mi familia, en especial a mis padres que siempre han estado pendiente del alcance de mis estudios, mis mejores amigos que me han motivado con sus palabras de aliento y a mi equipo de trabajo de investigación con las cuales he formado lazos de amistad por su apoyo, paciencia y perseverancia para alcanzar nuestro objetivo en el proceso académico.

Sandy Mayareth Bernal Ramírez.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN EJECUTIVO

Los despachos contables son entidades que se dedican a la prestación de servicios de contabilidad, estos manejan una gran cantidad de información de terceros ofreciendo a las empresas servicios que pueden ir desde asesorías, cumplimiento de obligaciones fiscales, planes de organización, contabilidad, elaboración y presentación de planillas de ISSS y AFP, trámites de legalización e inscripción de sociedades, hasta diagnósticos de la situación contable del negocio, entre otros.

Por lo tanto, en el caso de los despachos contables es importante la implementación de metodologías de gestión de riesgos para la protección de datos de la entidad y de sus clientes debido a que estas tienen la finalidad de proporcionar una orientación y ser una guía de aplicación para gestionar los riesgos a los que puede estar expuesta la información confidencial que manejan a causa de factores internos y externos. A partir de la incorporación de estas metodologías, los despachos se benefician puesto que en ella se determinan controles de mitigación de las amenazas identificadas en la empresa y se definen políticas de seguridad de la información y procedimientos que contribuyen a la minimización de los riesgos identificados.

La investigación está orientada al diseño de una metodología de gestión de riesgos para la protección de datos de un despacho contable y de sus clientes con el fin de realizar una evaluación de los riesgos que pueden afectar la seguridad de la información y asignar controles de mitigación que reduzcan o disminuyan las probabilidades de ocurrencia y el impacto que tendrían en la entidad.

La investigación se desarrolló utilizando el enfoque cualitativo mediante el método hipotético inductivo. El instrumento que sirvió de base para la recolección de información

consistió en una serie de interrogantes abiertas y planteadas de forma clave por medio de la técnica de entrevista, a la unidad de análisis en este caso, al socio del despacho contable, a fin de obtener información de la situación actual de la entidad con respecto a la temática de estudio.

Los resultados obtenidos por medio de la entrevista indican que el despacho contable no cuenta con un proceso de evaluación de riesgos que contemple las probabilidades de ocurrencia e impacto de las amenazas y que establezca, además, los respectivos controles de mitigación de estas. Por otra parte, en cuanto a políticas de seguridad se observa que la compañía carece de un documento formal debidamente aprobado por la alta dirección que contenga políticas y procedimientos que garanticen a los clientes el buen manejo y resguardo de la información.

Mediante los resultados obtenidos en la entrevista, expuestos en el párrafo precedente, se concluye que el despacho contable debe implementar una metodología de gestión de riesgos para la protección de datos que les ayude a prevenir y controlar la ocurrencia de los riesgos asociados a la seguridad de la información.

Tomando en cuenta lo anterior, se recomienda la implementación de una metodología de gestión de riesgos para la protección de datos, que le permita al despacho contable una gestión adecuada de los riesgos y que establezca políticas y procedimientos para garantizar la seguridad de la información que este maneja. Además, se sugiere que se implemente una cultura de capacitaciones al personal, enfocada en el tema de prevención de riesgos que amenacen la seguridad de los activos de información.

INTRODUCCIÓN

La gestión de riesgos para la protección de datos permite a las entidades identificar las amenazas a las que se puede ver expuesta la información confidencial que se maneja, de tal forma que se implementen medidas para evitar o subsanar estas situaciones. El presente trabajo contiene el desarrollo de un estudio basado en la importancia de la implementación de salvaguardas para la seguridad de la información de un despacho contable y de sus clientes, por lo que se ha diseñado una metodología con el fin de promover la adopción y desarrollo de procedimientos y políticas para el resguardo de esta.

Este documento consta de tres capítulos: el capítulo I aborda el planteamiento del problema y el marco teórico, el capítulo II contiene la metodología de la investigación y en el capítulo III se presenta la propuesta de una metodología de gestión de riesgos para la protección de datos de un despacho contable y de sus clientes.

El capítulo I está compuesto por el planteamiento del problema, en el cual están plasmados los antecedentes, la caracterización y la formulación de este, así como también, los objetivos de la investigación, los cuales se muestran de manera general y específica. Posteriormente, se presenta el marco teórico, en el cual se destacan aspectos como los antecedentes de la gestión de riesgos, generalidades, características, principios y beneficios de la implementación de las metodologías de gestión de riesgos para la protección de datos. Además, en el marco conceptual se definen los principales conceptos relacionados con el tema de investigación; el marco técnico y legal está conformado por todas aquellas normativas, leyes y regulaciones que sirven para el sustento de la investigación.

El capítulo II aborda la metodología de la investigación, en este se presentan el enfoque y tipo de estudio, el universo y muestra tomados para el desarrollo de la investigación, la unidad de análisis a quien se le ha dirigido una entrevista para identificar la situación de la entidad con relación a la temática de este trabajo, se definen los instrumentos y técnicas utilizados, las variables e indicadores, entre otros aspectos. También se muestran los resultados obtenidos por medio de la entrevista y su respectivo diagnóstico.

El capítulo III se compone por la propuesta de solución la cual consiste en una metodología de gestión de riesgos para la protección de datos de un despacho contable y de sus clientes integrada principalmente por una evaluación de riesgos y sus respectivos controles de mitigación, y, además, por políticas y procedimientos diseñados acorde a la evaluación antes mencionada y a las necesidades de la entidad.

CAPÍTULO I. PLANTEAMIENTO DEL PROBLEMA Y MARCO TEÓRICO

1.1 Planteamiento del problema

1.1.1 Antecedentes del problema

La protección de datos en algunos países tuvo mayor auge hace algunos años, debido a que las consultas de servicios de información en las páginas de internet y programas de navegación provocaron que existieran grandes flujos de datos sin límites por todo el mundo, por lo que esto produjo que diversas herramientas informáticas permitieran rastrear, filtrar información, y que además, las compañías de alta tecnología y usuarios se vieran inmersos a una falta de defensa legal por la carencia de normas, siendo este el motivo de la creación del Reglamento General de Protección de Datos, en adelante (RGPD), el cual entró en vigor el 24 de mayo de 2016, por parte de la Unión Europea; ante la problemática, se debía tomar nuevas medidas de control para proteger los datos personales y la libre circulación (Osorio, 2018).

A nivel global, de acuerdo con los resultados que presenta la Encuesta Global de Gestión en Riesgos 2021 realizada por una compañía británica proveedora de servicios de gestión de riesgos, llamada AON, cuyo nombre proviene de la palabra galesa *"oneness"*, y que traducida al español significa "unidad", los ataques cibernéticos y fuga de datos es uno de los cinco riesgos actuales que enfrentan las empresas alrededor del mundo (AON, 2022).

En la región de Latinoamérica, la protección de datos personales ha sido un escenario complejo, debido a que los estándares sobre este tema no habían sido lo suficientemente rigurosos como en Europa. Algunos países como Argentina, Uruguay, México, Perú, entre otros, desarrollaron sus leyes de protección de datos a partir del año 2000, siendo influenciados por la visión sobre el derecho a la privacidad de la Unión Europea. Posteriormente, con la entrada en

vigor del RGPD, en el año 2018 muchas naciones procedieron a realizar reformas a sus leyes de protección de datos, tomando como base dicho reglamento, y de esta forma fortalecer sus acciones en cuanto al resguardo de información confidencial (Enríquez, 2021).

Asimismo, en Centroamérica, surgieron diversas circunstancias en las que también los países que lo conforman se encontraron en la necesidad de adoptar medidas para la prevención de pérdida de información confidencial.

En el año 2022, El Salvador ocupa el puesto 100 en el Índice Mundial de Innovación, publicado anualmente por la Organización Mundial de la Propiedad Intelectual en adelante (WIPO, por sus siglas en inglés *World Intellectual Property Organization)*. Este índice revela cuáles son las economías más innovadoras del mundo, para ello se utilizan indicadores como: medidas sobre el entorno político, la educación, las infraestructuras y el crecimiento económico, posicionando a la nación salvadoreña como un país atrasado en las nuevas tecnologías e innovación que surgen año con año, como por ejemplo la incorporación del *blockchain*, que es una herramienta tecnológica a nivel mundial la cual ha empezado a estudiar diferentes usos, como las transacciones de datos, procesos que involucran la protección de información, entre otros (Dutta, Lanvin, Rivera, & Wunsch, 2022).

Por otra parte, algunos expertos opinan que los negocios con mayores riesgos de sufrir ciberataques, robo o fuga de información son aquellos de menor tamaño, como puede ser el caso de despachos contables que tienen en su poder cantidades importantes de datos pero que, por su tamaño, no implementan medidas de protección por no considerarse vulnerables a sufrir este tipo de situaciones (Mallet, 2019).

Conservar la imagen y prestigio de los clientes puede ser el valor agregado de algunas entidades, para ello se deben tener presente los factores de alto riesgo debido a que, en la actualidad, el comercio electrónico es uno de los más utilizados, por lo que existe la posibilidad de que los datos brindados como información personal, medios de pagos, direcciones de envío o facturación, sean altamente vulnerables para fraudes y robos.

Por lo tanto, los despachos contables tienen la obligación de garantizar la protección de datos de sus clientes debido a que existe un principio de confidencialidad que rige al profesional de la contaduría pública establecido en el Código de Ética, es por ello que deben adoptar medidas para dar cumplimiento a tal deber y mantener el resguardo de la información recibida y que le ha sido confiada para los fines pertinentes de los servicios profesionales que se prestan en la entidad, de tal manera que se reduzca el riesgo de una posible pérdida o divulgación de esta.

El Código de Ética para el Profesional de Contaduría Pública, edición 2018, desarrollado y aprobado por el Consejo de Normas Internacionales de Ética para Contadores, en adelante (IESBA), y adoptado por el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría en adelante (CVPCPA), para su implementación en El Salvador a partir del 1 de julio de 2020, promulga una guía aplicable al profesional de la contabilidad, marco conceptual y una serie de principios por los que se deben de regir los contadores públicos, precisamente uno de ellos es la confidencialidad que deben poner en práctica cuando se trata del manejo de información de sus clientes.

El 28 de abril del año 2021, la Asamblea Legislativa de la República de El Salvador, entregó al presidente de la República, el Decreto Legislativo No. 875 aprobado el 22 del mismo mes y año, este contenía la Ley de Protección de Datos Personales la cual tendría por objeto: *"La protección de los datos personales de las personas naturales o jurídicas de carácter privado o*

público, con la finalidad de regular su tratamiento legítimo e informado, para garantizar el derecho a la intimidad y el derecho a la autodeterminación informativa de las personas naturales".

Este decreto fue vetado por el presidente de la República el 7 de mayo del 2021 por considerarlo inconveniente, y, por tanto, fue devuelto al Órgano Legislativo (Asamblea Legislativa de El Salvador, 2021). Al año 2022, el país no cuenta con directrices legales para la regulación del resguardo de datos confidenciales.

1.1.2 Caracterización del problema

La protección de información personal de los clientes que manejan los profesionales de la contaduría pública hace referencia al desarrollo de prácticas, salvaguardas y principios fundamentales para proteger los datos confidenciales de cada uno de estos.

La implementación de procedimientos para la protección de información financiera se caracteriza porque se emplean salvaguardas razonables de seguridad para proteger los datos confidenciales contra riesgos, tales como pérdida, accesos no autorizados, destrucción, uso, modificaciones o divulgación de estos.

En ese sentido, la información financiera de los clientes que se maneja en los despachos contables muestra los movimientos de todas las áreas de trabajo de estos; todo dato reflejado en los estados financieros es útil para la toma de decisiones desde el punto de vista económico y financiero. En tiempos pasados se realizaba la contabilidad de forma manual, haciendo que esta fuera poco eficiente y vulnerable a la pérdida de datos. Posteriormente a medida ha transcurrido el tiempo, se han creado diferentes softwares contables encaminados al resguardo y protección de datos, por lo que las entidades se han visto en la necesidad empresarial de mantener el debido

control de la información y que no existan desviaciones de estas, a raíz de dichos acontecimientos las oficinas contables han ido modernizando sus métodos de trabajo en el mundo.

El área contable es uno de los ámbitos más beneficiados de la aplicación de los avances tecnológicos en materia de software de finanzas y contabilidad, debido a que contribuyen a que los registros sean más eficientes. Además, garantizan la veracidad de la información y permiten automatizar procesos para disponer de los estados financieros de forma más eficaz, eficiente, así como también, aseguran el resguardo de la información confidencial de los clientes.

