UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

"DISEÑO DE SISTEMA DE CONTROL INTERNO INFORMÁTICO BASADO EN RIESGOS DE TECNOLOGÍA DE INFORMACIÓN PARA LAS AGENCIAS DE VIAJES DEL MUNICIPIO DE SAN SALVADOR"

TRABAJO DE INVESTIGACIÓN PRESENTADO POR

CANALES MEDRANO, ALFREDO ALINSON
GONZÁLEZ FLORES, KARINA DE JESÚS

Para optar al grado de

LICENCIADO EN CONTADURÍA PÚBLICA

JULIO DE 2015

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES UNIVERSITARIAS

Rector	: Ingeniero Mario Roberto Nieto Lovo
Secretaria	: Doctora Ana Leticia Zavaleta de Amaya
Decano de la Facultad de Ciencias Económicas	: Máster Roger Armando Arias Alvarado
Secretario de la facultad de Ciencias Económicas	: Máster José Ciriaco Gutiérrez Contreras
Directora de la Escuela de Contaduría Pública	: Licenciada María Margarita de Jesús Martinez Mendoza de Hernández.
Coordinador de seminario	: Licenciado Mauricio Ernesto Magaña Menéndez
Docente director	: Licenciado Daniel Nehemías Reyes López
Jurado examinador	: Licenciado Daniel Nehemías Reyes López : Licenciado Víctor René Osorio Amaya : Licenciado Henry Amílcar Marroquín

Agradecimientos

A Dios, por brindarme todo lo necesario y darme las fuerzas para alcanzar la meta y culminar mis estudios. A mi papá Alfredo Canales por brindarme su guía en los momentos más difíciles, a mi madre Patricia de Canales por la paciencia y su motivación para alcanzar mis metas, a mis hermanos Romeo y Diego por motivarme cada día a librar mis luchas, a Raquel Guerrero y su familia por su apoyo incondicional, a mis amigas y amigos que estuvieron pendientes de mí en todo momento y a mi compañera Karina por haber sido valiente en conseguir este objetivo.

Alfredo Alinson Canales Medrano

A nuestro Señor Jesús por darme la sabiduría, salud y fortaleza durante mi carrera, sin Él nada hubiese sido posible. A mi madre Zoila Flores por sus incansables oraciones, consejos y cuidados. A mi padre Mario González, por sus oraciones y consejos que siempre estuvieron presentes en mi desempeño académico. A mis hermanos Hugo y Ever por depositar su amor y confianza en mí y apoyarme en todo momento. Agradezco a mi compañero de lucha Alfredo que jamás se rindió a pesar de las circunstancias y siempre fue un apoyo incondicional para cumplir nuestro objetivo trazado. Y a mis amigas y amigos que me apoyaron en todo momento y siempre tuvieron una palabra de aliento y consejo.

Karina de Jesús González Flores.

ÍNDICE

ÍNDICE DE CUADROS

RESUMEN EJECUTIVO

Las agencias de viajes han tomado a las tecnologías de información (TI) como parte de su negocio, realizando enormes inversiones en equipo y sistemas que le facilitan la realización de sus operaciones. Esto conlleva a implementar controles internos informáticos a la medida de sus actividades.

El profesional en contaduría pública normalmente no desarrolla sistemas de control interno orientados al área informática; no obstante la Federación Internacional de Contadores (IFAC) establece que su competencia debe abarcar el área de conocimientos en TI. El presente documento proporciona una herramienta de servicios convenidos, tema tratado en las Normas Internacionales de Servicios Relacionados, las cuales establecen lineamientos que permiten al profesional ofrecer un trabajo convenido, siempre que posea el conocimiento suficiente sobre la materia en cuestión y tenga el criterio razonable.

Por lo anterior expuesto, el objetivo trazado en esta investigación fue proveer al profesional en contaduría pública una modelo de diseño de sistema de control interno informático basado en riesgos, que beneficie bilateralmente tanto al profesional como a las agencias de viajes.

Para ello se ejecutó un estudio hipotético – deductivo, en donde se recopiló la información general del sector investigado; posteriormente se formuló la hipótesis con el objeto de explicar el problema de estudio y realizar su diagnóstico.

Se encontró que los profesionales en cuestión actualmente ofrecen en su mayoría solamente los servicios de auditoría financiera, quienes manifiestan que pocos de sus clientes implementan procedimientos de detección, prevención y corrección de datos. Mientras que la mayoría de las agencias de viajes declaran aplicar dichos procedimientos, sin embargo los controles que utilizan son inefectivos debido a los problemas que manifiestan tener. Estas entidades desconocen que al tener bien establecidos los procedimientos de control, el nivel de exposición al riesgo informático y los problemas inherentes se verían reducidos, ya que no tienen una filosofía de riesgo. Ambas partes expusieron que la creación de un modelo de diseño de sistema de control interno informático seria de utilidad.

Para el diseño de un sistema de control interno informático basado en riesgos es necesario identificar los activos o recursos que posee la entidad, luego realizar la gestión de los riesgos informáticos a los que

están expuestos. Una adecuada gestión determinada por la pericia del profesional, ayudará en el diseño adecuado de controles que actúen sobre la causa de los riesgos para disminuir la probabilidad de ocurrencia.

En cuanto a la decisión de cuales controles internos informáticos son requeridos para optimizar su exposición al riesgo, depende del conocimiento de la entidad y su actividad, el profesional en contaduría pública aplica su pericia técnica.

Si los controles propuestos se implementan con éxito en los riesgos identificados, se logra obtener el resguardo y la seguridad requerida en la información que maneja la compañía, reduciendo en gran medida la pérdida de datos y recursos ante cualquier eventualidad.

INTRODUCIÓN

La agencia de viaje es en la actualidad el principal agente de intermediación turística a escala mundial, siendo su rol como distribuidor quizás más significativo que el de otros intermediarios en diferentes industrias y productos. Las innovaciones tecnológicas le han dado un dinamismo a sus operaciones, contribuyendo a la diversificación de sus servicios.

La relación entre las entidades mencionadas y la tecnología de información, si bien ha sido beneficiosa, también ha generado dificultades en el manejo de datos, debido a la aplicación de un sistema de control interno informático deficiente, o a la ausencia de este.

El creciente uso de la tecnología de información y la manipulación de datos, ha desarrollado la necesidad imperiosa de establecer los mecanismos óptimos que faciliten su gestión, brinden confidencialidad y seguridad por parte de todos los participantes de un sistema informático.

Este documento pretende servir de guía para realizar la implementación de control interno informático, enfocados a las agencias de viajes, sin embargo, también puede ser de utilidad para otro giro de negocios el cual requiera del diseño de los controles, cuyo fin principal es la optimización del riesgo.

En el capítulo I, se recopilan los aspectos generales de las agencias de viajes, su historia tanto a nivel mundial como local; el uso de las tecnologías de información y el surgimiento del control interno informático; un glosario sobre conceptos empleados en la actividad comercial de las agencias, una descripción general del ciclo de operaciones de este rubro; se detallan las normativas que permiten al contador público, ser participe en el diseño de este tipo de controles.

Este capítulo también contiene un resumen sobre el marco teórico y legal aplicable a estas entidades; clasificaciones de los controles internos informáticos y el procedimiento para diseñar el sistema de control interno.

El capítulo II concentra el diagnóstico general sobre el diseño de los controles y enlista las dificultades que experimentan los sujetos de estudios con respecto al problema, tanto los contadores públicos con personería jurídica y las agencias de viajes, ambos del municipio de San Salvador.

El capítulo III proporciona un ejemplo sobre cómo se diseñan los sistemas de control interno informático, a través de la evaluación de los riesgos y la implementación de controles internos informáticos específicos que gestionen y optimicen en gran medida los riesgos asociados.

Finalmente, el capítulo IV refleja las conclusiones durante la investigación con respecto al uso de la tecnología de información en las agencias de viajes y recomendaciones dirigidas tanto a las firmas de contaduría pública del municipio de San Salvador y las agencias de viajes.

.

CAPITULO I: MARCO TEÓRICO, CONCEPTUAL, TÉCNICO Y LEGAL

1.1 ANTECEDENTES.

1.1.1 Agencias de viajes a nivel internacional.

Los historiadores relatan que en el año 1841, Thomas Cook organizo una expedición con destino a un congreso anti-alcohol en Loughborough, Reino Unido; siendo el primer empresario ingles en realizar este tipo de actividad de forma organizada a gran escala. Esta no genero éxito económico en ese momento; sin embargo, su actitud emprendedora, le motivó a fundar su agencia de viajes a la que denominó Thomas Cook & Son, siendo la primera en su tipo.

En 1866 viajó a Estados Unidos para concertar los servicios de diferentes compañías ferroviarias. Más adelante abrió sucursales de la empresa en las ciudades que le interesaban como abastecedoras. En 1868 consiguió la exclusiva para explotar el tráfico de pasajeros del continente europeo por la ruta de Harwich. Viajó a Holanda, Bélgica y Alemania con el fin de convenir el abastecimiento de servicios de transporte con diversas compañías, logrando obtener la vía del puerto de Brennero a Bríndisi.

Una de sus aportaciones más destacadas fue la creación del sistema de pago basado en cupones concertados con hoteles, usados como medio de liquidación para sus clientes. Este ejemplo fue imitado en América como en Europa, dando nacimiento a numerosas empresas dedicadas a la producción de turismo y a la intermediación de servicios de alojamiento.[1]

1.1.2 Agencias de viajes a nivel nacional.

Es difícil afirmar con certeza, la fecha en que surgieron estas entidades. Sin embargo se sostiene que la primera fue *El Salvador Travel Service*, fundada en 1941, por el señor Armando López Ulloa.

Luego inició *IBALACA TOURS* en 1948, organizada por los señores: Armando Ibáñez y Roberto Lacayo, con operaciones de venta de boletos terrestres a Guatemala y Honduras. Obteniendo reconocimiento por sus excursiones a América del Sur, implementando estrategias para satisfacer y dar un mejor servicio a los clientes.

---

[1]Muñoz de Escalona y Lafuente, F. (2003). *El Turismo explicado con claridad.* Libros en Red.

En marzo de 1954 emerge la *Agencia Ariel*, fundada por el señor Luis Alonso Rendón, quien posteriormente abre TUREX (Turismo y Excursiones). Don Ernesto Valencia, empleado de *Panamerican*, compró junto con León Ávila, *El Salvador Travel Service*, formando la empresa Ernesto Valencia y Compañía, siendo la primera en bridar servicio de oficina de viajes en los años 1956 y 1957.

Los señores Alfredo Morales, Cesar Hernández y Antonio Angulo fundaron la *Agencia de Viajes Morales*, en 1961. Derivándose en 1974 la agencia *Amor Tours*, la cual se dedicaba al transporte terrestre de pasajeros. En los años 1970 a 1975, existió una afluencia bastante considerable, debido entre otras cosas a la realización del concurso Miss Universo.[2]

A finales de los años 70 y principios de los 90, se suscitó la Guerra Civil en El Salvador, a pesar de la paralización en la inversión pública y privada en el país, el sector se benefició por la venta de boletos por la migración de la población a países como Canadá, Suecia y Australia.