La información de los clientes resulta de suma importancia para las empresas puesto que están en el compromiso de proteger la privacidad de los datos que les proporcionan a partir del momento de la obtención y resguardo de estos. Para ello, las entidades deben tener en cuenta políticas de privacidad, contratos de aceptación de términos sobre el manejo de la información, transparencia e inscripción en el registro nacional para protección de datos, en el caso que haya una institución que esté al tanto de su existencia y responsabilidad.

Los servicios del despacho objeto de este estudio, consisten en el registro contable de todas las transacciones de una empresa, así como la elaboración de los reportes financieros y tributarios mensuales y anuales, gestión de trámites administrativos, declaraciones de IVA, pago a cuenta e ISR, elaboración y presentación de planillas de ISSS y AFP’s, legalización e inscripción de empresas, elaboración y legalización de sistemas contables, entre otros.

Mediante consultas realizadas a uno de los socios del despacho contable, se ha identificado que la entidad no cuenta con procedimientos para la protección de datos para solventar aquellos riesgos a los que pueda enfrentarse en cuanto a la seguridad de la información, no hace uso de los medios correctos para la comunicación con sus clientes cuando se trata de aspectos confidenciales,

por lo que esto puede provocar el robo o fuga de datos, demandas por parte de la clientela, mala reputación y pérdida de credibilidad.

1.1.3 Formulación del problema

Uno de los principios éticos aplicables a los profesionales de contaduría pública, es la confidencialidad, la cual es sumamente importante cuando se trata del manejo de información confidencial de clientes en los despachos contables, pero si no se aplican procedimientos, surge la siguiente interrogante:

¿De qué manera puede afectar al despacho contable no contar con una metodología de gestión de riesgos para la protección de datos y de sus clientes?

1.2 Objetivos de la investigación

1.2.1 Objetivo general

Diseñar una metodología de gestión de riesgos para la protección de datos y de clientes de un despacho contable ubicado en el municipio de Mejicanos, departamento de San Salvador, que contribuya al resguardo de la información confidencial que manejan.

1.2.2 Objetivos específicos

- Determinar mediante un diagnóstico la forma en que la entidad resguarda la información confidencial propia y de sus clientes.
- Identificar los riesgos que puedan afectar la seguridad de la información manejada por el despacho contable.

- Realizar una valoración de los riesgos a partir de la probabilidad de ocurrencia e impacto que estos puedan generar en la entidad, para asignar procedimientos y controles de mitigación de este tipo de eventos.

1.3 Marco teórico

1.3.1 Antecedentes de la gestión de riesgos

La gestión de riesgos ha estado presente desde hace muchos años como una herramienta para generar una cultura preventiva, sin embargo, ha venido cambiando de acuerdo con el entorno, con su aplicabilidad y con los resultados que ha mostrado en los sectores donde se ha incorporado (Aliados en tecnología S.A.S., n.d.).

La ISO 27000 fue publicada el 1 de mayo de 2009, revisada con una segunda edición en diciembre de 2012, una tercera edición en enero de 2014 y una cuarta en febrero de 2016. Esta norma proporciona una visión general de las normas que componen la serie 27000, recoge todas las definiciones y aporta las bases de por qué es importante la implantación de un Sistema de Gestión de Seguridad de la Información (en adelante SGSI), introducción y una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (ISO 27000 ES, n.d.).

La ISO 27001 es la norma principal de la serie y contiene los requisitos del SGSI, su última versión fue publicada en el año 2018 con el fin de proporcionar confidencialidad, integridad y disponibilidad de la información, así como cumplimiento legal.

Ante la necesidad de certificar la gestión de la privacidad en el entorno empresarial, como extensión de la norma 27001, fue publicada el 6 de agosto de 2019 la Norma ISO 27701: 2019, Sistema de Gestión de Privacidad de la Información (EQA, 2019).

1.3.2 Generalidades

- **Gestión de riesgos**

El análisis de los riesgos identificados permite a la entidad conocer qué les podría ocurrir a sus activos si no se protegen de una forma adecuada (Grupo ESGiinova, 2018). En ese sentido, la gestión de este tipo de eventos consiste en la selección e implementación de medidas para salvaguardar, impedir, prevenir, reducir o controlar todas las amenazas que han sido identificadas en la empresa. Estas actividades, permiten elaborar un plan de seguridad que satisfaga todos los objetivos propuestos por la entidad para la protección de sus activos.

Para iniciar un proceso de gestión de riesgos es importante tener en cuenta tres aspectos:

- **Identificación de riesgos:** proceso que consiste en identificar y evaluar las amenazas y vulnerabilidades de una entidad, sus operaciones y su fuerza laboral. “Por ejemplo, la identificación de riesgos puede incluir la evaluación de amenazas de seguridad de tecnologías de la información como malware y ransomware, accidentes, desastres naturales y otros eventos potencialmente dañinos que podrían interrumpir las operaciones comerciales” (IBM, s.f.).
- **Análisis y evaluación de riesgos**: “El análisis de riesgos implica determinar la probabilidad de que se produzca un suceso de riesgo, así como el resultado potencial de cada suceso. La evaluación de riesgos compara la magnitud de cada riesgo y los clasifica según su importancia y sus consecuencias” (IBM, s.f.).
- **Monitoreo y mitigación de riesgos:** este proceso hace referencia a la planificación y desarrollo de métodos y opciones para reducir las amenazas a determinada área de una entidad. La mitigación de riesgos también incluye acciones a implementar para tratar los problemas y sus posibles efectos (IBM, s.f.).

La ISO 27001, constituye una herramienta de gestión de riesgos y establece que los métodos para la evaluación de estos deben contener estrategias sobre el tratamiento que se les debe aplicar y los controles que deben implementarse, con el fin de garantizar la seguridad de la información (Russell & NQA, s.f.).

Por otra parte, la ISO 27005, ofrece una guía de orientación para el desarrollo de una técnica de evaluación de riesgos, la cual debe contener los siguientes elementos clave:

1. "Proporcionar aviso para la identificación sistemática de riesgos (revisión de activos, grupos de activos, procesos, tipos de información), verificando la presencia de amenazas y vulnerabilidades comunes y registrando los controles que actualmente tiene implementados para administrarlos" (Russell & NQA, s.f.).
2. "Proporcionar un marco para evaluar la probabilidad de que el riesgo ocurra de manera persistente (una vez al mes, una vez al año)" (Russell & NQA, s.f.).
3. Proporcionar un marco para evaluar las consecuencias de cada riesgo que ocurra de manera consistente (Russell & NQA, s.f.).
4. "Proporcionar un marco para calificar o categorizar cada riesgo identificado (por ejemplo, alto/medio/bajo), teniendo en cuenta su evaluación de probabilidad y las consecuencias" (Russell & NQA, s.f.).
5. "Establecer criterios documentados que especifiquen, para cada categoría de riesgo, qué tipo de acción debe tomarse y el nivel o prioridad que se le asigna" (Russell & NQA, s.f.).

- **Protección de datos en las entidades**

La protección de datos se basa en una serie de prácticas, principios y medidas que ponen en marcha las empresas con el propósito de resguardar todo lo relacionado a sus clientes. Las empresas conforme van creciendo comienzan a crear, administrar y almacenar grandes grupos de información lo cual es sumamente necesario salvaguardar, por lo que, como parte de la seguridad, se deben implementar políticas y procedimientos que contribuyan al adecuado manejo de esta.

Los despachos contables, son entidades que manejan una gran cantidad de información de terceros; estos *"*ofrecen a las empresas servicios de contabilidad que pueden ir desde asesorías, cumplimiento de obligaciones fiscales, plan de organización, contabilidad, nóminas, impuestos, trámites, hasta diagnósticos de la situación contable del negocio" (Despacho Contable Monzón y Padilla, 2020).

Se considera protección de datos al conjunto de acciones coordinadas y encaminadas a su salvaguarda y tranquilidad aportando beneficios mutuos tanto para la empresa como para los clientes.

La protección de datos se caracteriza por emplear metodologías y tecnologías para salvaguardarlos, ponerlos a disposición de los usuarios autorizados en cualquier circunstancia y por el principio de confidencialidad, que obliga a resguardar la información intercambiada entre un emisor y un receptor frente a terceros. Para ello, los empresarios deben pensar y tomar todas las medidas de seguridad necesarias para garantizar la privacidad digital, y así cumplir con el propósito de evitar accesos no autorizados a los datos sensibles, que se encuentran alojados en las computadoras, bases y páginas web de las organizaciones (Grupo Ático 34, 2022).

Para Martínez Villena (2022), existen tres principios básicos para la protección de datos de clientes:

- ***Confidencialidad.*** Garantiza su accesibilidad únicamente a las personas autorizadas para tener acceso a la información.
- ***Integridad.*** Implica que los datos sean correctos y estén libres de cualquier modificación y error contribuyendo a su originalidad.
- ***Disponibilidad.*** La información debe estar disponible para el personal autorizado siempre que sea necesario.

Las entidades están acelerando su transición a implementaciones de herramientas tecnológicas o metodologías para la protección de datos. Al mismo tiempo, la información digital está creciendo rápidamente y las empresas dependen cada vez más de los sistemas informáticos para todos los aspectos de sus operaciones, lo que está generando un entorno en el que el resguardo de esta debe ser la máxima prioridad para los líderes empresariales (Martínez, 2022).

Dentro de los beneficios de la implementación de herramientas tecnológicas o de metodologías para la protección de datos se encuentran los siguientes:

- Aumenta la competitividad y calidad de trabajo en las organizaciones.
- Mejora la seguridad de la información objeto de tratamiento en las empresas, garantizando su integridad, confidencialidad y disponibilidad.
- Evita vulnerabilidades, al mejorar la seguridad de información y la gestión documental de toda empresa consiguiendo un control más eficaz no solo de datos de terceros, sino también, de la empresa.

- Ofrece confianza a los clientes, haciéndolos sentir más tranquilos y satisfechos con la entidad.
- Permite mantener la protección y seguridad de los datos en las compañías contribuyendo a proyectar una buena imagen tanto de la empresa, en general, como de sus trabajadores.
- Evita la pérdida de información sensible y las consecuencias que ello conlleva. Las fugas de información, así como las brechas de seguridad, pueden provocar grandes daños: perder activos, la confianza de los clientes, difamación de la empresa, pérdida de la reputación e incluso, cierre de la entidad, por lo que proteger los datos evita o previene esos daños.

1.4 Marco conceptual

Una metodología de gestión de riesgos para la protección de datos de clientes y del despacho se vuelve fundamental para identificar los activos de información, evaluar amenazas y controlar los riesgos a través de medidas de mitigación, políticas y procedimientos, con el fin de prevenir posibles vulnerabilidades. A continuación, se presentan los principales conceptos utilizados en esta investigación con la finalidad de facilitar la compresión de los lectores.

- **Datos personales:** es la información privada concerniente a una persona, identificada o identificable, relativa a su nacionalidad, domicilio, patrimonio, dirección electrónica, número telefónico u otra similar (Asamblea Legislativa de El Salvador, 2016).

- **Activo de información:** es todo aquello que tiene algún valor para la organización y, por ende, debe protegerse. Los activos pueden ser tangibles o intangibles.

- **Protección de datos:** es el proceso de salvaguardar información importante contra corrupción, filtraciones, pérdida o compromiso de los datos (Hefner et al., 2021).

- **Fuga de datos:** se denomina fuga de información al incidente (tanto interno como externo, y a la vez intencional o no) que pone en poder de una persona ajena a la organización, información confidencial y que sólo debería estar disponible para integrantes de la misma (Sebastián Bornik, 2010).

- **Seguridad de la información**: se entiende el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información (Tecón, s.f.).

- **Riesgos:** proximidad o posibilidad de que suceda un daño o perjuicio y sus posibles consecuencias (Editorial Etecé, 2021).

- **Gestión de riesgos:** es la selección e implementación de salvaguardas para conocer, prevenir, impedir, reducir o controlar todos los riesgos que han sido identificados (Grupo ESGiinova, n.d.).

- **Evaluación de riesgos:** proceso de identificación de riesgos, analizando el nivel de cada uno en particular y evaluando acciones adicionales necesarias para reducir dichos riesgos a niveles aceptables (Russell & NQA, s.f.)

- **Matriz de riesgos:** es una herramienta de gran utilidad para gestionar y controlar los riesgos (amenazas y vulnerabilidades) que pueden presentarse en la operación, en la implementación de servicios, en seguridad o en cualquier otro proceso de la empresa (Jiménez, 2022).