1.1.3 **Uso de la tecnología de información y surgimiento del control interno informático.**

En un principio, las aerolíneas que disponían de gran capital y recursos invirtieron grandes sumas en la creación de sistemas computarizados de reservas (CRS) que, se orientaban a la comercialización de los boletos de las compañías asociadas. Sólo las grandes empresas tuvieron la posibilidad de implantar en sus negocios los costosos ordenadores y programas que facilitaban el acceso. A finales del siglo XX para reducir costos y agilizar la gestión de datos de los involucrados, se diseñaron los Sistemas de Distribución Global (GDS) que permiten realizar reservas hoteleras, aéreas, cruceros, renta de carros, entre otros.

Con la generalización del uso del ordenador, las oficinas fueron aceptando estas herramientas de trabajo e incorporando programas que agilizaran la gestión y el acceso a información. En sus primeras fases la aplicación sistemática más usual era la gestión de los datos generados por la actividad del propio negocio, como clientes, ingresos, gastos, productos y expedientes.

Un segundo escalón en el tejido de redes informáticas; fue la conexión de varios ordenadores periféricos situados en distintos puntos de ventas con otro central, para compartir datos y facilitar la comercialización de productos y servicios turísticos.

---

[2]Benítez, M.R., Lara, G.A., Menjívar, M.A. (2003) *El control financiero como una herramienta para la toma de decisiones de las agencias de viajes del área metropolitana de San Salvador.* Tesis. UTEC, San Salvador, El Salvador.

Con la aparición de buscadores de ofertas de última hora, las múltiples páginas web de datos turística, las compañías aéreas de bajo costo que no tienen otros puntos de ventas más que internet, la implantación del billete electrónico y la propia intangibilidad que define el producto turístico, han permitido tejer un panorama confuso donde la revolución informática plantea indudables oportunidades, pero también profundas amenazas.

Por esta razón, se aprovecha el uso de la Tecnología de la Información (TI) para mejorar la gestión, automatizando los procesos y así dedicar conocimiento y tiempo en atención al cliente, brindando beneficios a través del uso de internet como: cobertura, agilidad, inmediatez, reducción de costos en los procesos de venta, conocimiento de compradores, elaboración de paquetes a la medida y comunicación directa con el usuario.

Se puede visualizar, paralelo al desarrollo de la TI, el surgimiento de los controles internos informáticos, con el propósito de vigilar que las actividades diarias cumplan los procedimientos, normas y estándares fijados por la dirección, formando parte de la gestión de la empresa. La Informática no gestiona propiamente la empresa, sino que ayuda a la toma de decisiones.

1.1.4 **Asociación de Auditoría y Control en Sistemas de Información (en inglés ISACA).**

En 1967, un grupo de personas dedicadas a la auditoría de controles en sistemas, detectaron que estos se estaban volviendo cada vez más críticos para las operaciones de sus respectivas organizaciones, por lo que se reunieron para discutir la necesidad de tener una fuente centralizada de información y guias en el tema.

En 1969, este grupo se formalizó, incorporándose bajo el nombre de Asociación de Auditores de Procesamiento Electrónico de Datos (EDP *Auditors Association*). En 1976 la EDP creó una fundación de educación para llevar a cabo proyectos de investigación de gran escala, para expandir los conocimientos y el valor en el campo de gobierno y control de TI.

Para el año 2013 los integrantes se contabilizaban por más de 115,000 distribuidos en más de 180 países y cubren una variedad de puestos profesionales; por ejemplo auditor de Sistemas Informáticos (SI), consultor, profesional de la educación, especialista en seguridad de SI, regulador, director ejecutivo de información (CIO) y auditor interno. Trabajan en casi todas las categorías de industrias, incluyendo finanzas y banca, contabilidad pública, gobierno y sector público, servicios y manufactura.

Esta diversidad facilita que los miembros aprendan unos de otros, e intercambien puntos de vista muy diferentes sobre una variedad de tópicos.

Desde sus inicios, se ha convertido en una organización global que establece las pautas para los profesionales en gobierno, control, seguridad y auditoría de la información. Sus estándares de auditoría y control de SI son seguidos en todo el mundo. Sus investigaciones abordan temas que son desafíos para sus integrantes[3].

1.1.5 **Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT).**

Para la primera y segunda edición, la Universidad Libre de Ámsterdam (Europa), Universidad Politécnica de California (Estados Unidos de Norte América) y Universidad de Nuevo Gales del Sur (Australia) se encargaron de la compilación, estudio, revisión, e incorporación apropiada de los estándares técnicos internacionales, códigos de conducta, estándares de calidad, estándares de auditoría, las prácticas, requisitos de la industria y como estos se relacionan con el marco y con los objetivos del control,

Para el desarrollo de la tercera edición los investigadores analizaron cada punto, modificaron los objetivos de control, y agregó el desarrollo de las pautas de la gerencia. La consolidación de los resultados fue realizada por el comité de dirección de COBIT.

Las pautas, fueron desarrolladas usando un panel mundial de 40 expertos de la academia, gobierno, del aseguramiento, del control y de la seguridad. Ellos participaron en un taller residencial dirigido los facilitadores profesionales y usando las pautas del desarrollo definidas por el comité de dirección de COBIT; el cual fue apoyado fuertemente por el grupo y *PricewaterhouseCoopers*, quienes no sólo proporcionaron la dirección del pensamiento sino también envió sus expertos en control, gerencia de funcionamiento y seguridad de la información. Los resultados fueron los modelos de madurez, los factores críticos del éxito, indicadores dominantes de la meta y del funcionamiento para cada uno de los objetivos de alto nivel del control. Esta fue publicada en julio de 2000.

La cuarta edición se publicó en diciembre de 2005, ayudando a llevar las directrices de gobierno TI a más ejecutivos de negocio. La versión 4.1 fue publicada en mayo de 2007.

---

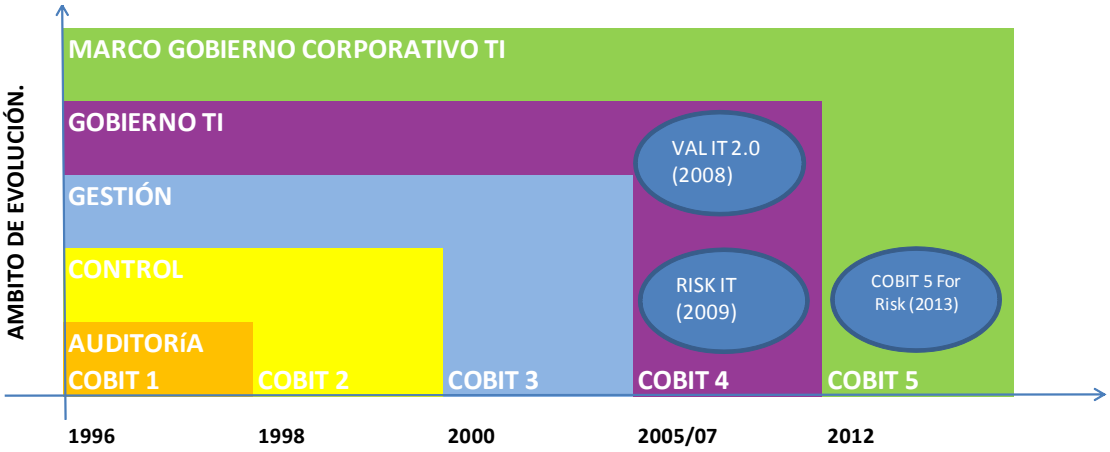
[3]http://www.isaca.org/spanish/Pages/default.aspx

El 10 de abril del 2012, ISACA lanzó la nueva edición de este marco de referencia. Siendo COBIT 5 la última del *framework* mundialmente aceptado, el cual proporciona una visión empresarial del Gobierno de TI que tiene a la tecnología y a la información como protagonistas en la creación de valor para las empresas; en el 2013 lanzan COBIT 5 For Risk.

COBIT 5 se basa en COBIT 4.1, y a su vez lo amplía mediante la integración de otros importantes marcos y normas como Val IT y *Risk* IT, *InformationTechnology Infrastructure Library* (ITIL) y las normas ISO relacionadas.

En la siguiente imagen, se puede apreciar la evolución del marco normativo a través de los años y la incursión de nuevos conceptos.

Cuadro No 1 Evolución de COBIT.



Fuente: COBIT.

1.2 CONCEPTOS.

1.2.1 Definiciones.

A continuación, se presentan algunas de importancia relativa:

Agencia de viajes: son entidades dedicadas a la intermediación entre el turista y el consumo turístico, incluyendo no solo los bienes y servicios que demanda, sino también la combinación de productos y paquetes, e incluso los destinos que el cliente elige para sus vacaciones.

Aplicaciones: se entienden como sistemas de información que integran procedimientos manuales, como aquellos basados en tecnología y que dan soporte a procesos de negocio.

BSP: Plan de liquidación bancaria implantado por las compañías aéreas, para la cancelación de los boletos emitidos por las agencias de viajes.

Controles compensatorios: son aquellos que surgen, cuando una entidad no puede cumplir con un requisito explícitamente de la manera establecida, debido a restricciones técnicas o comerciales legítimas y documentadas pero ha mitigado suficientemente el riesgo asociado con este; a través de la implementación de otros controles, llamados pruebas de cumplimiento.

Evaluación de riesgo: identifica las amenazas, vulnerabilidades y riesgos de la información, sobre la plataforma tecnológica de una organización, con el fin de crear un plan de implementación de los controles que permitan un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información.

Gestor de reservas (GDS): sistemas informáticos de reservas que abarcan varias áreas del sector turístico: boletos de avión, hoteles, alquiler de autos, entre otros.

Fraude: es un delito que tiene como objetivo inutilizar, destruir, alterar o suprimir datos, programas e información computarizada, sus inicios datan del año 1960 cuando fue diseñado un dispositivo destructivo mediante la utilización del lenguaje ensamblador, causando daños en la información almacenada en computadoras por medio de virus polimorfos, gusanos, virus del sector de arranque; entre otros.

IATA: la Asociación de Transporte Aéreo Internacional, por sus siglas en inglés, es el instrumento de cooperación entre aerolíneas, promoviendo la seguridad, fiabilidad, confianza y economía en el transporte aéreo en beneficio económico de sus accionistas privados.

Paquete turístico: se refiere al conjunto de servicios en el exterior que puede incluir o no, el boleto aéreo; tratarse de una reserva de hotel, renta de auto, tramite de visa, traslados en el destino o tarjeta de asistencia en caso de emergencia.

***Phishing* (fraude electrónico):** es una técnica que utilizan los delincuentes para obtener información personal, con el fin de causar daños; la cual consiste en hacerle creer a la víctima que se encuentra en una página de confianza y así obtener sus datos personales.

Políticas: son reglas de comportamiento definidas para la interacción entre usuarios y los activos informáticos, son independientes de los ambientes propios de la entidad y representan la base de un modelo de seguridad.

Procedimientos: es la descripción detallada de la forma como se implanta una política. El procedimiento incluye todas las actividades requeridas, los roles y responsabilidades de las personas encargadas de llevarlos a cabo.

Prueba de penetración (*Pen Test*): consiste en una evaluación activa de las medidas de seguridad de la información. El propósito es detectar los puntos débiles que puedan ser capitalizados para violar cualquiera de las tres condiciones necesarias: confidencialidad, integridad y disponibilidad.

Riesgo operativo: Es la posibilidad que se produzcan pérdidas debido a eventos originados en fallas o insuficiencia de procesos, personas, sistemas internos, tecnología y presencia de situaciones imprevistas externas.

Sistema de información automatizado: es la columna vertebral de cualquier organización, porque éstos son los que procesan transacciones y hacen posible la realización de actividades de administración y operación, controlando diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijadas por la dirección de la organización y/o la dirección informática, así como los requerimientos legales.

1.3 CICLO DE OPERACIONES DE LAS AGENCIAS DE VIAJES.

Cada agencia de viajes tiene distintas maneras de realizar sus actividades económicas, depende si son mayoristas o minoristas, si venden boletos, paquetes u otros servicios. Sin embargo estas operaciones siguen el mismo patrón descrito a continuación:

En primer lugar el cliente solicita de forma presencial, vía telefónica, correo o redes sociales uno de los dos tipos de servicios: boleto o paquete turístico, donde es atendido por el asesor de viajes siguiendo el protocolo definido por la agencia, para identificar el producto que necesita. Se consulta en el gestor de reservas la disponibilidad y precios, explicándole los requisitos migratorios y de salud requeridos para ingresar al destino.

1.3.1 **Venta de boletos.**

Al obtener la aceptación del cliente, el asesor realiza una última verificación de fechas, nombres, entre otros datos. Existen tres formas de pago para los boletos:

- ✓ Tarjeta de crédito del cliente, el boleto se carga directamente y se le cobra aparte el servicio administrativo.
- ✓ Crédito, se pasa la solicitud al departamento de créditos y cobros, el cual le realiza un estudio crediticio para calificar y aprobar al cliente.
- ✓ En efectivo, se pasa directamente a caja.

El asesor llena la solicitud de facturación donde detalla toda la información del cliente y el servicio prestado, para emitir el respectivo documento como: factura consumidor final, de exportación o comprobante de crédito fiscal.

Al cierre diario, facturación traslada a contabilidad los documentos para revisión y registro, y al departamento de BSP para efectuar la conciliación con el reporte semanal que envía IATA de los boletos emitidos. Es de aclarar que aquellos que se facturan al crédito y al contado, son los que se liquidan en el reporte. Los cargados a la tarjeta de crédito del cliente, no tienen otra intervención, porque en el gestor de reservas se liquidan directamente a las aerolíneas.

Terminada la conciliación por parte de BSP, se solicita a Finanzas la programación del pago de la liquidación, la cual debe elaborarse a más tardar ocho días después de la recepción del reporte. Cometer

un error en la retribución o no realizarla, implica para la agencia, el retiro de la acreditación por parte de IATA.

Finanzas, hace los movimientos necesarios para obtener los fondos suficientes para la liquidación de la solicitud. Asegurándose que ya se encuentren disponibles, se procede a elaborar la transferencia y se pasa a las autorizaciones respectivas.

1.3.2 **Venta de paquete turístico.**

De la misma manera como se describió anteriormente la interacción del cliente con el asesor de reservas, se determina la cantidad de servicios requeridos. El agente propone al cliente paquetes preparados que comprenden desde el boleto aéreo, alojamientos y seguros de viaje. Si este no se acomoda a su necesidad, se procede a investigar con los proveedores tarifas y disponibilidades. Luego de proponer el precio del paquete, el solicitante decide si acepta la oferta o si requiere una nueva cotización que se adapte a su necesidad.

Si está de acuerdo, en caso de requerir boleto aéreo, se le solicita el depósito por el monto de los boletos a emitir. El agente se comunica con el proveedor a través de los medios que esté haya dispuesto para gestionar las reservas (correo electrónico, uso de sistemas en línea o vía telefónica). Ya confirmados los servicios, se procede a ingresar la información de todo el paquete, dentro del sistema interno de gestión de reservas: nombres de pasajeros, servicios requeridos, fechas de pago al proveedor, costos, fechas de viaje y forma de pago.

Se revisa para validar la información, si todo se encuentra en orden, se autoriza la documentación para la respectiva facturación, gestionando el cobro ya sea al contado o tarjeta de crédito. Si se trata de venta al crédito, se le delega al departamento de Créditos y Cobros.

El agente de reservas emite los voucher y reconfirma con los proveedores los servicios, con el propósito de disminuir el riesgo de cancelación de los mismos. Se entregan los voucher a los pasajeros.

En contabilidad, se examinan las obligaciones con los proveedores y se programan los egresos con el departamento de tesorería, para asignar los fondos necesarios. Algunos proveedores solicitan que los desembolsos sean efectuados con días de anticipación. Otros consideran enviar quincenal o mensualmente estados de cuentas para que se cancelen posteriormente.

Ya asignados, contabilidad efectúala preparación de los pagos, pasa las revisiones y autorizaciones respectivas. Estos deben realizarse en un tiempo prudencial, en función de no afectar los servicios de los pasajeros. Así termina el ciclo de operación.

Es necesario mencionar la participación de la tecnología de la información en las operaciones de las agencias de viajes, intervienen sistemas predeterminados por el proveedor de boletos-reservas (AMADEUS y SABRE), asimismo algunos de ellos han diseñado sus propios sistemas para la gestión de los servicios; por lo tanto, la participación del recurso humano también es indispensable. En consecuencia, el nivel de riesgos informáticos es latente.

1.4 EL PAPEL DEL CONTADOR PÚBLICO EN EL CONTROL INTERNO INFORMÁTICO.

El papel del profesional en contaduría pública, sobre el área de control interno informático, es sustentado a través de las siguientes normativas:

IEPS o Normas Internacionales de Formación para Contadores Profesionales, define las buenas prácticas en la formación y desarrollo de la profesión, así también indica los estándares de referencia que se espera de los organismos miembros a IFAC. Implica la creación de habilidades y estrategias que facilitan a los individuos aprender eficazmente, para luego utilizarlas a lo largo de su vida profesional.

Su objetivo principal en la contaduría pública, es la preparación de profesionales competentes, capaces de contribuir a la profesión a lo largo de su carrera y a la sociedad en donde se desempeñan.

De acuerdo a IEPS 2, para que el profesional en contaduría pública desarrolle sus competencias ante un entorno cambiante y complejo, debe instruir su conocimiento principal en tres áreas, las cuales se mencionan en el cuadro No. 2.

De acuerdo a la norma, se espera que los profesionales en contaduría pública, participen dentro de los equipos de TI en los puestos de gerente, diseñador, evaluador de sistemas o un combinado de cada área. Esta competencia le permite utilizar los sistemas y herramientas para resolver los problemas de la empresa y la contaduría, demostrar comprensión de los negocios y sus sistemas contables.

Según al párrafo 2 de la Norma Internacional sobre Servicios Relacionados, establece que el profesional puede desempeñar el trabajo solicitado, cuando cumpla con el conocimiento adecuado y los criterios razonables para emitir su conclusión.

Cuadro No 2 Áreas de competencia profesional del contador público.

Áreas:	Relacionado con:
Contabilidad y finanzas.	• Historia de la profesión. • Estructura de Informes. • Conocimiento de normas internacionales.
Organizacional y de negocios.	• Entendimiento sobre cómo funciona la entidad, su administración y operación • Entendimiento del entorno del negocio, economía, ética y toma de decisiones
Conocimiento de tecnologías de información.	• Oportunidad de formar parte del equipo de diseño, gestión y evaluación de los sistemas. • Conocimiento general y de control de TI. • Competencias de control y de usuario de TI.

Fuente: Elaboración propia, de acuerdo a lo establecido en IEPS 2.

Por lo expuesto anteriormente, es un campo abierto y pueden ofrecer como servicio de consultoría la evaluación y diseño del control interno en TI, utilizando los métodos que en la educación continua, adquirió para la realización de su trabajo, con el objeto de expresar una conclusión sobre el uso de las TI.

1.5 OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS.

Para las empresas, la información constituye un recurso clave, en el cual la tecnología juega un importante rol en almacenarla, distribuirla y analizarla. Esta ha evolucionado de forma omnipresente en el desempeño empresarial, en los medios sociales, públicos y de negocios.

Los Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT 5) suministran una red integral que apoya a las entidades en el logro de sus objetivos para la gobernación y administración de la tecnología de información. En otras palabras, crea el óptimo valor de TI, manteniendo un balance entre la obtención de beneficios y la optimización de los niveles de riesgos y uso de los recursos.

En el tema de riesgos, existe una guía que suministra los detalles necesarios para la gestión de estos en todos los niveles de la compañía.

El uso de este marco normativo incrementa las capacidades de gestión del riesgo en la entidad:

- ✓ Mayor precisión en la identificación de riesgos y la medición del éxito en el tratamiento de los mismos.
- ✓ Mejor entendimiento sobre el impacto del riesgo en la empresa.
- ✓ Orientación de extremo a extremo sobre la forma de gestionar el riesgo, incluyendo un extenso conjunto de medidas.
- ✓ Conocimientos de cómo sacar provecho de las inversiones relacionadas con TI sobre prácticas de gestión de riesgos.
- ✓ Compresión sobre como el valor de la gestión de riesgo de TI, junto con procesos efectivos y eficientes, mejora la calidad y reduce los desperdicios y costos de la entidad.
- ✓ Oportunidades para integrar la gestión de riesgo de TI con el riesgo de la empresa y su estructura.
- ✓ Mejora en la comunicación y entendimiento entre las partes interesadas, tanto internas como externas, debido a un marco comúnmente aceptado.
- ✓ Promoción sobre la responsabilidad del riesgo y la aceptación sobre toda la empresa.
- ✓ Un perfil completo del riesgo, identificando la exposición total de la entidad al mismo y la mejor utilización de los recursos.

Estos beneficios se logran mediante el uso de factores llamados catalizadores. Son guiados por cascada de metas u objetivos de alto nivel. Están descritos en siete categorías las cuales se mencionan y describen en el cuadro No. 3 Catalizadores de COBIT 5.

Cuadro No 3 Catalizadores de COBIT 5.

Nivel	No.	Catalizador	Descripción
Gobierno Corp.	1	Los principios, políticas y marcos de referencia	Comprenden el vehículo principal que traduce el comportamiento deseado en la organización, a través de guías prácticas.
	2	Los procesos	Detallan el conjunto ordenado de actividades y prácticas para alcanzar los objetivos.
	3	Las estructuras organizativas	Son los encargados de la toma de decisiones clave de la entidad.
	4	La cultura, ética y comportamiento	Son el factor de éxito en las actividades de gobierno y gestión.
Recursos	5	La información	Es el elemento que hace funcionar a toda la organización, en términos sencillos, el producto clave.
	6	Los servicios, infraestructura y aplicaciones	Comprende las redes y tecnologías que proporcionan a la entidad el procesamiento de la información.
	7	Las personas, habilidad y competencias	Se relacionan al recurso humano, necesario para completar satisfactoriamente todas las actividades y en la toma correcta de las decisiones y acciones correctivas.