1.5 Marco técnico

Para el desarrollo de esta investigación se han tomado de referencia las siguientes bases técnicas a través de las cuales se fundamenta este estudio:

1.5.1. Código de Ética para el Profesional de Contaduría Pública

Promulga una guía aplicable al profesional de la contaduría pública, marco conceptual y una serie de principios por los que se deben de regir los contadores públicos, precisamente uno de ellos es la confidencialidad, la cual deben poner en práctica cuando se trata del manejo de información de sus clientes.

El Código Internacional de Ética para Profesionales de la Contabilidad establece que el profesional de la contabilidad debe cumplir con el principio de confidencialidad lo cual implica respetarlo y llevarlo a la práctica cuando se trata del manejo de la información obtenida como resultado de sus relaciones profesionales y empresariales (Consejo de Normas Internacionales de Ética para Contadores, 2018).

El Código Internacional de Ética para Profesionales de la Contabilidad (2018, p. R114.1), establece que el profesional de la contabilidad:

a. Estará atento a la posibilidad de una divulgación inadvertida, incluido en un entorno no laboral, y en especial a un socio cercano, a un familiar próximo o a un miembro de su familia inmediata:
b. Mantendrá la confidencialidad de la información dentro de la firma o de la entidad para la que trabaja;

c. Mantendrá la confidencialidad de la información revelada por un potencial cliente o por la entidad para la que trabaja;
d. No revelará información confidencial obtenida como resultado de relaciones profesionales y empresariales ajenas a la firma o a la entidad para la que trabaja, salvo que medie una autorización adecuada y específica o que exista un deber o derecho legal o profesional para su revelación;
e. No utilizará información confidencial obtenida como resultado de relaciones profesionales y empresariales en beneficio propio o de terceros;
f. No utilizará ni revelará información confidencial alguna, obtenida o recibida como resultado de relaciones profesionales y empresariales, después de finalizar la relación; y,
g. Tomará medidas razonables para asegurar que el personal bajo su control y las personas de las que obtiene asesoramiento y apoyo respetan el deber de confidencialidad del profesional de la contabilidad.

1.5.2. Guía de Implantación de la ISO 27001, Sistemas de Gestión de Seguridad de la Información

La ISO 27001, es la norma internacional orientada hacia los Sistemas de Gestión de Seguridad de la información, en adelante (SGSI), la cual proporciona un marco de protección de información que puede ser adaptado a todo tipo de organizaciones, independientemente de su tamaño.

Es una norma internacional que proporciona el aseguramiento, la confidencialidad e integridad de los datos y de la información, asimismo, de los sistemas que la procesan (Grupo ESGinnova, s.f.).

Un SGSI tiene como objetivo principal proporcionar protección a la información sensible o valiosa; la primera puede incluir información sobre empleados, clientes y proveedores; y la segunda puede incorporar propiedad intelectual, datos financieros comerciales y operativos, y registros legales (Russell & NQA, s.f.).

1.5.3. Guía de Implantación de la ISO 27005, Gestión de Riesgos de la Seguridad de la Información.

Es el estándar internacional orientado a la gestión de riesgos de seguridad de la información. Esta norma es aplicable a todo tipo de entidades que estén interesadas en gestionar las vulnerabilidades que pueden afectar el resguardo de los datos debido a que suministra diversas directrices y recomendaciones, apoyándose principalmente de los requerimientos del SGSI definidos en la ISO 27001 (ISOTools Excellence, 2014).

La ISO 27001, establece que el núcleo de todo SGSI eficaz es la evaluación de riesgos, es por ello que mediante la ISO 27005 se obtiene una orientación para el desarrollo de una técnica orientada a este proceso, puesto que esta norma no proporciona una metodología en concreto, por lo que establece una serie de elementos clave que se deben tomar en cuenta al momento de desarrollar una determinada técnica (Russell & NQA, s.f.).

1.5.4. Guía de Implantación de la ISO 27701, Sistema de Gestión de Privacidad de la Información

Esta norma es una extensión de la ISO 27001, en materia de privacidad de datos, debido a que se basa en los requisitos, controles y objetivos de esta. La ISO 27701 especifica una serie de

requisitos para establecer, implementar, mantener y mejorar de forma continua un sistema de gestión de información de privacidad (Instituto Nacional de Ciberseguridad, 2019).

La aplicación de esta normativa permite a las organizaciones demostrar su compromiso con el SGSI a través de iniciativas de liderazgo y creación de políticas, roles, responsabilidades y orientación, además, para la aplicabilidad de esta, las entidades deben de evaluar riesgos de seguridad de la información para identificar los que están asociados con la pérdida de confidencialidad, integridad y disponibilidad.

Además, deben de garantizar a lo largo de los procesos de evaluación de riesgos que la relación entre seguridad de la información y la protección de la información personal se gestiona de forma adecuada.

1.5.5. Principios Actualizados sobre la Privacidad y la Protección de Datos Personales publicado por la Organización de Estados Americanos (OEA)

Es una publicación preparada para disposición del público acerca de los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, adoptados por el Comité Jurídico Interamericano (CJI) y aprobados por la Asamblea General de la OEA. Esta publicación proporciona principios que prevalecen en los Estados Miembros sobre temas centrales de la protección de datos, los cuales se detallan a continuación: (OEA, 2022).

- **Propósitos legítimos y justos:** Los datos personales deben ser recopilados solamente para fines legítimos y por medios justos y legales.
- **Claridad y consentimiento**: Se deben especificar los fines para los cuales se recopilan los datos personales en el momento en que se recopilen. Como regla general, los datos

personales solamente deben ser recopilados con el consentimiento de la persona a que se refieran.

- **Pertinencia y necesidad:** Los datos deben ser verídicos, pertinentes y necesarios para los fines expresos de su recopilación.
- **Uso limitado y retención:** Los datos personales deben ser mantenidos y utilizados solamente de manera legítima no incompatible con el fin o fines para los cuales se recopilaron. No deberán mantenerse más del tiempo necesario para su propósito o propósitos y de conformidad con la legislación nacional correspondiente.
- **Deber de confidencialidad**: Los datos personales no deben divulgarse, ponerse a disposición de terceros ni emplearse para otros propósitos que no sean aquellos para los cuales se obtuvieron, excepto con el conocimiento o consentimiento de la persona en cuestión o bajo autoridad de la ley.
- **Protección y seguridad:** Los datos personales deben ser protegidos mediante salvaguardas razonables y adecuadas contra accesos no autorizados, pérdida, destrucción, uso, modificación o divulgación.
- **Fidelidad de los datos:** Los datos personales deben mantenerse fieles y actualizados hasta donde sea necesario para los propósitos de su uso.
- **Acceso y corrección:** Se debe disponer de métodos razonables para permitir que aquellas personas cuyos datos personales han sido recopilados puedan solicitar el acceso a dichos datos y puedan solicitar al controlador de datos que los modifique, corrija o elimine. En caso de que fuera necesario restringir dicho acceso o corrección, deberían especificarse las razones concretas de cualquiera de estas restricciones de acuerdo con la legislación nacional.

- **Datos personales sensibles:** Los controladores de datos deberían adoptar medidas de privacidad y de seguridad que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los individuos sujetos de la información.
- **Responsabilidad:** Los controladores de datos adoptarán e implementarán las medidas correspondientes para el cumplimiento de estos principios.

1.6 Marco legal

1.6.1. Ley Reguladora del Ejercicio de la Contaduría

De conformidad a lo que establece el artículo 1, esta ley tiene por objeto la regulación del ejercicio de la profesión de la Contaduría Pública, la función de la fe pública auditora, los derechos de las personas naturales o jurídicas que la ejerzan. Además, se establece que: *"Las personas naturales o jurídicas que la ejerzan, dan fe plena y pública, sobre una base contable de Normas Internacionales de Contabilidad y Normas Internacionales de Auditoría, respectivamente, adoptadas y legalizadas por el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoria, que podrá denominarse el Consejo o CVPCPA"*.

En el último inciso del artículo 2 de la ley se establece que: *"Quienes ejerzan la contaduría y la función de la auditoria, además de cumplir con la normativa internacional de contaduría y de auditoría, deberán cumplir el Código de Ética para Profesionales de la Contabilidad y Auditoría, adoptado y legalizado por el Consejo y Norma de Educación Continuada emitida por el mismo"*.

El artículo anterior contempla la aplicación de normativas internacionales de contaduría y auditoría, así como del Código de Ética para Profesionales de la Contaduría y Auditoría adoptado

por el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría para su implementación en El Salvador a partir del 1 de julio de 2020.

1.6.2. Ley Especial contra Delitos Informáticos y Conexos

La presente ley tiene por objeto proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación, así como la prevención y sanción de los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, intimidad e imagen de las personas naturales o jurídicas en los términos aplicables y previstos en la Ley (Asamblea Legislativa de El Salvador, n.d.).

Esta ley contiene una serie de capítulos, en los cuales se encuentran los delitos informáticos relacionados con el contenido de los datos.

El artículo 26 de esta Ley establece que: *"El que sin el consentimiento del titular de la información de carácter privado y personal revele, difunda o ceda en todo o en parte, dicha información o datos a los que se refiere el presente artículo, sean éstos en imágenes, video, texto, audio u otros, obtenidos por alguno de los medios indicados en los artículos precedentes, será sancionado con prisión de tres a cinco años".*

1.7 Hipótesis del trabajo

La implementación de una metodología de riesgos para la protección de datos de un despacho contable y de sus clientes, contribuirá a que los profesionales de contaduría pública apliquen procedimientos que garanticen el adecuado manejo y resguardo de la información.

CAPÍTULO II: METODOLOGÍA DE LA INVESTIGACIÓN

2.1 Enfoque y tipo de estudio

2.1.1 Enfoque

La investigación se desarrolló bajo el enfoque cualitativo, debido a que se partió de la observación y estudio de la situación del despacho contable por medio de una entrevista realizada a la unidad de análisis, representada por un socio de la entidad. Este estudio permitió efectuar un diagnóstico sobre las deficiencias del negocio con el fin de desarrollar una metodología de gestión de riesgos para la protección de datos del mismo y de sus clientes, adaptada a sus necesidades y características específicas.

2.1.2 Tipo de estudio

El tipo de estudio fue hipotético – inductivo debido a que se partió de lo específico a lo general; a través de las fuentes bibliográficas consultadas fue posible formular diversas preguntas y con ello realizar una entrevista a fin de recopilar información que permitiera el desarrollo de una metodología de gestión de riesgos para la protección de datos del despacho contable y de sus clientes.

2.2 Delimitación espacial y temporal

2.2.1 Delimitación espacial

La investigación se realizó en un despacho contable ubicado en el municipio de Mejicanos, departamento de San Salvador.

2.2.2 Delimitación temporal

El periodo que comprendió la investigación corresponde del mes de julio a diciembre del 2022. Se optó por realizar el estudio en el periodo antes mencionado debido a que, en el 2021, el presidente de la República vetó el Decreto Legislativo No. 875 que contenía la Ley de Protección de Datos Personales, por lo que, en El Salvador, no se cuenta con mecanismos legales que regulen la protección de información confidencial.

2.3 Sujetos y objeto de estudio

2.3.1 Unidad de análisis

La unidad de análisis de la presente investigación es el socio a cargo de la entidad, esto debido a que es la persona que cuenta con la mayor capacidad en cuanto a conocimiento y experiencia dentro del despacho contable.

2.3.2 Universo y muestra

Debido a que la investigación se realizó bajo el método cualitativo, el universo se integró por un despacho contable, por lo tanto, no fue necesaria la determinación de una muestra. Este estudio servirá de apoyo para otras entidades de igual naturaleza.

2.3.3 Variables e indicadores

- **Variable independiente:** La metodología de gestión de riesgos para la protección de datos de un despacho contable y de sus clientes.
- **Variable dependiente:** Adecuado manejo y resguardo de la información por parte de los profesionales de la contaduría pública.

2.4 Técnicas e instrumentos

2.4.1 Técnicas

- **Entrevista**

Adicional a las consultas realizadas en las fuentes bibliográficas, se hizo uso de la entrevista, la cual fue dirigida al socio a cargo del despacho contable de manera presencial.

2.4.2 Instrumentos

- **Guía de preguntas**

Se utilizó como instrumento una guía de preguntas, la cual fue previamente diseñada, y que está conformada por una serie de interrogantes abiertas y planteadas de forma clave, a fin de obtener información de la situación actual del despacho contable con respecto a la implementación de medidas para la protección de datos y de sus clientes.