Fuente: basado en lo descrito en COBIT.

Dentro del modelo de referencia del proceso se contemplan dos: el gobierno y la gestión, en esta última se encuentran los dominios, que se describen de la siguiente forma:

Cuadro No 4 Dominios de COBIT 5.

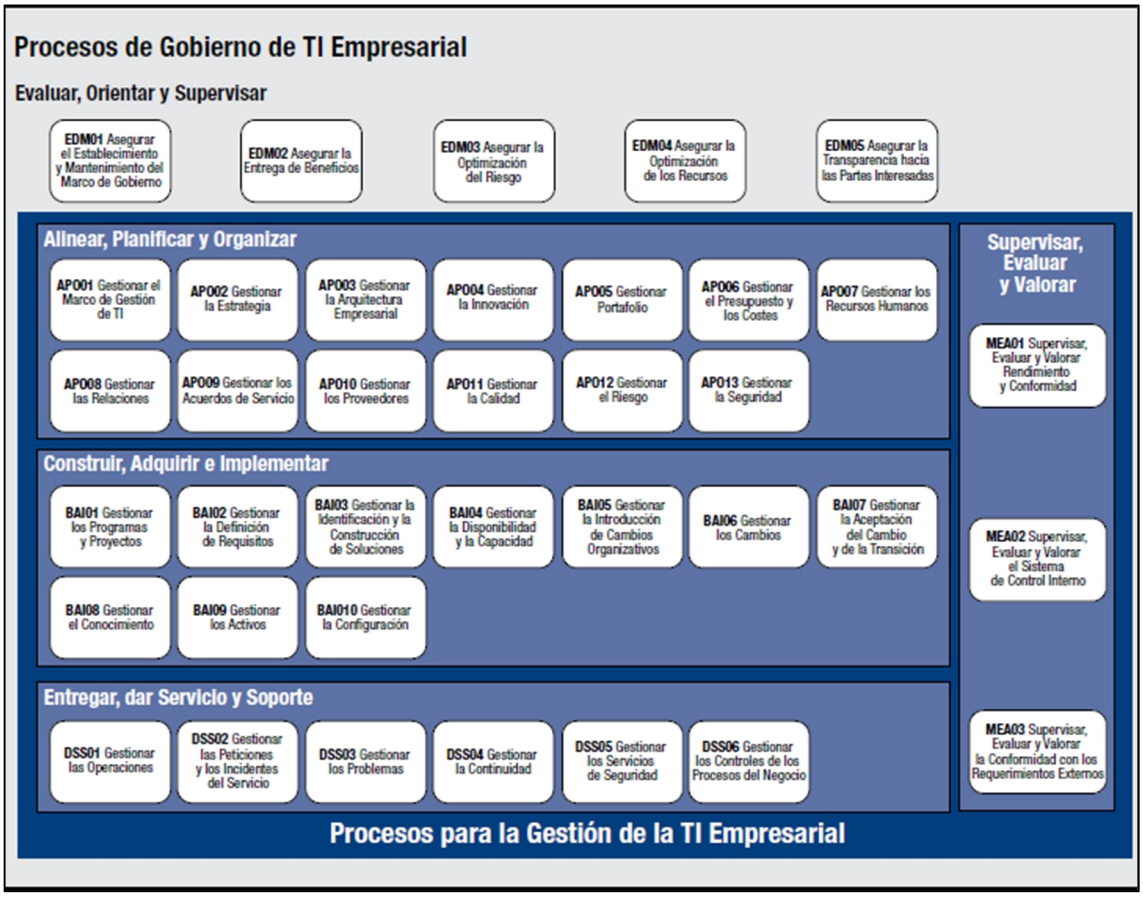
Siglas.	Acciones
EDM	Evaluar, Orientar y Supervisar. *(Evalute, Direct and Monitor)*
APO	Alinear, Planificar y Organizar (*Align, Plan and Organise*)
BAI	Construir, Adquirir e Implementar (*Build, Acquire andImplement*)
DSS	Entregar, dar Servicio y Soporte (*Deliver, Service and Support*)
MEA	Supervisar, Evaluar y Valorar (*Monitor, Evaluate and Assess*)

Fuente: basado en lo descrito en COBIT.

De los dominios mencionados en el cuadro anterior, para la elaboración de un sistema de control interno informático, se utilizarán APO, DSS y MEA.

Los procesos están situados en dominios de acuerdo con el área más relevante de actividad cuando se considera la TI a un nivel empresarial. El cuadro No. 5 muestra el conjunto de los 37 procesos de gobierno y gestión.

Cuadro No 5 Procesos de gobierno y gestión.



Fuente: ISACA, Cobit 5, (2012)

Cuadro No 6 Resumen Catalizadores de COBIT 5.

No.	Catalizador.	Información.	Gestión de rendimiento de los catalizadores (Dimensiones)			
			Partes interesadas.	Metas y métricas.	Ciclo de vida.	Buenas prácticas.
1	Principios, Políticas y Marcos de Referencia.	Se refiere a los mecanismos de comunicaciones disponibles para transmitir a la dirección e instrucciones de los cuerpos de gobierno y de dirección.	Grupos de interés, internos o externos de la empresa	Principios limitados en números y redactados en lenguaje sencillo. Políticas efectivas, eficientes y no intrusivas.		Las buenas prácticas requieren que las políticas formen parte del marco de gobierno y de gestión general
2	Procesos.	Se define como la colección de prácticas influenciadas por las políticas y procedimientos de la empresa.	Externas: clientes, socios comerciales, accionistas. Internas: el Consejo, la dirección y empleados.	Son las declaraciones que describen el resultado deseado de un proceso. Se categorizan como metas intrínsecas, metas contextuales y de seguridad-acceso.	Crea, Opera. Supervisa. Planificar Diseñar Construir Utilizar Evaluar Actualizar Actualiza o Retira.	Declaraciones sobre acciones que generan beneficios, optimizan el nivel de riesgo y el uso de recursos.
3	Estructuras Organizativas.	Este catalizador describe la estructura y los roles de la organización	Internos y Externos.	Su principal meta es incluir un mandato adecuado, principios operativos bien definidos y la aplicación de buenas practicas	Creada. Existe. Ajustada. Disuelta	Principios Operativos. Composición. Ámbito de control. Niveles de autorización. Delegación de autoridad. Procedimiento de Escalado para toma de decisiones.

No.	Catalizador.	Información.	Gestión de rendimiento de los catalizadores (Dimensiones)			
			Partes interesadas.	Metas y métricas.	Ciclo de vida.	Buenas prácticas.
4	Cultura, ética y Comportamiento.	Se refiere al conjunto de conductas individuales y colectivas dentro de una empresa.	Internos y Externos.	Ética organizativa. Éticas individuales. Comportamientos individuales, en función sobre la toma de riesgos, cumplimiento de políticas y hacia los resultados negativos.	Planificar Diseñar Construir Utilizar Evaluar Actualizar	Comunicación a lo largo de toda la compañía de los comportamientos deseados y los valores corporativos.
5	Información.	Este catalizador considera a la información relevante para la empresa, aunque no se encuentre automatizada.	Internos y Externos	Calidad Intrínseca. Calidad contextual. Accesibilidad y Seguridad	Planificar Diseñar Construir Utilizar Evaluar Actualizar	Hacer consideraciones sobre donde se almacenará la información, como se podrá acceder, como se va a estructurar, que tipo y como se va a retener.
6	Servicios, Infraestructura y aplicaciones	Trata sobre los recursos tales como las aplicaciones y las infraestructuras que están designadas en la prestación de servicios de TI	Internos y Externos	Estos se expresan en términos de servicio y niveles de servicios, tanto en el aspecto económico de la empresa y su nivel de apoyo de contribución en los procesos	Planificar Diseñar Construir Utilizar Evaluar Actualizar	Reutilización. Comprar en lugar de construir. Simplicidad. Agilidad. Aperturas.
7	Personas, Habilidades y Competencias	Enfoque al recurso humano.	Internos y Externos	Niveles de educación y capacitación al personal, habilidades técnicas y experiencia.	Planificar, Diseñar, Construir, Utilizar Evaluar Actualizar	Definición de requisitos de formación requeridos para cada papel dentro de la compañía.

Fuente: COBIT 5.

1.5.1 **Enfoque de riesgo en tecnologías de información (TI).**

Riesgo, se define como la eventualidad que imposibilita el cumplimiento de un objetivo. Enfocándolo con el tema de la tecnología de información, este se plantea como amenaza, determinando el grado de exposición a la ocurrencia de una pérdida.

La Organización Internacional por la Normalización (ISO) define riesgo tecnológico como: "La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole pérdidas o daños". [4]

De la definición anterior, se identifican varios elementos: probabilidad, amenazas, vulnerabilidades, activos e impactos; estás se describen a continuación:

Probabilidad: establecer la posibilidad de ocurrencia, puede realizarse de manera cuantitativa o cualitativa, pero siempre considerando que la medida no debe contemplar la existencia de ninguna acción moderadora, tomando en cada caso qué posibilidades existen que la amenaza se presente independientemente del hecho que sea o no contrarrestada.

Amenazas: son acciones que pueden ocasionar consecuencias negativas en la operatividad de la entidad. Comúnmente se indican como amenazas a las fallas, a los ingresos no autorizados, a los virus, uso inadecuado de software, los desastres ambientales como terremotos o inundaciones, accesos no autorizados, facilidad de acceso a las instalaciones, entre otros.

Vulnerabilidades: son condiciones inherentes a los activos, presentes en su entorno, facilitando que las amenazas se materialicen, mediante el uso de las debilidades existentes, sin embargo estas últimas no causan ningún impacto sino se identifica una vulnerabilidad.

Activos: los relacionados con tecnologías de información, ejemplos típicos son: los datos, el hardware, el software, servicios, documentos, edificios y recursos humanos.

Impactos: las consecuencias de las distintas amenazas son siempre negativas. Las pérdidas generadas pueden ser financieras, no financieras, de corto plazo o de largo plazo.

---

[4]Guías para la gestión de la seguridad de TI /TEC TR 13335-1, 1996

1.5.2 **Gestión de riesgo.**

Como herramienta de diagnóstico para establecer la exposición real a los riesgos por parte de una organización, se recurre a lo que se llama gestión de riesgos. Este análisis tiene como objetivos identificar los riesgos y lograr establecer el riesgo total, luego el residual, tanto en términos cuantitativos o cualitativos.[5]

Cuando se refiere al riesgo total, se trata de la combinación de los elementos que lo conforman. Comúnmente se calcula el valor del impacto promedio por la probabilidad de ocurrencia para cada activo y amenaza.

De esta manera se obtiene, para cada combinación válida de activos y amenazas:

RT (riesgo total) = probabilidad x impacto.

A este cálculo se debe agregar el efecto de medidas mitigantes de las amenazas, generándose el riesgo residual, que es el remanente luego de la aplicación de acciones destinadas a disminuir los riesgos existentes. Las medidas mencionadas son aquellas que generalmente se conocen como controles, que se abordan en el tema 1.6 Control interno informático.

El riesgo residual es una medida del riesgo total remanente luego de contemplar la efectividad de las acciones mitigantes existentes. Sin embargo no es sencillo cuantificar adecuadamente los riesgos. Por lo anterior es que usualmente se utiliza un enfoque cualitativo, expresando los riesgos en altos, medios y bajos, o en niveles similares.

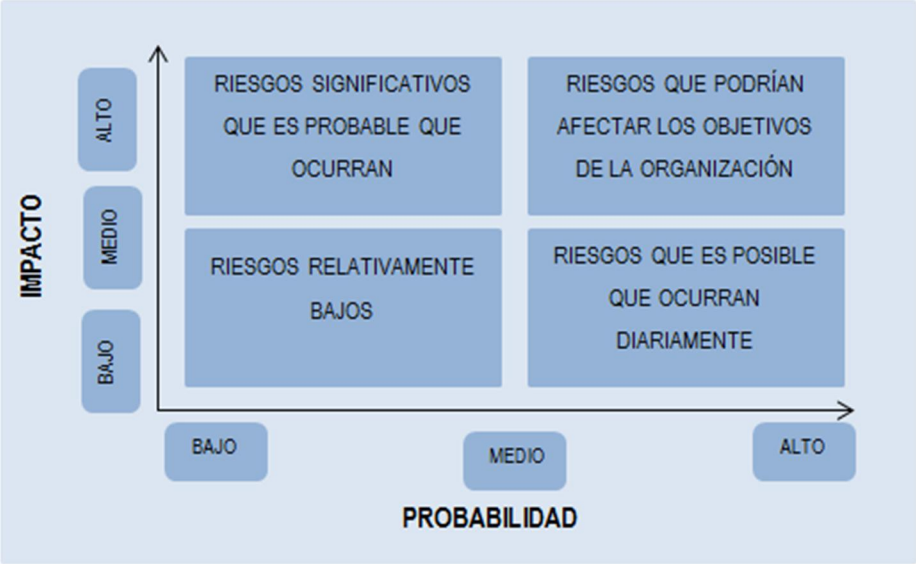
Una herramienta usada es el mapa de riesgo, que es una representación gráfica que traza en sus ejes estimaciones cuantitativas y cualitativas de la probabilidad e impacto de uno o más riesgos que podrían afectar a la organización. Estos se representan de manera que los más significativos (mayor probabilidad e impacto) resaltan, diferenciándose de aquellos menos significativos (menor probabilidad e impacto).

---

[5] Introducción a Riesgo Informático, FCEA, Agosto de 2004, L. Sena, S.M. Tenzer.

De acuerdo con el nivel de detalle y la profundidad del análisis, los mapas de riesgo podrían representar la probabilidad y el impacto general esperado, o bien incorporar un elemento de variabilidad. En el siguiente cuadro se ilustra el diagrama conceptual del mapa de riesgo.[6]

Cuadro No. 7 Diagrama conceptual del mapa de riesgo.



Fuente: Fonseca, Oswaldo (2011) *Sistemas de control interno para organizaciones.* Perú: Instituto de Investigación en Accountibility y Control.

Por lo tanto, la gestión del riesgo se resume en cinco etapas:

- Identificar las actividades principales o activos.
- Determinar la amenaza: factores de riesgo o riesgos inherentes.
- Establecer la probabilidad de ocurrencia del riesgo
- Evaluar el impacto: un cálculo de los efectos potenciales sobre el capital o las utilidades de la entidad.
- Respuesta al riesgo

[6] Fonseca, Oswaldo (2011) *Sistemas de control interno para organizaciones.* Perú: Instituto de Investigación en Accountibility y Control.

Matriz de Riesgo.

El proceso de análisis descriptivo genera un documento que se conoce como matriz de riesgo, donde se ilustran todos los elementos identificados, sus relaciones y cálculos realizados. La sumatoria de los riesgos residuales calculados es la exposición neta total de la organización a los riesgos, bajo el supuesto que el resultado obtenido es positivo. Caso contrario, se establece que se encuentra cubierta de todos los riesgos analizados, sin embargo, es ineficiente porque tiene muchos controles que realmente necesita.

Realizar el análisis es indispensable para lograr administrar adecuadamente los riesgos. Implica gestionar los recursos de la empresa para lograr un nivel de exposición determinado, el cual es establecido por el tipo de activo, permitiendo menor exposición cuanto más crítico es éste.

La matriz es un punto clave en analizar y determinar los riesgos en el manejo de los datos e información de las organizaciones. Esta no brindará un resultado detallado sobre los conflictos y peligros de cada recurso (elemento de información) de la institución, sino una mirada aproximada y generalizada de los mismos.

Debe tomarse en cuenta que el análisis de riesgo detallado, es un trabajo muy extenso, porque requiere que se compruebe todos los posibles daños de cada recurso de una institución contra todas las posibles amenazas.

Lo que se pretende con el enfoque de la matriz es localizar y visualizar los recursos de una organización, que están en peligro de sufrir un daño por algún impacto negativo, y posteriormente tomar las decisiones y medidas adecuadas para la superación de las vulnerabilidades y la reducción de las amenazas.

Evaluar el cumplimiento y la efectividad de las medidas de protección requiere del levantamiento constante de los registros sobre la ejecución de las actividades, los eventos de ataques y sus respectivos resultados. Estos tienen que ser analizados frecuentemente. Dependiendo de la gravedad, el incumplimiento y el sobrepasar de las normas y reglas, requieren sanciones institucionales para los funcionarios.

En el proceso continuo de la gestión de riesgo, las conclusiones que salen como resultado del control de riesgo, funcionan como fuente de información, cuando se entra otra vez en el proceso del análisis de riesgo.

El siguiente cuadro muestra una ilustración de matriz de riesgos, donde se evalúa el área de Sistemas e Infraestructura, identificando la magnitud del impacto y la probabilidad de amenaza. La cual será necesaria ajustar y aplicar en el desarrollo de la propuesta en el capítulo 3.

Cuadro No 8 Ilustración de Matriz de análisis de riesgos.

Matriz de Análisis de Riesgo					**Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]**											
	Clasificación				**Actos originados por la criminalidad común y motivación política**											
Sistemas e Infraestructura	**Acceso exclusivo**	**Acceso ilimitado**	**Costo de recuperación (tiempo, económico, material, imagen, emocional)**	**Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]**	**Allanamiento (ilegal, legal)**	**Persecución (civil, fiscal, penal)**	**Orden de secuestro / Detención**	**Sabotaje (ataque físico y electrónico)**	**Daños por vandalismo**	**Extorsión**	**Fraude / Estafa**	**Robo / Hurto (físico)**	**Robo / Hurto de información electrónica**	**Intrusión a Red interna**	**Infiltración**	**Virus / Ejecución no autorizado de programas**
					0	0	0	0	0	0	0	0	0	0	0	0
Equipos de la red cableada (router, switch, etc.)																
Equipos de la red inalámbrica (router, punto de acceso, etc.)																
Cortafuego																
Servidores																
Computadoras																
Portátiles																
Programas de administración (contabilidad, manejo de personal, etc.)																
Programas de manejo de proyectos																
Programas de producción de datos																
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)																
Impresoras																
Memorias portátiles																
PBX (Sistema de telefonía convencional)																
Celulares																
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)																
Vehículos																

Fuente: Solarte S. Francisco Nicolás Javier, Universidad Modular Abierta y a la Distancia, Colombia, http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_5_matrices_y_mapas_de_riesgo.html

1.5.3 **Respuesta al riesgo: optimización según COBIT 5.**

La introducción del concepto de "optimización de riesgos" como objetivo de gobierno, muestra una clara evolución frente al enfoque tradicional de "mitigación de riesgos", basada en la visión clásica de la auditoría. Este cambio de visión se debe a que las organizaciones hoy se desempeñan en entornos cada vez más dinámicos, cambiantes y competitivos, donde la búsqueda constante es la maximización sustentable de beneficios, y la optimización de recursos.

COBIT 5 define el concepto como: "garantizar que los riesgos para el negocio relacionados con TI no exceden el nivel aceptable establecido por la dirección y que el impacto de los riesgos inherentes a TI que podrían afectar al negocio son gestionados y que la probabilidad de potenciales incumplimientos a leyes es minimizada."[7]

1.5.4 **Matriz de control interno informático.**

Posterior a la gestión de riesgos, se procede a crear los controles (tema desarrollado en 1.6 Control interno informático), luego para relacionar cada control se construye una matriz donde se citan los riesgos detectados y se organizan de una manera lógica los controles para cada recurso o activo.

El siguiente cuadro es un ejemplo de visualización de la matriz, es útil mencionar que depende del criterio del profesional el agrupar los controles en la intersección de las celdas.

En el cuadro No. 9, se entiende que el recurso "Documentación contable" puede ser protegido del riesgo "Fraude/estafa", utilizando los controles 6, 8 y 9, los cuales deben ser detallados en una lista determinada. Esta lista de controles es definida por el profesional.

---

[7] COBIT 5 *For Risk*.ISACA

Cuadro No 9 Ilustración de matriz de control interno informático.

	RIESGOS	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Fraude / Estafa	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión
RECURSOS / ACTIVOS	**Documentos**	Control 1					
	Finanzas						Control 13
	Documentación contable			Control 6, 8 9			
	Precios de productos				Control 45, 48		
	Correo electrónico						Control 18, 20
	Bases de datos clientes	Control 20 al 30					
	Bases de datos proveedores			Control 3, 6			
	Página Web interna (Intranet)					Control 45, 50	
	Respaldos		Control 5, 9, 25				

Fuente: Controles Internos para sistemas de computación, Jerry Fitzgerald, Editorial Limuza, México.

1.6 CONTROL INTERNO INFORMÁTICO.

Son actividades realizadas de forma manual o automática para prevenir y corregir irregularidades que puedan afectar el funcionamiento de un sistema para lograr sus objetivos. Existen diversas clasificaciones, tales como los preventivos, detectivos y correctivos.[8]

La misión es realizar el control diario de las actividades de sistemas de información, cumpliendo los procedimientos, estándares y normas fijados por la dirección de la organización y/o la informática, así como los requerimientos legales. Su función es asegurarse que las medidas de los mecanismos implantados por cada responsable sean correctas y válidas.

Suele ser un órgano *staff* de la dirección del departamento de informática y está dotado de las personas y medios materiales óptimos para esta función. La diferencia entre el control interno informático con respecto al tradicional es la especialización del primero con respecto a la tecnología de información, mientras que el segundo engloba a todos los procesos que ejecuta la entidad.

[8]Solano, O.J. (2012) *Referencias teóricas para la construcción de un marco Teórico en el estudio del sistema de control interno Informático en ambiente computacional en la organización*. Universidad del Valle.

Sus principales objetivos:

- ✓ Controlar que todas las actividades se realicen cumpliendo los procedimientos y normas fijados, evaluar su bondad y asegurarse del cumplimiento de las normas legales.
- ✓ Asesorar sobre el conocimiento de las normas.
- ✓ Colaborar y apoyar el trabajo de auditoría informática, así como de las externas al grupo.
- ✓ Definir, implantar y ejecutar mecanismos y controles adecuados del servicio informático.