2.5 Cronograma de actividades

A continuación, se presenta el cronograma de actividades para el desarrollo de este trabajo de investigación, en el cual se reflejan cada uno de los pasos que se realizaron durante todo el proceso del seminario de trabajo de graduación, iniciando desde el anteproyecto de la investigación y finalizando con la entrega del documento final y la defensa de este.

Tabla 1

Cronograma de actividades

ACTIVIDADES	2022												2023																							
	Septiembre				Octubre				Noviembre				Diciembre				Enero				Febrero				Marzo				Abril				Mayo				Junio				Julio			
	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
Inicio de seminario de graduación																																											
Elaboración de anteproyecto																																											
Entrega del documento final del Anteproyecto																																											
Aprobación de anteproyecto																																											
CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA Y MARCO TEÓRICO																																											
Asesorías Capítulo I																																											
Entrega de Capítulo I																																											
CAPÍTULO II: METODOLOGÍA DE LA INVESTIGACIÓN																																											
Asesorías Capítulo II																																											
Entrega de Capítulo II																																											
CAPÍTULO III: PROPUESTA DE SOLUCIÓN																																											
Asesorías Capítulo III																																											
Entrega de Capítulo III																																											
ENTREGA DE TRABAJO FINAL																																											
DEFENSA DE TRABAJO DE GRADUACIÓN																																											

2.6 Presentación de los resultados

2.6.1 Tabulación y análisis de los resultados

Partiendo de la información obtenida mediante la entrevista dirigida al socio del despacho contable, se efectuó el análisis correspondiente, con el objetivo de conocer la situación actual de la entidad con respecto a la gestión de riesgos, aplicación de políticas y procedimientos para la protección de sus datos y de clientes. A continuación, se presentan los resultados:

Tabla 2

Análisis de la entrevista

	Pregunta	Respuesta	Análisis de la respuesta
1.	**¿Qué medios físicos e informáticos utilizan en el despacho contable para el resguardo de la información confidencial de la entidad y de sus clientes?**	Actualmente tenemos información y documentación de nuestros clientes en formato físico y digital; los documentos físicos se mantienen almacenados en archivadores dentro de una bodega, un pequeño espacio cerrado donde hay un mueble con diferentes cubículos para colocar los archivadores y cajas que contienen los documentos para su entrega o devolución a los clientes; por otra parte, la información y documentos digitales, se encuentran en nuestro servidor. La información propia, está almacenada en el equipo de uso de la jefatura. La bodega donde almacenamos los documentos físicos se encuentra a disposición de cualquier empleado.	Se identificó que, el despacho contable cuenta únicamente con un medio físico para el resguardo de información, en este caso, una bodega la cual no cumple con el adecuado nivel de seguridad puesto que cualquier empleado tiene acceso a ella. En lo que respecta a los medios informáticos, se indicó que poseen un servidor que está a cargo de la jefatura, donde almacenan la documentación e información; se considera que este medio puede ser susceptible a riesgos que ocasionen la pérdida total de los datos ahí almacenados.
2.	**¿Cuál es el proceso de autorización para solicitar información confidencial y modificar datos tales como contraseñas, usuarios, correos de los clientes y del despacho contable?**	Referente a los usuarios y contraseñas, se tiene manejo de los accesos de los clientes a la plataforma de los servicios en línea del Ministerio de Hacienda, éstos son entregados a la jefatura cuando contratan nuestros servicios y no se modifican a menos que el Representante Legal del	Se identificaron los procesos de autorización que realizan para solicitar información confidencial y modificar datos de los clientes y del despacho, sin embargo, se considera que, la utilización de un único correo al cual pueden acceder todos los empleados puede

		cliente lo solicite a la jefatura. Hay otros accesos que sólo maneja el despacho, debido a que, con un mismo usuario se gestiona información de varios clientes, por ejemplo, en el Sistema para la Elaboración de Planillas Previsionales (SEPP) y en la Oficina Virtual del ISSS (OVISSS), tales accesos solamente son gestionados por las personas autorizadas, en este caso, para la presentación de las planillas de algunos de los clientes. Respecto a los correos, nosotros actualmente manejamos solamente un correo, al que tienen acceso los empleados y que diariamente es revisado por la jefatura.	conllevar a riesgos de pérdida, desvío o manipulación indebida de la información puesto que las contraseñas no son cambiadas de manera periódica, ni aun cuando un empleado renuncia o es despedido de su cargo.
3.	**Según su experiencia, ¿qué tipo de información es más susceptible a amenazas de pérdida, robo o extravío?**	Los documentos físicos, éstos son muy susceptibles al deterioro con el paso del tiempo, esto debido al polvo, humedad y a la acción de otros agentes, insectos, por ejemplo, como termitas y lepismas.	Se identificó que, para el despacho contable únicamente la información almacenada en físico es susceptible a riesgos de pérdida, robo o extravío, no obstante, se considera que la información digital también puede serlo, debido a que existen amenazas como virus o malware, hackeos, fallos en discos duros, sobrecargas de energía, entre otras, que puede poner en riesgo la seguridad de la información confidencial.
4.	**¿Cómo contribuyen los socios del despacho a garantizar la protección de los datos que les han sido confiados por los clientes y la**	Verificando en coordinación con la jefatura (gerente financiero) la condición de los equipos (si necesitan algún mantenimiento o reemplazo) el estado de la bodega (si se	Se observó que el despacho contable cuenta con procedimientos empíricos para garantizar la protección de los datos,

	información del despacho?	necesita alguna mejora en el acondicionamiento) y que se estén efectuando respaldos periódicos de la información del servidor. Los respaldos periódicos de la información almacenada en el servidor se realizan mediante un disco externo.	puesto que no están documentados, además, estos son limitados debido a que no han tomado en cuenta los diversos riesgos que pueden conllevar a la pérdida, robo o extravío de la información. Asimismo, se denota que se enfocan más en la protección de la información física y no toman el debido interés que requiere el resguardo de la información digital.
5.	**¿Cuáles son los medios que utiliza el despacho contable con sus clientes para la comunicación y los mecanismos que utiliza internamente con los empleados para la distribución de la información?**	Como despacho contable tenemos un correo electrónico, que se utiliza para comunicarnos con nuestros clientes en los casos que necesitemos pedir o enviar información, también, tenemos números de teléfono fijo, es nuestro medio principal para una comunicación más inmediata, asimismo, tenemos un número celular con WhatsApp, éste último lo utilizamos con los clientes que solicitan comunicación por esa vía, ellos expresan que les resulta más fácil y rápida la comunicación por esa vía, debido a que algunos no pueden revisar frecuentemente sus correos. Todos los empleados tienen acceso al correo del despacho y a los teléfonos, e internamente, para comunicarse entre ellos y especialmente con la jefatura, cada empleado tiene en su estación un teléfono fijo con una extensión propia.	Se considera que estos medios deberían contener controles de seguridad para el resguardo de la información, debido a que principalmente no es conveniente la utilización de un mismo correo por parte de todo el personal, esto no permite tener un adecuado control de todas las acciones que pueden realizar los empleados.

6.	**¿Cuál es la forma en que se le brinda mantenimiento al hardware y software del despacho?**	Nosotros tenemos un proveedor de servicios de mantenimiento de equipos informáticos, a ellos se le solicitan revisiones, mantenimientos, cambio de equipos, no periódicos, sino especialmente cuando algún equipo presenta problemas.	El despacho contable tiene un proveedor de servicios de mantenimiento de equipos informáticos, este servicio se contrata únicamente si alguna máquina presenta fallas o problemas en su funcionamiento. Lo anterior denota que la entidad no cuenta con una política escrita que establezca mantenimientos preventivos y correctivos de hardware y software ni tampoco, la periodicidad adecuada con que deben realizarse.
7.	**¿Qué controles de seguridad han implementado para mitigar los riesgos a los que puede enfrentarse la información confidencial del despacho contable y de sus clientes?**	La información y documentación de cada cliente se almacena por separado, por cliente, y se hacen respaldos periódicos de la información digital, los documentos físicos importantes, son entregados a los clientes (porque los utilizan para trámites y otras gestiones) y nosotros archivamos copias de los documentos. Referente al despacho, ningún empleado tiene acceso a la información propia, ésta la maneja la jefatura.	Se señaló que, han implementado controles para mitigar los riesgos asociados a la pérdida de información, pero están orientados principalmente a la documentación física, sin embargo, se considera que las medidas son limitadas tomando en cuenta la cantidad de posibles riesgos a los que se puede enfrentar la información confidencial de la entidad y de sus clientes tanto en formato físico como en digital.
8.	**¿Cuál es la norma implementada en el despacho contable para documentar la información que puede ser utilizada para realizar actividades desde casa o en modalidad de teletrabajo?**	Actualmente no contamos con la modalidad de teletrabajo.	Se indicó que la entidad no cuenta con la modalidad de teletrabajo, por lo tanto, esto denota que no cuentan con una política que establezca un plan de contingencia en caso de que por razones de fuerza mayor no sea posible desarrollar las actividades laborales desde las instalaciones del despacho

			contable.
9.	**¿Cuáles son las políticas de seguridad de la información establecidas en el despacho para garantizar a sus clientes el buen manejo y resguardo de la información que les proporcionan?**	No contamos con políticas escritas. La documentación que recibimos de los clientes es posteriormente devuelta a los mismos al cierre de cada ejercicio, los documentos se devuelven en archivadores, rotulados. Por otra parte, la información que en nuestro servicio generamos de forma mensual como declaraciones, informes, planillas, entre otros, se envían de forma digital mes a mes.	No cuentan con políticas escritas para garantizar a los clientes el buen manejo y resguardo de la información que ellos proporcionan, únicamente mencionan que la documentación que reciben la devuelven posteriormente a la prestación del servicio, no obstante, se considera que es de suma importancia que se establezcan políticas de seguridad por escrito para que se realicen los procedimientos adecuados según sea el caso.
10.	**¿Cuáles son los procedimientos que aseguran que no exista manipulación indebida en la información confidencial que se maneja de los clientes y del despacho?**	La supervisión de la jefatura, de todo el proceder de los auxiliares, se revisa la documentación que se genera, que se envía a los clientes, las solicitudes que se hacen a los mismos, se mantiene una comunicación diaria con los auxiliares referente al trabajo que está haciendo cada uno y las gestiones de sus clientes delegados.	Se identificó que la entidad sí cuenta con procedimientos, pero estos son implementados de forma empírica y no están estructurados de la forma más adecuada para asegurar que no exista manipulación indebida de la información confidencial, también se observó que estos procedimientos no están relacionados a una política de seguridad, esto debido a que la entidad no cuenta con este tipo de directrices.
11.	**¿Cuáles son los procedimientos que tienen en el despacho para la prevención de riesgos de fuga, extravío o hurto de información**	Ningún empleado tiene permitido extraer del despacho documentación de los clientes, tampoco puede modificar usuarios y contraseñas, ni borrar o eliminar	Se considera importante que las entidades preparen a sus empleados en la prevención de riesgos que involucren los datos confidenciales de quienes

	confidencial de los clientes?	información importante o sensible sin previa autorización. En el caso de capacitaciones sobre prevención de riesgos de fuga, extravío o hurto de información nunca se les han brindado a los empleados este tipo de recursos.	contratan sus servicios. Se identificó que, el despacho contable no posee procedimientos adecuados y estructurados que aseguren el buen manejo de la información, es necesario que se implementen medidas que bloqueen la copia de archivos a dispositivos externos sin previa autorización de la jefatura.
12.	**Describa el proceso de evaluación que se realiza en el despacho para identificar los riesgos que podrían afectar la seguridad de la información que se maneja en el despacho contable.**	No tenemos por escrito un proceso de evaluación definido.	Debido a que no cuentan con un proceso de evaluación de riesgos por escrito, se considera que es necesario que se implemente una metodología de gestión de riesgos para la protección de datos a fin de que sea de ayuda para el diseño de políticas y procedimientos en concordancia con los riesgos a los que se puede ver expuesta la información confidencial de la entidad.
13.	**¿Cuáles son los procesos de gestión con los que cuenta el despacho contable para la configuración de usuarios y cambios de contraseñas en sus equipos informáticos?**	Los equipos que utilizan los auxiliares no tienen contraseña, el servidor sí y sólo empleados de confianza tienen acceso a ella. Por lo general no se guarda información importante de los clientes en las computadoras de los empleados, todo se guarda en el servidor.	Se considera necesario que el despacho contable implemente políticas y procedimientos que permitan mantener una gestión eficiente de los procesos de configuración de usuarios y cambios de contraseñas.
14.	**¿Cuáles son los mecanismos para la protección de datos que tiene el**	Nadie ajeno al despacho puede acceder a una computadora o incluso a la bodega; sólo	Se observa que la entidad no cuenta con mecanismos adecuados para la