1.6.1 **Clasificación general de los controles**

Controles Preventivos.

Controles diseñados para prevenir y disuadir eventos indeseables, antes de que suceda una intrusión en el sistema. Por ejemplo, mediante el uso de software de seguridad que impida accesos no autorizados a un sistema.

Controles Detectivos.

Cuando está sucediendo una intrusión, los sistemas activados alertan la existencia de un intruso, basándose en los eventos que han sido disparados. Es en esta situación, en la que actúan los controles detectivos, durante la intrusión, cuando los controles preventivos han fallado. Por ejemplo, una reconfiguración dinámica de las reglas del firewall, un bloqueo de cuenta de usuario después de varios intentos de inicio de sesión fallidos, registros de actividad diaria para detectar errores u omisiones.

Controles Correctivos.

Los controles correctivos facilitan la recuperación de un sistema a su estado anterior, es decir, retornar al sistema al estado que tenía antes del ataque o intrusión, en el menor tiempo posible. Por ejemplo, utilizar estrategias de copia de seguridad y planes de recuperación. También se pueden implementar controles correctivos en base a la experiencia de intrusiones ya ocurridas, al analizar las causas y debilidades que las ocasionaron.

1.6.2 **Tipos de controles internos según ISACA.**

Según ISACA se dividen en generales y de aplicación, es necesario asegurarse de que existen suficientes controles para mitigar los riesgos y que están operando con la efectividad necesaria para proveer información confiable.

Los controles generales.

Son los que están inmersos en los procesos y servicios de TI. Algunos ejemplos son: desarrollo de sistemas, administración de cambios, seguridad y operaciones de cómputo.Son comunes a las diferentes actividades del departamento de informática. Los aspectos más significativos que cubren son los que se detallan a continuación.[9]

a) Plan de organización y realización de operaciones.

La redistribución de funciones que antes se realizaban de forma independiente comporta un debilitamiento en la consistencia del control interno, si no se adoptan los oportunos controles compensadores. Para ello es fundamental una cuidada planificación de la organización, la distribución de las funciones y la definición de responsabilidades. Los departamentos de organización e información han de estar debidamente relacionados dentro del organigrama de la empresa para coordinar adecuadamente sus funciones.

Es conveniente la definición del sistema de información y de un plan estratégico de la empresa, que partiendo de los medios actuales establezca los sucesivos proyectos a emprender, evalúe alternativas y asigne prioridades, en orden de optimizar la utilización de los recursos informáticos.

La organización interna del Procesamiento Electrónico de Datos (en adelante PED). es difícil de generalizar; de todas formas debe existir un manual que disponga la debida segregación de las funciones y responsabilidades básicas: planificación, desarrollo y programación de proyectos, mantenimiento de aplicaciones, explotación, archivo, control, uso de la información.

---

[9] Poch Ramón (1997), *Manual de control interno: los circuitos informativos en la administración empresarial.* Ediciones Gestión 2000, S.A. Barcelona

En cualquier caso, su diseño y concreción habrá de efectuarse atendiendo a cada organización en particular, en función de su dimensión, centralización del “hardware”, y modalidades de proceso utilizadas.

Son igualmente de aplicación, los procedimientos de rotación del personal y exigencia de vacaciones anuales. El control de la localización y responsabilidad sobre el “hardware” distribuido por toda la entidad es fundamental, en previsión del riesgo de uso indebido.

b) Desarrollo y documentación de aplicaciones.

La complejidad y especialidad de los sistemas informáticos requiere la existencia y seguimiento de unas normas y metodología de ejecución de las tareas relativas a las diferentes etapas de su desarrollo: concepción, estudios de oportunidad, autorización, análisis funcional y orgánico, programación, prueba y autorización, implantación y mantenimiento. Es necesario implicar a los propios usuarios en el desarrollo de los proyectos mediante su participación en comités de dirección y de control de los mismos.

Las grandes organizaciones informáticas precisan la implantación de un sistema de control de proyectos pendientes y en curso, que permita planificar la adecuada asignación de recursos y controlar debidamente su carga de trabajo, coste y productividad.

Deben establecerse documentos y procedimientos normalizados de análisis y programación que faciliten la realización de las tareas. La documentación relativa a cada aplicación formara un expediente, que permitirá su revisión, dando una mayor seguridad y permitirá independizar la relación de cambios, mantenimiento y perfeccionamiento de los programas.

El desarrollo de un diccionario de datos es un elemento de gran utilidad para optimizar el conocimiento y la utilización de la información elaborada.

c) Controles propios del equipo (hardware) y de los programas (software): el PED lleva incorporado procedimientos intrínsecos de control cuyo grado de seguridad depende de las especificaciones del propio fabricante. Los más comunes son:
    1. Paridad de bits: control automático de cualquier pérdida de las señales binarias que componen los caracteres.
    2. Doble lectura sucesiva y validación de todos los datos contenidos en soportes de información antes de iniciar su tratamiento.

3. Registro cronológico de todas las operaciones realizadas por el ordenador, con indicación de quien se ha ejecutado.
4. Control de secuencia: en los procesos que deben ser realizados siguiendo un orden secuencial, el programa comprueba su seguimiento.
5. Aviso de sobrecarga: el programa avisa cuando, como consecuencia de cálculos aritméticos más complejos de lo previsto, campo reservado a totales ha resultado insuficiente y el dato de salida es erróneo.
6. Control de archivos: comprobación de que la etiqueta de los archivos es la adecuada según las instrucciones del programa.
7. Control de registros: ante todo proceso que implica la lectura integra de un fichero, puede disponerse un mecanismo que compruebe que el número de registros leídos coincida con el de existentes.

d) Controles de acceso.

Para salvaguardar la integridad de la información y su adecuada utilización, se limita el acceso del personal a los diferentes elementos del sistema. Especialmente en los sistemas basados en el empleo de terminales operados por los propios usuarios debe establecerse un riguroso cuadro de controles de acceso y de incompatibilidades.

En cada caso hay que limitar el acceso a los archivos de datos y bibliotecas de programas, tanto en función de los terminales de que se trate como del propio personal. Definida las funciones y necesidades de información de cada empleado o grupo de empleados, se les otorga un código de identificación o “password”, que el ordenador requerirá ante cualquier acción que se le solicite.

Este control es muy importante en la actualidad, puesto que los procesos interactivos permiten a los usuarios tener acceso a bases de datos de utilización general que no deben autorizarse indiscriminadamente. Para incrementar la seguridad, también existen técnicas de identificación basadas en la voz y huellas dactilares del usuario.

El acceso a la sala del servidor central suele, igualmente, limitarse a aquellos empleados que desarrollan labores especificas en las mismas.

e) Control de datos y procedimientos.

Debe definirse y establecerse una función de control del trabajo del PED, que alcance a la recepción de datos para su proceso, garantice su completo tratamiento, efectué el seguimiento y corrección de los errores detectados durante el mismo y se responsabilice de la distribución de los resultados entre los usuarios.

El almacenamiento y rotación de memorias de alto almacenamiento deben estar perfectamente controlados, tanto en informática como por procedimientos, mediante etiquetas de identificación, registro de inventario, documentación de rotación y recuentos físicos. Periódicamente ha de revisarse el diario de operaciones con el objeto de detectar acciones no autorizadas.

En los sistemas de cierta dimensión es aconsejable implantar la función de administrador de datos, al que le incumben el control de la integridad y seguridad de la información. Participa en el desarrollo de nuevas aplicaciones, controla la evolución de los sistemas existentes y revisa la eficaz organización de las bases de datos.

f) Seguridad física.

Es importante la adopción de medidas de seguridad en prevención de accidentes o destrucción intencionada de soportes que pueden ocasionar un grave quebranto en la empresa. Las precauciones básicas a tal objeto son:

- Deben mantenerse en otro lugar, duplicados de todos los archivos, programas y documentación básica.
- Protección contra excesos de humedad, variaciones de temperatura, caídas de tensión, cortes de suministro, campos magnéticos, actos delictivos, entre otros.
- Protección contra incendios, inundaciones, desastres naturales, entre otros.
- Plan de emergencia que prevea las actuaciones básicas y medios alternativos disponibles ante distintos niveles de sucesos catastróficos.
- Designación de un responsable de seguridad y revisión periódica de la operatividad de los medios dispuestos.
- Seguro que cubra el riesgo de interrupción del negocio y el costo de recuperación de datos.

Controles de aplicación

Consisten en actividades manuales o automatizadas que aseguran que la información cumple con ciertos criterios, los que COBIT refiere como requerimientos de negocio para la información. Estos criterios son: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento, confiabilidad.

Se establecen para proporcionar una seguridad razonable de que los objetivos que la gerencia establece sobre las aplicaciones, se alcanzan. Estos objetivos se articulan típicamente a través de funciones específicas para la solución, la definición de las reglas de negocio para el procesamiento de la información y la definición de procedimientos manuales de soporte.[10]

a) De entrada: la confianza en el equipo es muy alta pero el problema de la entrada continua de datos afecta a todas las personas y máquinas relacionadas con la información. Asimismo la información de las salidas debe ser controlada, no debe ser enviada a aquellos que no están autorizados para recibirla. Los errores en los datos de entrada pueden producirse por cuatro razones:
   - Pueden estar registrados incorrectamente en el punto de entrada
   - Conversión incorrecta del lenguaje de la máquina.
   - Pueden haberse perdido y/o que toda la información haya sido procesada.
   - Y por último que la lectura del ordenador haya sido incorrecta.

   Se pueden establecer en tres puntos distintos de un sistema de PED.

   - En el punto en que los datos son convertidos al lenguaje de la máquina.
   - En el punto en que los datos entran al ordenador.
   - En los puntos en los cuales la información es manejada, movida o transmitida en la organización.

[10] Poch Ramón (1997), *Manual de control interno: los circuitos informativos en la administración empresarial.* Ediciones Gestión 2000, S.A. Barcelona

El número y tipo de controles estará en función de la capacidad y tipo de aplicación del ordenador.

b) Sobre la información de salida: su función es determinar que los datos procesados no incluyan alteración desautorizada por la sección de operación del sistema de P.E.D. y que los datos sean correctos o razonables. Uno de los controles más importantes en cualquier sistema tiene lugar cuando la información de salida es revisada antes de llevarla fuera del proceso de datos. Los departamentos que utilizan la información detectan errores en el empleo de información. Asimismo es importante tener un informe de distribución de los datos de salida y asegurar que la información llega solo a aquellas personas que están autorizadas.

c) De proceso: el programa debe garantizar no solamente la ejecución de todas las operaciones necesarias, sino además que estas se relacionen en el orden preciso.