	despacho para el acceso a la información física y digital de sus clientes?	los socios tienen llave de la oficina.	protección de la información física y digital debido a que las instalaciones no poseen, por ejemplo, con alarmas sincronizadas con el dispositivo móvil de los socios, cámaras de videovigilancia, programas anti hackers, entre otros.
15.	**¿Qué mecanismos tiene el despacho contable para garantizar la confidencialidad de sus empleados sobre la información a la que tienen acceso?**	Cuando una persona es contratada firma un documento donde acepta ciertas normas internas del despacho y entre ellas hay una que especifica que no se puede divulgar información de los clientes con personas ajenas al despacho, claro, esto no aplica cuando a causa de algún trámite o gestión en instituciones, se tenga que entregar cierta información o documentación de un cliente, por supuesto que, si hacemos eso, contamos con la previa autorización de los mismos. Por otra parte, estamos atentos y evaluamos la conducta y el perfil profesional de cada empleado, para asegurarnos de mantener en nuestro despacho a personas con ética y que practiquen valores.	Se considera que el despacho contable sí implementa procedimientos para garantizar la confidencialidad de sus empleados, sin embargo, tales procedimientos no se encuentran formalmente documentados.
16.	**¿Qué medidas aplica el despacho contable con respecto a la destrucción del papel borrador o reciclado en el cual puede estar reflejada información confidencial de sus clientes?**	Sí reciclamos papel, pero procuramos darle un segundo uso temporal, no para ser archivado o para imprimir información importante, es decir, dicho papel es posteriormente desechado y la regla es romperlo antes de botarlo, por otra parte, la basura se saca al exterior el día que pasa el	Se observó que las medidas tomadas para la destrucción de papel borrador o reciclado no garantizan en su totalidad la correcta eliminación del papel que puede contener información confidencial, por ello se considera conveniente el uso de una máquina trituradora de papel para destruir de manera apropiada estos

		camión recolector.	documentos.
17.	**¿Con qué medidas de contingencia cuenta el despacho contable para evitar la pérdida de información propia y de sus clientes en casos de incendios, inundaciones, interrupciones de energía eléctrica, etcétera?**	Cuando los empleados se retiran de las oficinas, se verifica que los grifos queden debidamente cerrados, cuando hay fuertes lluvias, se revisan las instalaciones para verificar que no existan goteras, filtraciones por medio de ventanas o paredes y que funcionen correctamente los drenajes o tragantes. Para proteger a los equipos en caso de interrupciones de energía eléctrica, todos los equipos cuentan con un UPS y se verifica que éstos funcionen correctamente. Para casos de incendios, no contamos con un extintor, pero no se manipula fuego en las oficinas.	El despacho contable sí cuenta con medidas de contingencia para evitar la pérdida de información propia y de sus clientes en caso de siniestros, no obstante, se considera que deben documentarse como parte de las políticas de seguridad de la entidad. Además, se considera que es necesario incorporar otras medidas de contingencia como adquirir un extintor, un seguro, almacenamiento en la nube para todos los documentos digitales, entre otras, en caso de que ocurra un siniestro.
18.	**¿Considera importante contar con una metodología de gestión de riesgos para la protección de los datos tanto del despacho como de sus clientes?**	Consideramos que realmente es importante.	El socio considera realmente importante contar en la entidad, con una metodología de gestión de riesgos para la protección de los datos tanto del despacho contable como de sus clientes.
19.	**¿El despacho consideraría implementar la metodología de gestión de riesgos para la protección de datos del despacho y de sus clientes propuesta en la presente investigación?**	Por supuesto, es primera vez que participamos en algo así y agradeceremos cualquier sugerencia.	El socio del despacho contable muestra interés en obtener la propuesta de la metodología de gestión de riesgos para la protección de datos.

2.6.2 Diagnóstico de la investigación

Contar con una metodología de gestión de riesgos para la protección de datos es de suma importancia para los despachos contables debido a que constituye un mecanismo para la identificación y evaluación de riesgos con el fin de implementar controles de mitigación de estos y garantizar la seguridad y privacidad de la información de los clientes y del despacho. Mediante los resultados obtenidos en la entrevista se realizó el siguiente diagnóstico:

- Con respecto a la evaluación de riesgos, la cual es una parte fundamental de la metodología se determinó que, el despacho contable no cuenta con un proceso de evaluación de riesgos por lo que se considera relevante contar con un plan detallado y organizado, que contemple las probabilidades de ocurrencia e impacto de las amenazas y que establezca, además, los respectivos controles de mitigación de estas.
- Con relación a políticas de seguridad, la compañía carece de un documento por escrito debidamente aprobado por la alta administración, que contenga políticas de seguridad que garanticen a los clientes el buen manejo y resguardo de la información, la falta de políticas puede conllevar a la pérdida, robo o extravío de la misma.
- En cuanto a la aplicación de procedimientos para la protección de datos se identificó que, la entidad sí posee procedimientos sin embargo estos no han sido elaborados de acuerdo con las políticas respectivas debido a que no cuentan con estas y, además, no están establecidos en un documento como tal.

Lo anterior representa una oportunidad de mejora para el despacho contable puesto que incorporar una metodología de gestión de riesgos para la protección de datos de sus clientes y los propios, les permitirá identificar estratégicamente las amenazas para poder elaborar políticas y procedimientos acordes con el proceso de evaluación de riesgos.

CAPÍTULO III. PROPUESTA DE METODOLOGÍA DE GESTIÓN DE RIESGOS PARA LA PROTECCIÓN DE DATOS DE UN DESPACHO CONTABLE Y DE SUS CLIENTES

3.1 Planteamiento del caso

La protección de datos es una temática de relevancia en el sector empresarial, debido a que las compañías manejan grandes cantidades de información confidencial tanto de la misma empresa como de terceros, por lo que es importante que cuenten con mecanismos que garanticen la salvaguarda de esta.

Algunos expertos opinan que los negocios que son más susceptibles a sufrir pérdida, robo o fuga de información confidencial son aquellos de menor tamaño, como puede ser el caso de muchos despachos contables los cuales tienen cantidades importantes de datos, pero que por su tamaño no estiman relevante implementar medidas de protección debido a que no se consideran vulnerables a estos tipos de riesgos.

Los despachos contables tienen la obligación de garantizar la seguridad de la información de sus clientes debido a que existe un principio de confidencialidad establecido en el Código de Ética para Profesionales de la Contaduría Pública, que deben poner en práctica en su labor profesional.

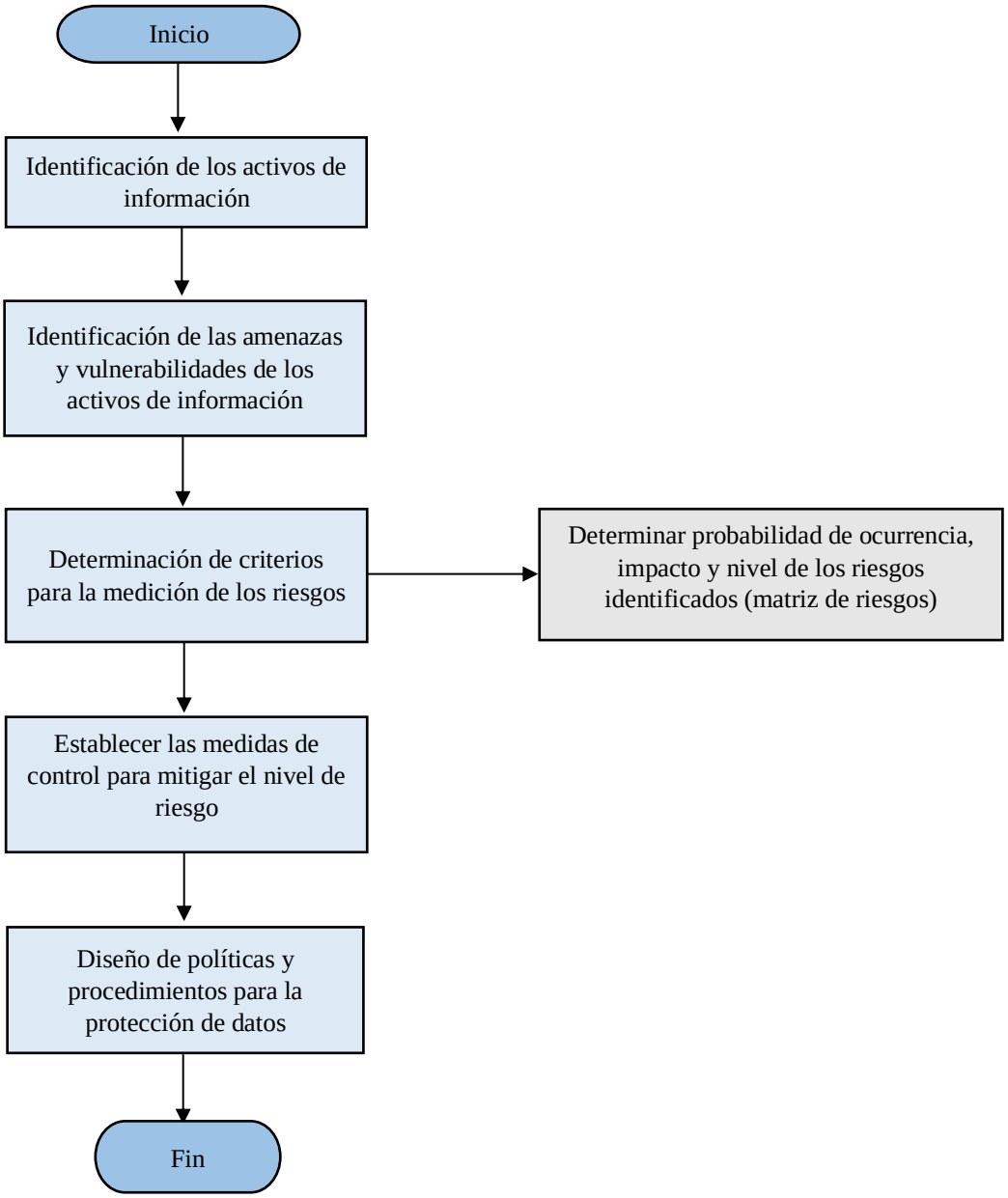
En el despacho contable objeto de este estudio se identificó que, no cuentan con un documento formal en el cual se establezca un proceso de evaluación de riesgos y lo que este conlleva, y de esa forma diseñar políticas y procedimientos adecuados para garantizar la seguridad de la información.

3.2 Estructura de la propuesta

El contenido y estructura de la metodología de gestión de riesgos para la protección de datos del despacho contable y de sus clientes es la siguiente:

Figura 1

Etapas para la elaboración de la propuesta de metodología de gestión de riesgos.



3.3 Beneficios y limitantes

3.3.1 Beneficios

- Identificación de riesgos que podrían afectar la seguridad de los activos de información del despacho contable con el fin de implementar controles para mitigarlos.
- Mejora continua de la entidad desde una perspectiva en la cual se identifican y se disminuyen los riesgos.
- Atenuación de las posibles responsabilidades legales que pueden producirse por la pérdida, robo o fuga de la información confidencial de los clientes.
- Protección de la imagen y reputación del despacho contable al garantizar que su información confidencial y las de sus clientes se maneje y resguarde de manera segura y confiable.

3.3.2 Limitantes

Durante el desarrollo de la investigación no surgieron ningún tipo de limitantes que pudieran afectar la realización de este trabajo.

3.4 Propuesta de solución

A continuación, se presenta la metodología de gestión de riesgos para la protección de datos del despacho contable y de sus clientes:

3.4.1 Identificación de activos de información e identificación de amenazas y vulnerabilidades de los activos de información

Para iniciar la metodología de gestión de riesgos para la protección de datos se procede con la identificación de los activos de información del despacho contable y sus respectivos riesgos, además, se establecen las consecuencias que pueden provocar las amenazas identificadas.

Tabla 3

Identificación de activos de información e identificación de las amenazas y vulnerabilidades de los activos de información.

N°	Activo de información	Riesgo identificado	Consecuencia asociada
1	Computadoras	Fallas en los equipos. Malware y virus. Accesos no autorizados a las computadoras.	− Daño del disco duro de la máquina y, por ende, pérdida de los datos allí almacenados. − Pérdida de datos o robo de la información y daño a los equipos. − Manipulación indebida de la información digital.
2	Servidor	Ataques de denegación de servicio. Fallas en el servidor. Accesos no autorizados al servidor.	− Pérdida del control de los equipos e inaccesibilidad a los recursos alojados en el sistema. − Pérdida de información. − Puede ocasionar la pérdida, eliminación accidental, entre otras, de la información confidencial.
3	Discos externos	Robo del dispositivo. Daño o extravío del dispositivo.	− Pérdida absoluta de la información almacenada en el dispositivo.
4	Teléfono móvil	Robo o extravío del dispositivo. Robo de identidad. Daño del dispositivo. Caída de red móvil.	− Pérdida de la información confidencial de los clientes y del despacho contable. − Pérdida de comunicación con los clientes.
5	UPS	Energía eléctrica limitada. Fallo en el dispositivo, cortocircuitos.	− La batería o UPS funcionará por un corto espacio de tiempo. − Incendios.

6	Documentos físicos	Pérdida total de los documentos por desastres naturales. Deterioro por factores ambientales, insectos, etc. Acceso a las instalaciones.	– Pérdida total de la documentación. – Documentos dañados e ilegibles. – Robo de los equipos y pérdida de la información.
7	Routers	Infiltración de un hacker.	– Control de todos los dispositivos, robo y manipulación de la información.
8	Software contable	Ataque al sistema. Fallas en el programa por la falta de mantenimiento y actualizaciones. Acceso no autorizado al sistema.	– Hackeo del sistema y manipulación indebida de los datos. – Pérdida de la información.

3.4.2 Determinación de criterios para la medición de riesgos

Para realizar el proceso de medición de los riesgos identificados en el despacho contable, es necesario establecer criterios, el primero corresponde a la probabilidad de ocurrencia de las amenazas y el segundo, es el impacto que estas tendrían en la entidad si ocurrieran.

- **Probabilidad de ocurrencia**

Este criterio es utilizado para determinar las posibilidades de que se produzcan los riesgos identificados y que puedan llegar a afectar la seguridad de la información del despacho contable y de sus clientes. La probabilidad de ocurrencia de cada uno de los riesgos se ponderará del 1 al 5, de acuerdo con la siguiente tabla:

Tabla 4

Ponderación de la probabilidad de ocurrencia de los riesgos.

Valor	Probabilidad	Descripción
5	Frecuente	Una vez por semana
4	Moderado	Una vez por mes
3	Ocasional	Una vez por semestre
2	Remoto	Una vez por año
1	Improbable	Cada cinco años

- **Impacto**

Mediante este criterio se determinará la magnitud de los riesgos si ocurrieran, es decir, el efecto que provocaría la ocurrencia de estos eventos en el despacho contable con respecto a la seguridad de la información que este maneja. El impacto de los eventos sobre la entidad se ponderará del 1 al 5, tal como se muestra a continuación:

Tabla 5

Ponderación del impacto de ocurrencia de los riesgos.

Valor	Impacto	Descripción
5	Catastrófico	De suceder las consecuencias serían catastróficas.
4	Mayor	De suceder tendría altas consecuencias sobre la entidad, sin embargo, puede continuar aún con pérdidas.
3	Moderado	De presentarse el hecho tendría medianas consecuencias sobre la entidad.
2	Menor	De suceder habría un bajo impacto sobre la entidad.
1	Insignificante	Si llegara a presentarse su impacto sería mínimo, lo que significa que las acciones de mitigación absorben completamente las consecuencias del riesgo.

- **Nivel de riesgos**

Mediante este criterio se cuantifican e identifican el nivel de los riesgos determinados para cada activo de información, los cuales han sido agrupados por áreas, en esta parte se establecen parámetros de ponderación de la probabilidad e impacto de las amenazas para asignar valores en la matriz de riesgos con el fin de determinar el nivel de exposición a dichos riesgos:

Tabla 6

Calificación de los riesgos.

Categoría	Puntaje	Descripción
Extremo	> 20	Requiere acción inmediata.
Alto	> 14 y ≤ 20	Revisión de controles de mitigación.
Moderado	> 7 y ≤ 14	Dar seguimiento continuo a los riesgos.
Menor	≥ 4 y ≤ 7	Revisión de la aplicación de procedimientos de rutina.
Bajo	< 4	Se están aplicando controles adecuados.

Tabla 7

Matriz de riesgos con ponderación de probabilidad de ocurrencia e impacto.

Identificación del riesgo					Análisis		Evaluación	Nivel del riesgo
Áreas	**ID**	**Riesgo**	**Causas**	**Consecuencias**	**Probabi - lidad**	**Impacto**		
Seguridad lógica	R.1	Accesos no autorizados a sistemas, servidor y software contable.	Hackeo o acceso no autorizado.	Robo de la información, manipulación indebida, eliminación malintencionada de la información	4	5	20	Alto
	R.2	Malware y virus.	Descargar e instalar programas de fuentes desconocidas, abrir documentos o links maliciosos.	Pérdida de datos o robo de la información y daño a los equipos.	5	5	25	Extremo
	R.3	Ataques de denegación de servicio.	Sistemas vulnerables.	Pérdida del control de los equipos e inaccesibilidad a los recursos alojados en el sistema.	4	4	16	Alto

	R.4	Fallas en el servidor.	Falta de conectividad a internet.	Pérdida de información.	3	4	12	Moderado
	R.5	Ataque al sistema.	Existencia de hackers.	Hackeo del sistema y manipulación indebida de los datos.	4	4	16	Alto
	R.6	Fallas en el programa por la falta de mantenimiento y actualizaciones.	Carencia de mantenimientos preventivos y correctivos de los programas.	Pérdida de información confidencial.	4	5	20	Alto
Seguridad física	R.7	Acceso a las instalaciones.	No contar con sistemas de videovigilancia, alarmas y seguridad débil del acceso al sitio.	Robo de los equipos y pérdida de la información	3	5	15	Alto
	R.8	Acceso a la bodega donde se resguardan los documentos físicos.	No contar con una puerta de acceso segura, sin llave.	Robo y extravío de información.	4	4	16	Alto
	R.9	Fallas en el suministro de energía eléctrica.	Condiciones climatológicas y otros sucesos imprevistos que afecten la energía eléctrica.	Daño en los equipos, ralentización de las actividades laborales.	2	2	4	Menor

	R.10	Desastres naturales.	Falta de planes de contingencia ante situaciones de emergencia.	Pérdida total de la documentación almacenada en físico y digital.	4	5	20	Alto
Hardware	R.11	Fallas en los equipos.	Falta de mantenimientos preventivos y correctivos a los equipos.	Daño del disco duro de la máquina y, por ende, pérdida de los datos allí almacenados.	3	4	12	Moderado
	R.12	Robo o extravío de los equipos informáticos y dispositivos móviles.	Asalto a las instalaciones de la entidad.	Pérdida de información confidencial de clientes y del despacho, como también el bloqueo del dispositivo.	2	4	8	Moderado
	R.13	Daño o extravío de dispositivos informáticos.	Accidentes involuntarios.	Pérdida absoluta de la información almacenada en el dispositivo.	2	3	6	Menor
	R.14	Energía eléctrica limitada.	Los UPS poseen energía limitada para su funcionamiento.	La batería o UPS funcionará por un corto espacio de tiempo.	3	3	9	Moderado
	R.15	Cortocircuitos.	Contacto accidental con los	Incendios.	2	4	8	Moderado

			tomacorrientes, cables eléctricos expuestos y apagones de energía eléctrica.					
Redes	R.16	Robo de identidad.	Hackeos, pérdida de credenciales y de los dispositivos móviles.	Pérdida de la información confidencial de los clientes y del despacho contable.	2	5	10	Moderado
	R.17	Caída de la red móvil.	Mejoras a la red por parte de la compañía proveedora del servicio.	Pérdida de comunicación con los clientes.	4	3	12	Moderado
	R.18	Infiltración de un hacker.	Contraseñas poco seguras y vulnerables al hackeo.	Control de todos los dispositivos, robo y manipulación de la información.	2	5	10	Moderado

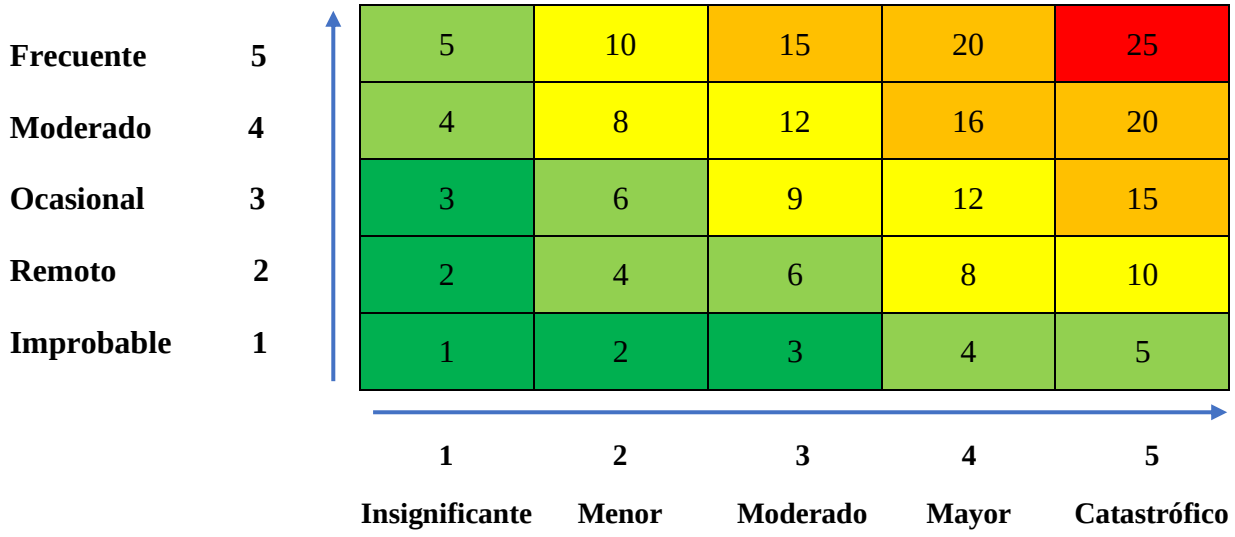
- **Mapa de riesgos.**

Mediante la probabilidad de ocurrencia y el impacto es posible identificar la exposición que tiene el despacho contable con respecto a los riesgos asociados a sus activos de información, y esto puede plasmarse en un mapa de calor.

El mapa de calor constituye una herramienta de visualización de las áreas o riesgos que reflejan mayor interés de ser atendidos. Esto le ayudará al despacho contable a identificar aquellos riesgos que requieren prioridad de ser controlados para evitar su ocurrencia en el futuro. A continuación, se muestra un modelo de mapa de riesgos o de calor de cinco por cinco:

Figura 2

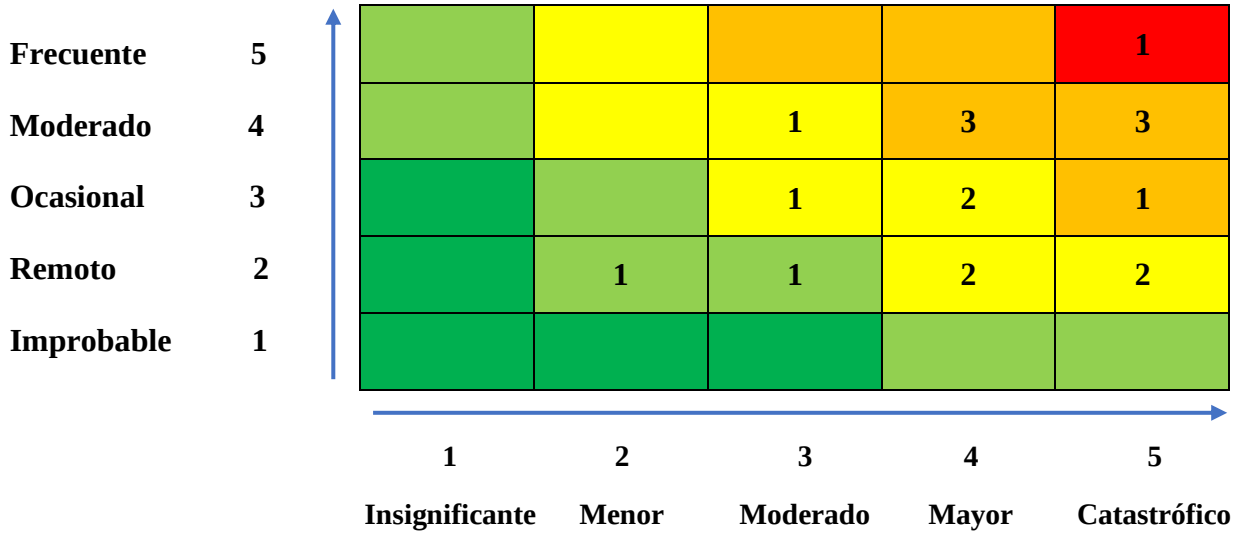
Modelo de mapa de riesgos.