Los errores se pueden agrupar en:

1. Errores en los programas: no solo puede ir en el programa sino que también puede originarse al corregir otro error, modificar incorrectamente un programa pudiendo ser esta modificación intencionada o accidental
2. Errores en el procesamiento del ordenador: al detectarse un error en el procesamiento, este puede interrumpirse o continuar en programas que requieren mucho tiempo de proceso. Es interesante incluir puntos de repetición de corrida, pudiendo así aprovechar el procesamiento realizado y sin tener que empezar de nuevo.
3. Errores cometidos por el operador, puede introducir errores como: conectando incorrectamente los contactos de la consola, montando archivos incorrectos, montando datos incorrectos de operaciones, colocando los archivos de operaciones en una pieza del equipo equivocado.

d) Sobre el hardware: los equipos de procesamiento electrónico de datos actuales poseen un elevado grado de fiabilidad. Este grado de confianza puede verse afectado por fallos mecánicos o de alguna parte electrónica de la máquina.

1.6.3 **Diseño del sistema de control interno informático.**

Para la creación de un sistema de control interno informático, se siguen los siguientes pasos:

1. Conocimiento de la entidad a través de su planeación estratégica y áreas operativas, e identificar las medidas de control interno informático aplicadas: en este paso el profesional utilizará técnicas para recolectar información de la entidad y su entorno, realizando entrevistas y observación directa de las actividades. Además, debido a lo especial del trabajo, debe enfocarse en indagar sobre las medidas de control interno informático que actualmente está aplicando, independientemente si están escritas o son empíricas, para establecer el diagnóstico preliminar. De esta manera obtendrá un panorama general, determinando problemáticas y riesgos asociados.
2. Identificación de la normativa legal relacionada a la actividad y la TI.: al obtener el conocimiento general de la entidad, el consultor debe estudiar las leyes relacionadas a la actividad del negocio. Esto con el fin de facilitar la redacción de los cuestionarios para verificar su cumplimiento e identificar posibles riesgos legales.
3. Elaboración de cuestionarios por áreas para identificar los riesgos: al completar los pasos uno y dos de este procedimiento, se elaboran cuestionarios dirigidos a cada área operativa de la entidad, con el objetivo de indagar los posibles problemas y riesgos asociados en el uso de las TI que requieren atención.
4. Evaluar los riesgos identificados: luego de identificar los riesgos detectados en los cuestionarios, se procede a evaluar la probabilidad de ocurrencia y su impacto en la entidad. Elaborando la matriz de riesgos, de acuerdo al tema 1.5.2 Gestión de riesgo, de este documento.
5. Establecer los controles internos informáticos.: finalizada la evaluación, el profesional establece la respuesta al riesgo, de acuerdo a Cobit 5 for Risk, optimizándolos por medio de controles, por lo que se enlistan en dos tipos: generales y de aplicación.
6. Elaboración de la matriz de control interno informático por área examinada: cuando los controles ya fueron establecidos, mediante el método de la matriz de control interno informático, se procede a ilustrar para cada área analizada, los controles aplicables al recurso y al riesgo relacionado, esto con el fin de relacionarlos con mayor facilidad.

Beneficios del control interno informático.

1. Proteger los activos de la empresa.
2. Obtener la exactitud y confiabilidad de la contabilidad y otros datos e informes operativos.
3. Promover y juzgar la eficiencia de las operaciones.
4. Comunicar las políticas administrativas, y estimular y medir el cumplimiento de las mismas.

1.6.4 **Políticas de control interno.**

Las políticas representan los estándares definidos por la alta gerencia de una organización. Definen las medidas y procedimientos que deben observar los usuarios al utilizar los activos y la información, con el objetivo de asegurar su salvaguarda.

Es recomendable que se actualicen por lo menos una vez al año o cuando existan cambios significativos, y deben darse a conocer a todo el personal involucrado.

Dentro de las políticas de informática se encuentran la asignación y uso de claves de acceso al sistema, el reglamento para el uso del correo electrónico, restricciones de acceso al departamento de informática, manejo de servidores, *backup* y recuperación de información, entre otros.

Las políticas de seguridad para tecnología de información son parte fundamental de las organizaciones impulsadas por la tecnología, como primer paso para construir una estructura de seguridad y control de riesgos, además de los siguientes beneficios:

- ✓ Proporciona una base uniforme, estable y formal a seguir por parte del personal.
- ✓ Se crea conciencia de los riesgos.
- ✓ Contienen reglas y lineamientos a seguir en las actividades y se evitan especulaciones, especialmente para el personal de nuevo ingreso.

Son diseñadas por la organización, deben estar hechas a la medida según los requerimientos específicos de la misma. Para su definición se realiza un proceso de validación en conjunto con todas las áreas, con el fin de generar políticas y procedimientos que se ajusten a ésta. Como punto de partida para la definición de las políticas se tiene como referencia el análisis de riesgo realizado y los controles.

Cubriendo los siguientes temas:

Seguridad de la organización	Clasificación de la Información	Seguridad Física	Administración de las operaciones de cómputo y comunicaciones
• Responsabilidades y Roles. • Políticas para la conexión con terceros.	• Responsabilidades y Roles. • Polìticas para la conexión con terceros.	• Seguridad Ambiental. • Control de acceso físico.	• Políticas de uso del correo electrónico • Uso del Internet • Uso de Recursos

Los procedimientos son el detalle que contiene la documentación de los procesos y los controles integrados en los mismos. Se derivan de las políticas y están creados para guiar a los usuarios, por lo que estos deben conocerlos a fondo. Así mismo, deben actualizarse cuando existan cambios significativos.

1.7 MARCO TÉCNICO.

A continuación se desarrollan las diferentes bases técnicas a utilizar para la elaboración de un sistema de control interno informático.

Cuadro N°10 Marco técnico.

Nombre:	Nombre detallado:	Aplicación al CII
COBIT 5	Objetivos de Control para la Información y Tecnologías Relacionadas.	Abarca las ideas generales para la creación de un sistema de control interno, englobando a la empresa en un anillo holístico que cubre todas sus áreas, utilizando los dominios: APO, encargado de gestionar estrategias, arquitectura empresarial, innovación, presupuestos, recursos, riesgo, seguridad. DSS: dominio que administra las operaciones, peticiones e incidentes de servicio, continuidad y controles de los procesos de negocio. MEA: este dominio realiza las supervisiones en cuanto a materia de rendimiento, conformidad, sistema de control interno y requerimientos externos
COBIT 5 for Risk	Objetivos de Control para la Información y Tecnologías Relacionadas 5 para Riesgos.	En lo que respecta a la identificación, análisis, y respuesta al riesgo de TI, esta guía detalla incluye lineamientos que reflejan cómo COBIT 5 soporta y asisten en la gestión y gobierno del riesgo informático y cómo implementar y mantener una función eficaz y eficiente basada en los siete catalizadores.
NISR 4400	Norma Internacional sobre Servicios Relacionados	Establece que el profesional en auditoría puede desempeñar el trabajo solicitado, cuando cumpla con el conocimiento adecuado y los criterios razonables para emitir su conclusión.

Fuente: basado en COBIT 5, COBIT 5 for Risk y Norma Internacional sobre Servicios Relacionados 4400.

1.8 MARCO LEGAL.

A continuación se destacan las leyes principales que rodean las agencias de viajes, en función de sus operaciones, y con el tema de control interno informático:

Cuadro Nº 11 Constitución de la República de El Salvador.

Legislación: Constitución de la República de El Salvador, principio: "Habeas Data"	
Artículo.	**Aplicación.**
2	Menciona el derecho a la intimidad personal y familiar en éste artículo, así los datos confidenciales deben ser resguardados.
Comentario: debido a que estas entidades manipulan bases de datos de clientes, proveedores e intermediarios, muestran vulnerabilidad al riesgo de hurto de información. Es necesario aplicar políticas de divulgación y manipulación de datos, además de procedimientos de registro y control, que garanticen la seguridad lógica dentro de la organización.	

Fuente: artículo 2 de la Constitución de la República de El Salvador.

Cuadro Nº 12 Ley de impuesto a las operaciones financieras.

Legislación: Ley de impuesto a las operaciones financieras.	
Alcance.	**Aplicación.**
La ley establece el impuesto al cheque y a las transferencias electrónicas por pagos de cualquier tipo, además el impuesto para el control de la liquidez.	El adecuado control de las operaciones financieras contempladas en la ley, disminuirá el riesgo al incumplimiento del pago del impuesto respectivo.

Fuente: Ley de impuesto a las operaciones financieras.

Cuadro Nº 13 Ley de propiedad intelectual.

Legislación: Ley de propiedad Intelectual.	
Capítulos, secciones y artículos.	**Aplicación.**
Capítulo II, Sección "E"	En el contrato pactado con el autor se establece el uso ilimitado y exclusivo de los programas de ordenador, código fuente o programa objeto, considerados por esta ley como obras literarias; obligando a las agencias proteger el software.
Capítulo III, art. 45, 49.	La entidad puede crear una sola copia del programa de ordenador, logrando también almacenar en la memoria del equipo, para el resguardo y seguridad ante cualquier amenaza de hurto de información. Además puede modificar un sistema estándar adaptándolo a sus necesidades, lo cual es fundamental cuando las agencias adquieren programas de este tipo.
Capítulo X	Establece la duración de la protección de los derechos del autor.
Comentario: la ley protege y regula la propiedad intelectual y artística, es de atención en las entidades estudiadas debido al manejo de *software* de aplicación, es necesaria la implementación de políticas que reduzcan el riesgo de alteración no autorizada al sistema, con ayuda de procedimientos que controlen a los usuarios que accesan, así mismo resguardar los dispositivos de *backups* y *usb* utilizados.	

Fuente: Ley de Propiedad Intelectual.

Cuadro Nº 14 Ley contra el lavado de dinero y de activos.

Legislación: Ley contra el lavado de dinero y de activos.	
Artículos.	**Aplicación.**
Art. 2 literal m)	La ley tiene como objeto prevenir, detectar, sancionar y erradicar el delito de lavado de dinero y de activos, así como su encubrimiento. Nombra a las agencias de viajes como sujetos de aplicación de la ley.
Comentario: es de interés realizar la adecuación de los controles de gestión, selección de proveedores, manejo de fondos en cuentas del extranjero, selección de personal honesto y responsable, protección de información de clientes y proveedores, entre otros. Estos facilitan la detección de cualquier operación, transacción, acción u omisión encaminada a ocultar el origen ilícito de valores provenientes de actividades delictivas cometidas dentro o fuera del territorio salvadoreño.	

Fuente: Ley contra el lavado de dinero y de activos.

Cuadro Nº 15 Ley de impuesto sobre la renta.

Legislación: Ley de impuesto sobre la renta.
Objeto regulado
Las rentas obtenidas en el territorio de El Salvador, son gravadas con el respectivo impuesto, la ley menciona los gastos que debe considerar como deducibles para determinar la base imponible.

Fuente: Ley de Impuesto sobre la Renta.

Cuadro Nº 16 Ley de protección al consumidor.