La figura 2 muestra un mapa de calor que detalla el nivel de cada uno de los riesgos identificados para los activos de información del despacho contable:

Figura 3

Mapa de riesgos del despacho contable.



A través del mapa de calor se pueden observar los niveles de riesgos que presentan los eventos, se visualiza un alto nivel de una amenaza lo que indica que requiere de atención inmediata, por otra parte, hay otros identificados con magnitud alta, los cuales necesitan una revisión de los controles de mitigación. Además, surgieron eventos con un grado moderado lo cual es conveniente dar un seguimiento continuo de tales riesgos.

3.4.3 Establecimiento de controles de mitigación de los riesgos identificados

En esta etapa la entidad ya posee una visión más clara de los riesgos a los que pueden verse expuestos sus activos de información, la probabilidad de ocurrencia y el impacto que estos eventos producirían en el despacho contable, esto tiene como resultado la implementación de controles de mitigación de estas amenazas. Los controles de mitigación constituyen medidas que se implementan con el propósito de reducir o disminuir las probabilidades de ocurrencia y el impacto de los riesgos identificados en la empresa. En la tabla 9 se muestran los controles de mitigación sugeridos para los riesgos identificados para los activos de información del despacho contable.

Tabla 8

Controles de mitigación de los riesgos identificados en el despacho contable.

Controles de mitigación de los riesgos				
Área	**ID**	**Riesgo**	**Evaluación**	**Control**
Seguridad lógica	R.1	Accesos no autorizados a sistemas, servidor y software contable.	20	Control de acceso del personal del despacho a ingreso de los sistemas, servidores y software contable.
	R.2	Malware y virus.	25	Incorporación de herramientas (antivirus) que analicen el tránsito de la red en busca y prevención de posibles ataques al software.
	R.3	Ataques de denegación de servicio.	16	Monitorear el tráfico de la red. Adquisición de un sistema de detección y prevención de intrusiones.
	R.4	Fallas en el servidor.	12	Implementación de planes oportunos de respuestas a fallas o ataques al servidor.
	R.5	Ataque al sistema.	16	Incorporar medidas de identificación y autenticación de usuarios. Encriptación de datos. Monitorización y control de actividades.
	R.6	Fallas en el programa por la falta de mantenimiento y actualizaciones.	20	Implementación de políticas de mantenimiento y resguardo de la información.
Seguridad física	R.7	Acceso a las instalaciones	15	Instalación de cámaras de videovigilancia y alarmas sincronizadas a los dispositivos móviles de la alta dirección.

	R.8	Acceso a la bodega donde se resguardan los documentos físicos	16	Instalación de una puerta que pueda abrirse únicamente con las llaves (estas a cargo de las jefaturas), y, además, procurar que la bodega se mantenga siempre cerrada.
	R.9	Fallas en el suministro de energía eléctrica	4	Verificar que los UPS funcionen correctamente para continuar con las labores. Contar con un modem de internet inalámbrica para casos de emergencia.
	R.10	Desastres naturales	20	Contar con un plan detallado de medidas de contingencia en caso de emergencias o desastres naturales.
Hardware	R.11	Fallas en los equipos	12	Mantenimiento preventivo y correctivo de forma periódica, al menos cada 6 meses. Instalación de programas de antivirus o actualización de licencias.
	R.12	Robo o extravío de los equipos informáticos y dispositivos móviles	8	Copias de seguridad en la nube de la información más importante y confidencial.
	R.13	Daño o extravío de dispositivos informáticos	6	Delimitar un listado de las personas autorizadas para su manipulación y evitar el contacto con materiales, comida, etc., que puedan generar algún daño al dispositivo.
	R.14	Energía eléctrica limitada de los UPS.	9	Limpieza y mantenimiento de los equipos. Guardar inmediatamente los últimos cambios realizados a las actividades que se están realizando en el momento en que ocurre el apagón de energía eléctrica. Uso adecuado.

	R.15	Cortocircuitos.	8	Crear una política para el mantenimiento y la seguridad de las instalaciones eléctricas.
Redes	R.16	Robo de identidad	10	Implementar medidas de control para verificar las salidas de equipos de información y que tengan la debida autorización.
	R.17	Caída de la red móvil.	12	Incorporar un mantenimiento preventivo para los lugares donde se tienen los routers.
	R.18	Infiltración de un hacker.	10	Controles de detección y prevención para proteger los sistemas informáticos, asignar contraseñas seguras a las redes que imposibiliten su hackeo.

3.4.4 Políticas y procedimientos para la protección de datos del despacho contable y de sus clientes

Las políticas de seguridad de la información son importantes debido a que mediante estas se establecen reglas y procedimientos para el manejo y resguardo de los datos. El objetivo de la implementación de políticas y procedimientos es proteger la información confidencial de la entidad y minimizar los riesgos a los que se pueden enfrentar los activos de información para que exista una mejora continua en la compañía. A continuación, se presentan las políticas y procedimientos para la seguridad de la información del despacho contable:

1. **Política:** Toda persona que forme parte del despacho contable en calidad de empleado, debe mantener la confidencialidad de la información que se maneja y administra en la entidad.

    - **Procedimiento:** Firma de una declaración jurada de confidencialidad donde se juramenta que todos aquellos datos que se maneje de la entidad y de terceros deberán

ser tratados estrictamente de manera confidencial, y, además, se aceptan las consecuencias del incumplimiento de las cláusulas y términos establecidos en el documento.

2. **Política:** Capacitación, concientización y formación adecuada a los empleados sobre los equipos informáticos y la protección de datos.

    - **Procedimiento:** Brindar de forma periódica a los empleados, capacitaciones acerca de la prevención de riesgos a los que puede verse expuesta la información confidencial almacenada en físico y digital.

3. **Política:** Cambios de contraseñas de acceso a las diferentes plataformas digitales y software contable de la entidad cada tres meses y en los casos en que ocurra de una baja en el personal del despacho.

    - **Procedimiento:** Realizar cambios de contraseñas de manera trimestral en las plataformas digitales y software contable, las claves deberán contener ocho caracteres como mínimo, estos pueden ser minúsculas, mayúsculas, símbolos y números. Lo anterior deberá realizarse también, de manera inmediata, cuando ocurra una baja en el personal del despacho.

4. **Política:** Realización de respaldos de la información de los servidores de forma mensual y previo a una modificación significativa en el sistema operativo de las computadoras.

    - **Procedimiento:** Respaldar la información almacenada en los servidores cada mes, y en aquellos casos previo a la fecha de actualización del sistema operativo de las computadoras.

5. **Política:** Cifrado de información sensible clasificada como confidencial, que puede estar expuesta a usuarios no autorizados, con relación a su confidencialidad.

    - **Procedimiento:** Codificar toda la información confidencial susceptible a riesgos de pérdida, robo o extravío.

6. **Política:** Asignación de usuarios personales a cada empleado para el acceso y uso del software contable.

    - **Procedimiento:** Crear usuarios para el acceso y uso del software contable, para cada uno de los empleados del despacho para que posteriormente les sean asignados.

7. **Política:** Mantenimiento preventivo y correctivo de los equipos informáticos de forma periódica.

    - **Procedimiento:** Los mantenimientos preventivos de los equipos informáticos deben realizarse cada seis meses, y en el caso de los mantenimientos correctivos estos deben realizarse cuando se presentan problemas con los equipos.

8. **Política:** Mantenimiento preventivo y correctivo de las instalaciones eléctricas del despacho.

    - **Procedimiento:** Realizar una revisión e inspección una vez por año, de las instalaciones eléctricas del despacho.

9. **Política:** Los respaldos de la información deben realizarse mediante el almacenamiento en la nube.

    - **Procedimiento:** Realizar un respaldo de la información una vez por semana en el almacenamiento en nube.

10. **Política:** Establecimiento de un plan de contingencia ante emergencias por desastres naturales para el resguardo de la información confidencial.

    - **Procedimiento:** Documentar en un plan de contingencia las medidas a seguir en caso de emergencias por la ocurrencia de desastres naturales.

11. **Política:** Renovar y cambiar las contraseñas de forma periódica.

    - **Procedimiento:** Cambiar cada dos meses las contraseñas de la red de internet y software contable.

12. **Política:** Es prohibido para los empleados extraer documentos de los equipos informáticos en dispositivos de almacenamiento externo.

    - **Procedimiento:** Restringir mediante bloqueo de acceso a cualquier unidad de almacenamiento externa a través del editor de directivas de grupo local y limitar el acceso a la información solo a aquellos empleados que la necesitan para realizar alguna actividad de trabajo.

13. **Política:** Queda prohibido descargar programas informáticos de sitios web y archivos no seguros que puedan poner en riesgo la seguridad de la información.

    - **Procedimiento:** Por medio de configuraciones a los equipos informáticos, específicamente programas de antivirus, restringir la descarga de programas externos, archivos no seguros que provengan de fuentes no confiables y el acceso a sitios web maliciosos.

14. **Política:** Restricción del consumo de alimentos y bebidas en las áreas donde se encuentra la documentación física y los equipos informáticos.

- **Procedimiento:** Brindar capacitaciones a los empleados acerca del buen uso de los equipos informáticos, la información física que se encuentra en las instalaciones y las maneras en qué pueden contribuir a la protección de datos del despacho contable.

15. Política: Queda prohibido el acceso a la bodega donde se resguarda la información física del despacho contable y de clientes sin previa autorización de la jefatura correspondientes.

- **Procedimiento:** El empleado debe solicitar el acceso a los medios de almacenamiento de la documentación física.

CONCLUSIONES

Mediante el presente trabajo de investigación se determinó que la gestión de riesgos es un proceso fundamental para garantizar la seguridad de la información de un despacho contable, debido a que la implementación de metodologías enfocadas a la gestión de riesgos permite priorizar las amenazas y establecer controles apropiados para su respectiva minimización. En ese sentido, se concluye que:

- No se cuenta con un proceso de evaluación de riesgos, siendo una parte fundamental de la metodología debido a que constituye un plan detallado y organizado que contempla las probabilidades de ocurrencia e impacto de las amenazas y establece los respectivos controles de mitigación de estas.

- No poseen un documento debidamente aprobado por la alta dirección que establezca políticas de seguridad que garanticen a los clientes el buen manejo y resguardo de la información, la falta de políticas puede conllevar a la pérdida, robo o extravío de la misma.

- Se cuentan con procedimientos para la protección de datos, sin embargo, estos no han sido elaborados de acuerdo con las políticas respectivas debido a que no cuentan con estas y, además, estos no están debidamente establecidos en un documento como tal.

- No se promueve una cultura de capacitaciones en el despacho contable, debido a que se identificó que, hasta la fecha de realización de esta investigación, los empleados nunca han recibido ninguna preparación en materia de prevención de riesgos que pueden afectar la seguridad de la información de la entidad y de sus clientes.

- No se cuenta con personal designado a llevar a cabo un proceso de gestión de riesgos que involucre evaluaciones de las amenazas que se ha identificado que pueden afectar la confidencialidad de la información del despacho y de sus clientes, asimismo, controles y acciones para mitigarlos de forma apropiada.

RECOMENDACIONES

Con base a las conclusiones antes detalladas, se recomienda al despacho contable lo siguiente:

- La implementación de la metodología de gestión de riesgos para la protección de datos del despacho contable y de sus clientes desarrollada como propuesta en este documento, para que contribuya a la gestión y prevención de amenazas que pueden afectar la seguridad de la información.
- Documentar de forma adecuada las políticas y procedimientos desarrollados en este estudio, mediante la respectiva aprobación de la alta administración, y tomando en consideración la evaluación de riesgos a los que se puede ver expuesta la seguridad de la información de la entidad y de sus clientes.
- La oportuna gestión por parte de la alta dirección en cuanto a la gestión de los riesgos identificados en las evaluaciones, debido a que es importante que se implementen acciones y controles adecuados en el momento apropiado.
- La adopción de una cultura de capacitaciones dirigidas a los empleados para prepararlos en materia de prevención de riesgos que pongan en peligro la información del despacho y de los clientes.

BIBLIOGRAFÍA

Aliados en tecnología S.A.S. (s.f.). *GESTIÓN DE RIESGOS: IMPORTANCIA, EVOLUCIÓN Y EXIGENCIAS.* Recuperado el 1 de December de 2022, de IMPLEMENTANDO SGI: https://www.implementandosgi.com/procesos/gestion-de-riesgos-1/

AON. (30 de Noviembre de 2022). *Encuesta Global de Gestión de Riesgos 2021 de Aon.* Obtenido de AON: https://www.aon.com/2021-global-risk-management-survey/latam/es.jsp

Asamblea Legislativa de El Salvador. (26 de Febrero de 2016). Ley Especial contra los Delitos Informáticos y Conexos. Obtenido de https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/2/2010-2019/2016/02/B6B74.PDF

Asamblea Legislativa de El Salvador. (11 de Mayo de 2021). *Asamblea Legislativa de El Salvador.* Obtenido de https://www.asamblea.gob.sv/sites/default/files/documents/correspondencia/EFBA7BEE-871B-40BE-BD0A-5BD80237CA90.pdf

Bornik, S. (13 de April de 2010). *¿Qué es la fuga de información?* Recuperado el 30 de November de 2022, de WeLiveSecurity: https://www.welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion/

Consejo de Normas Internacionales de Ética para Contadores. (Abril de 2018). Código Internacional de Ética para Profesionales de la Contabilidad (incluidas Normas Internacionales de Independencia). Obtenido de https://www.ifac.org/system/files/publications/files/Final-Pronouncement-The-Restructured-Code-ES.pdf

Despacho Contable Monzón y Padilla. (19 de August de 2020). *Funciones de un Despacho Contable.* Obtenido de Despacho Contable Monzón y Padilla: https://despacho-contable.mx/2020/08/19/automatizacion-de-procesos-con-software-para-contabilidad/

Dutta, S., Lanvin, B., Rivera, L., & Wunsch, V. (2022). *Global Innovation Index*. Obtenido de Organización Mundial de la Propiedad Intelectual: https://www.wipo.int/edocs/pubdocs/en/wipo-pub-2000-2022-section1-en-gii-2022-at-a-glance-global-innovation-index-2022-15th-edition.pdf

Editorial Etecé. (5 de Agosto de 2021). *Concepto de Riesgo - tipos, prevención, diferencia con el peligro.* Recuperado el 30 de November de 2022, de Concepto: https://concepto.de/riesgo/#ixzz7lOSKLLYX

Enríquez, L. (15 de June de 2021). *La protección de datos en América latina: influencia del RGPD - Observatorio Ciberderechos y Tecnosociedad.* Recuperado el 30 de November de 2022, de Universidad Andina Simón Bolívar: https://www.uasb.edu.ec/ciberderechos/2021/06/15/la-proteccion-de-datos-en-america-latina-influencia-del-rgpd/

EQA. (6 de Agosto de 2019). *EQA*. Obtenido de CERTIFICACIÓN ISO 27701: https://eqa.es/seguridad-informacion/iso-27701

EQA. (s.f.). *EQA*. Obtenido de https://eqa.es/seguridad-informacion/iso-27701

Grupo Ático 34. (2022). *Privacidad Digital en Internet. Guía 2022*. Obtenido de https://protecciondatos-lopd.com/empresas/privacidad-digital/

Grupo ESGiinova. (s.f.). *¿Cuáles son las metodologías para la gestión de riesgo?* Recuperado el 30 de November de 2022, de ISOTools México: https://www.isotools.com.mx/cuales-las-metodologias-la-gestion-riesgo/

Grupo ESGiinova. (31 de January de 2018). *¿Cuál es la metodología que se utiliza en la gestión de riesgo?* Recuperado el 30 de November de 2022, de ISOTools: https://www.isotools.org/2018/01/31/la-metodologia-se-utiliza-la-gestion-riesgo/

Hefner, K., Peterson, S., & Crocetti, P. (Agosto de 2021). *¿Qué es Protección de datos?* Obtenido de Computer Weekly: https://www.computerweekly.com/es/definicion/Proteccion-de-datos

IBM. (s.f.). *IBM*. Obtenido de ¿Qué es la gestión de riesgo?: https://www.ibm.com/ar-es/topics/risk-management

Instituto Nacional de Ciberseguridad. (10 de Octubre de 2019). *incibe*. Obtenido de ¿Conoces la nueva forma para la gestión de la privacidad?: https://www.incibe.es/protege-tu-empresa/blog/conoces-nueva-norma-gestion-privacidad#:~:text=La%20ISO%2027701%20especifica%20los,de%20la%20Informaci%C3%B3n%20%28SGSI%29

ISO 27000.ES. (s.f.). *Serie 27k*. Recuperado el 1 de December de 2022, de ISO27000.es: https://www.iso27000.es/iso27000.html

ISOTools Excellence. (31 de Enero de 2014). *Seguridad de la Información*. Obtenido de https://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/

Jiménez, M. M. (11 de October de 2022). *Así puedes hacer una matriz de riesgos para tu empresa*. Recuperado el 30 de November de 2022, de Pirani: https://www.piranirisk.com/es/blog/asi-puedes-hacer-una-matriz-de-riesgos-para-tu-empresa

Mallet, C. (2 de September de 2019). *4 maneras de proteger tu asesoría o despacho profesional ante una filtración de datos*. Recuperado el 30 de November de 2022, de Sage: https://www.sage.com/es-es/blog/4-maneras-de-proteger-tu-asesoria-o-despacho-profesional-ante-una-filtracion-de-datos/

Martínez, V. (1 de Junio de 2022). *Audidat Protección de Datos*. Obtenido de https://www.audidat.com/beneficios-para-su-empresa-al-cumplir-con-la-normativa-de-proteccion-de-

datos/#:~:text=Beneficios%20de%20cumplir%20con%20la,de%20confianza%20para%20sus%20clientes

OEA. (3 de Enero de 2022). Principios Actualizados sobre la Privacidad y la Protección de Datos Personales. Obtenido de https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

Osorio, J. (30 de Enero de 2018). *IPANDETEC.* Obtenido de https://www.ipandetec.org/2018/01/30/privacidad-datos-personales-en-el-salvador/

Russell, J., & NQA. (s.f.). *ISO 27001: 2013 Guía de Implantación para la Seguridad de la Información*. Obtenido de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Tecón, S. I. (s.f.). *Simplificando la Tecnología*. Obtenido de https://www.tecon.es/la-seguridad-de-la-informacion/

ANEXOS

Anexo No. 1

Guía de entrevista dirigida a un socio del despacho contable

Universidad de El Salvador

Facultad de Ciencias Económicas

Escuela de Contaduría Pública

Entrevista sobre: Metodología de gestión de riesgos para la protección de datos de un despacho contable y de sus clientes.

Dirigida a: Socio del despacho contable.

Objetivo de la entrevista: Obtener información acerca de la situación actual del despacho contable en cuanto a la implementación de medidas para la protección de datos de la entidad y de sus clientes.

Preguntas:

Objetivo: Identificar los medios físicos e informáticos que se utilizan en el despacho para resguardar la información confidencial del despacho y de sus clientes.

1. **¿Qué medios físicos e informáticos utilizan en el despacho contable para el resguardo de la información confidencial de la entidad y de sus clientes?**

Objetivo: Identificar el proceso de autorización para solicitar información confidencial y modificación de datos de clientes y del despacho contable.

2. **¿Cuál es el proceso de autorización para solicitar información confidencial y modificar datos tales como contraseñas, usuarios, correos de los clientes y del despacho contable?**

Objetivo: Identificar el tipo de información que puede ser susceptible a amenazas de pérdida, robo o extravío.

3. **Según su experiencia, ¿qué tipo de información es más susceptible a amenazas de pérdida, robo o extravío?**

Objetivo: Determinar de qué formas los socios del despacho contribuyen a que se garantice la protección en los datos que los clientes les proporcionan y la información de la entidad.

4. **¿Cómo contribuyen los socios del despacho a garantizar la protección de los datos que les han sido confiados por los clientes y la información del despacho?**

Objetivo: Identificar los medios de comunicación que tiene el despacho con sus clientes y los mecanismos que utiliza internamente con los empleados para la distribución de la información.

5. **¿Cuáles son los medios que utiliza el despacho contable con sus clientes para la comunicación y los mecanismos que utiliza internamente con los empleados para la distribución de la información?**

Objetivo: Identificar la forma en que se le brinda mantenimiento al hardware y software del despacho contable.

6. **¿Cuál es la forma en que se le brinda mantenimiento al hardware y software del despacho?**

Objetivo: Identificar los controles de seguridad que ha implementado el despacho para mitigar los riesgos a los que puede enfrentarse la información confidencial de la entidad y de sus clientes.

7. **¿Qué controles de seguridad han implementado para mitigar los riesgos a los que puede enfrentarse la información confidencial del despacho contable y de sus clientes?**

Objetivo: Identificar la norma que implementa el despacho contable para documentar la información que puede ser utilizada por los empleados del despacho contable para realizar actividades desde casa o en modalidad de teletrabajo.

8. **¿Cuál es la norma implementada en el despacho contable para documentar la información que puede ser utilizada para realizar actividades desde casa o en modalidad de teletrabajo?**

Objetivo: Identificar si el despacho contable cuenta con políticas para el buen manejo y resguardo de la información que sus clientes les proporcionan.

9. **¿Cuáles son las políticas de seguridad de la información establecidas en el despacho para garantizar a sus clientes el buen manejo y resguardo de la información que les proporcionan?**

Objetivo: Identificar los procedimientos que se emplean para asegurar que no exista manipulación indebida en la información confidencial del despacho y de sus clientes.

10. **¿Cuáles son los procedimientos que aseguran que no exista manipulación indebida en la información confidencial que se maneja de los clientes y del despacho?**

Objetivo: Identificar los recursos que utiliza el despacho contable con sus empleados para la prevención de riesgos de fuga, extravío o hurto de información confidencial.

11. **¿Cuáles son los procedimientos que tienen en el despacho para la prevención de riesgos de fuga, extravío o hurto de información confidencial de los clientes?**

Objetivo: Identificar el proceso de evaluación que realiza el despacho contable para determinar los riesgos que pueden afectar la confidencialidad de la información que se maneja en la entidad.

12. **Describa el proceso de evaluación que se realiza en el despacho para identificar los riesgos que podrían afectar la seguridad de la información que se maneja en el despacho contable.**

Objetivo: Indagar los procesos de gestión que posee el despacho contable con respecto a la configuración de usuarios y cambios de contraseñas de sus equipos informáticos.

13. **¿Cuáles son los procesos de gestión con los que cuenta el despacho contable para la configuración de usuarios y cambios de contraseñas en sus equipos informáticos?**

Objetivo: Identificar los mecanismos de protección de datos que tiene el despacho para el acceso a la información física y digital de la entidad y de sus clientes.

14. ¿Cuáles son los mecanismos para la protección de datos que tiene el despacho para el acceso a la información física y digital de sus clientes?

Objetivo: Identificar los mecanismos que posee el despacho para garantizar la confidencialidad de sus empleados sobre la información a la que tienen acceso.

15. ¿Qué mecanismos tiene el despacho contable para garantizar la confidencialidad de sus empleados sobre la información a la que tienen acceso?

Objetivo: Indagar las medidas que implementa el despacho contable para la destrucción del papel borrador o reciclado que puede contener información de clientes.

16. ¿Qué medidas aplica el despacho contable con respecto a la destrucción del papel borrador o reciclado en el cual puede estar reflejada información confidencial de sus clientes?

Objetivo: Identificar las medidas de contingencia que posee el despacho contable para evitar la pérdida de información propia y de clientes en casos de incendios, inundaciones, interrupciones de energía eléctrica, etcétera.

17. **¿Con qué medidas de contingencia cuenta el despacho contable para evitar la pérdida de información propia y de sus clientes en casos de incendios, inundaciones, interrupciones de energía eléctrica, etcétera?**

Objetivo: Conocer la opinión del socio del despacho contable con respecto a la aplicación de una metodología de gestión de riesgos para la protección de datos en la entidad.

18. **¿Considera importante contar con una metodología de gestión de riesgos para la protección de los datos tanto del despacho como de sus clientes?**

Objetivo: Conocer el nivel de interés que tiene el socio del despacho contable con relación a la implementación de una metodología de gestión de riesgos para la protección de los datos de la entidad y de sus clientes.

19. **¿El despacho consideraría implementar la metodología de gestión de riesgos para la protección de datos del despacho y de sus clientes propuesta en la presente investigación?**