Legislación: Ley de protección al consumidor.	
Título I De la protección al consumidor.	**Aplicación.**
Capítulo II Derecho a la seguridad y calidad.	El alcance de la seguridad y calidad garantizada es la fiabilidad de los servicios ofrecidos por parte de las agencias.
Capítulo III Protección de los intereses económicos y sociales.	Por las ventas al crédito (plazos), cálculo de los intereses, pagos anticipados, cuando el cliente solicite la baja de un servicio, promociones y ofertas.
Capítulo IV Derecho a la información.	Los servicios ofrecidos deben tener todos los datos para que el consumidor tenga el conocimiento necesario. Así como la información de promociones.
Capítulo V Garantías y responsabilidades sobre bienes y servicios.	La garantía ofrecida por la agencia debe quedar clara. La responsabilidad es solidaria con el facilitador de los servicios.
Comentario: como proveedor de un servicio, las agencias de viajes tienen la responsabilidad de responder ante cualquier insatisfacción, reclamo o denuncia de un cliente, es necesario tener procedimientos que guíen al gestor de ventas y demás personal involucrado para responder con eficiencia y eficacia.	

Fuente: Ley de Protección al Consumidor.

Cuadro Nº 17 Ley de impuesto a la transferencia de bienes muebles y a la prestación de servicios.

Legislación: Ley de impuesto a la transferencia de bienes muebles y a la prestación de servicios.	
Título y Capítulo.	**Aplicación.**
Título I Hechos generadores del impuesto, Capítulo IV Prestaciones de servicios.	Es de estudio debido a que estas entidades realizan la actividad de prestación de servicio de intermediación, la regulación exige el control fiscal de los documentos que amparan el hecho generador contemplado.
Título IV Determinación de la obligación tributaria.	El diseño de procedimientos que colecten la documentación contable para respaldar las ventas y compras son necesarios al determinar la base imponible.
Comentario: en los manuales de procedimientos se debe considerar los requerimientos legales para sustentar el servicio de intermediación, desde el momento de la solicitud, cotización, negociación hasta la facturación y cobro.	

Fuente: Ley de impuesto a la transferencia de bienes muebles y a la prestación de servicios.

Cuadro Nº 18 Ley de turismo.

Legislación: Ley de turismo.	
Capítulos, secciones y artículos.	**Aplicación.**
Capítulo V, de los ingresos para la promoción turística. **Art. 16 – 19**	El hecho generador del impuesto se causa por dos situaciones: 1) El pago del alojamiento por parte del sujeto pasivo (5% sobre el monto gravado) 2) En la salida del territorio nacional por parte del sujeto pasivo, por vía aérea. ($7.00)
Comentario: la contribución es recaudada al momento de la realización del pago de los servicios, en su caso la liquidación a la empresa turística (hotel y aerolínea), al prestar el servicio de intermediación, la agencia de viaje debe captar la contribución y trasladarla al momento del pago a su proveedor quien es el responsable de enterarlos al Fondo General del Estado.	

Fuente: Ley de turismo.

Cuadro Nº 19 Código Penal.

Legislación: Código Penal.	
Artículo.	**Trata el delito de:**
Art. 184	Violación de Comunicaciones Privadas: Descubrir los secretos o vulnerar la intimidad de otro, apoderándose de comunicación escrita, soporte informático o cualquier otro documento o efecto personal que no le esté dirigido. O si difundiere o revelare a terceros los datos reservados que hubieren sido descubiertos.
Art. 185	Violación Agravada de Comunicaciones: Si los hechos descritos en el artículo 184 se realizaren por las personas encargadas o responsables de los ficheros, soportes informáticos, archivos o registros. Se hace hincapié en el manejo de la información en las entidades ya que puede ser susceptible de robo, perdida o daño, por las personas que laboran en la empresa y que no están autorizadas, si no se encuentra protegida o resguardada.
Art. 186	Revelación de Secreto Profesional: El que revela un secreto del que se ha impuesto en razón de su profesión u oficio.
Art. 230	Infidelidad Comercial: El que se apodera de documentos, soporte informático u otros objetos, para descubrir o revelar un secreto evaluable económicamente, perteneciente a una empresa y que implique ventajas económicas.
Comentario: los delitos que se cometen en el manejo inadecuado de datos, pueden prevenirse con los debidos controles que garanticen la seguridad física y lógica en las agencias.	

Fuente: Código Penal.

Cuadro Nº 20 Código Tributario.

Legislación: Código Tributario.	
Título III Deberes y obligaciones	**Aplicación.**
Capítulo I Obligaciones formales, Sección Cuarta, Art. 92	Establece que el Ministerio de Hacienda autoriza por resolución la presentación de declaraciones tributarias mediante redes de comunicaciones como internet, medios de almacenamiento extraíbles y correo electrónico. Esta presentación disminuye errores y el uso de recursos.
Capítulo I Obligaciones formales, Sección Quinta, Art. 113.	Sostiene el uso electrónico de formularios tributarios, siempre que estos conserven lo establecido a las obligaciones formales que deben cumplir garantizando el interés fiscal. Asimismo el uso del formulario único, y se genere un número correlativo independiente en cada documento. Con la condición que la información sea transmitida en línea a la Administración tributaria.
Capítulo II, Obligaciones de Pago, Sección Tercera, Art. 156 - A	Si las entidades adquieren intangibles a personas domiciliadas deben retener en concepto de anticipo al impuesto sobre la renta el 10% a personas naturales y 5% si son distintas a ellas.
Capítulo II, Obligaciones de Pago, Sección Tercera, Art. 158	Si las entidades adquieren intangibles a personas no domiciliadas deben retener en concepto de anticipo al impuesto sobre la renta el 20%.
Comentario: si la agencia opta por la facilidad de los servicios que el Ministerio de Hacienda ofrece *on line*, es preciso que se adopten medidas para el envío o presentación de obligaciones formales, para evitar el espionaje cibernético, *malware*, robo de información, descarga de virus, publicar dirección IP, riesgo de entrar en sistemas operativos no cifrados, entre otros. En los manuales de procedimientos, considerar las obligaciones tributarias al adquirir intangibles.	

Fuente: Código Tributario.

Cuadro Nº 21 Reglamento de aplicación del Código Tributario.

Legislación: Reglamento aplicación del Código Tributario.	
Artículos.	**Aplicación.**
Art. 35	Seguridad Electrónica en DET. Respaldo virtual en base de datos del Ministerio de Hacienda así como en correo electrónico registrado, uso de firmas digitales, encriptación.
Art. 77	Cuando se utiliza un sistema de información computarizado el contribuyente debe conservar el código fuente de dicho sistema, base de datos, diagramas e informar sobre los técnicos relacionados con el sistema.
Comentario: al implementar sistemas de información para la entrada, proceso y salida de datos es necesario crear medidas de protección del software para evitar la piratería o robo de datos ingresados al sistema. Es importante conservar la información del proveedor y todo lo relacionado a la instalación legal.	

Fuente: Reglamento de aplicación del Código Tributario

.

CAPITULO II: METODOLOGÍA DE LA INVESTIGACIÓN Y DIAGNÓSTICO.

2.1 TIPO DE ESTUDIO.

Se ejecutó un estudio hipotético – deductivo, en donde se recopiló la información general del sector a investigar; posteriormente se formularon hipótesis con el objeto de explicar el problema de estudio y por último realizar su diagnóstico.

2.2 UNIDAD DE ANÁLISIS.

Las unidades de análisis consideradas en la investigación fueron dos, que a continuación se detallan:

Primero, los profesionales en contaduría pública, con domicilio en el municipio de San Salvador, quienes son los que diseñarán el sistema de control informático.

Segundo, las entidades dedicadas a las actividades de agencias de viajes del municipio de San Salvador, a fin de obtener la información apropiada de las operaciones en las cuales interviene el uso de la TI, y debido a la importancia del control sobre las mismas.

2.3 UNIVERSO Y MUESTRA.

2.3.1 **Universo.**

Se constituyó por los profesionales en contaduría pública autorizados por el Consejo de Vigilancia de la Profesión de la Contaduría Pública y Auditoría de El Salvador (CVPCPA), con domicilio en el municipio de San Salvador, personas jurídicas, tomando como base al listado que emite el Consejo actualizado al 24 de enero de 2014, y el Directorio de empresas de 2011 proporcionado por la Dirección General de estadística y Censos (DIGESTYC), presentando una población de 132 firmas que cumplen las características requeridas.

Con respecto a las agencias de viajes, la población era de 90 empresas dedicadas a esta actividad, las cuales están registradas y ubicadas en el municipio de San Salvador, del departamento de San Salvador, según listado emitido por la Dirección General de Estadística y Censos para el año 2011.

2.3.2 **Muestra.**

Al determinar la muestra de los profesionales en contaduría pública, se efectuó de forma aleatoria simple a través de selección sistemática de elementos muestrales, sobre las personas jurídicas que ejercen la profesión mencionada, y que reunieron las características previamente definidas para la población en estudio, la cual fue finita. Se determinó utilizando la siguiente fórmula estadística:

$$n = \frac{NPQZ^2}{(N-1)e^2 + PQZ^2}$$

Dónde:

n= tamaño de la muestra.

N= Población.

Z^2= Coeficiente de confianza al cuadrado.

e^2= Margen de error al cuadrado.

P= Probabilidad de éxitos de que la problemática exista.

Q= Probabilidad de fracaso.

Estableciendo los valores en la ecuación:

Variables	Valores
n	?
N	132
Z	1.96
e	0.05
P	0.96
Q	0.04

$$n = \frac{(132)(0.96)(0.04)(1.96)^2}{(132-1)(0.05)^2 + (0.96)(0.04)(1.96)^2}$$

$$n = \frac{19.4723}{0.3275 + 0.1475}$$

$$n = \frac{19.4723}{0.4750} = 40.9928 \approx 41\ Unidades$$

Con respecto a la variable de las agencias de viaje, como se manejó una población finita, se empleó la misma fórmula, por lo cual la ecuación tomó los siguientes valores.

Variables	Valores
n	?
N	90
Z	1.96
e	0.05
P	0.96
Q	0.04

$$n = \frac{(90)(0.96)(0.04)(1.96)^2}{(90-1)(0.05)^2 + (0.96)(0.04)(1.96)^2}$$

$$n = \frac{13.2765}{0.2225 + 0.1475}$$

$$n = \frac{13.2765}{0.3700} = \ 35.88 \ \approx 36 \ Unidades$$

Durante la investigación de campo, se detectó que la cantidad de unidades de la variable agencias de viajes, sufrió una disminución, en la que se pudo detectar que muchas de ellas dejaron de operar, no se dedicaban a la actividad o se cambiaron de ubicación, por lo que únicamente se pudo obtener contacto de 20 agencias, de las cuales 18 aportaron su opinión con respecto al tema y dos se abstuvieron de responder al instrumento.

2.4 INSTRUMENTOS Y TÉCNICAS UTILIZADAS.

Para el desarrollo de la investigación se utilizó la siguiente técnica e instrumento:

Técnica: encuestas; estas fueron dirigidas a los responsables de las firmas de contaduría pública y a la gerencia general de las agencias de viajes del municipio de San Salvador, del departamento de San Salvador.

Instrumento: cuestionario; se utilizó para realizar las encuestas a los sujetos en estudio.

2.5 PROCESAMIENTO DE LA INFORMACIÓN.

Una vez realizada la recopilación de la información de la encuesta, se tabuló con la herramienta ofimática Microsoft Office Excel 2010, generando análisis estadísticos y gráficos, la edición de la información se realizó a través de la aplicación Microsoft Office Word 2010.

2.6 ANÁLISIS E INTERPRETACIÓN DE DATOS.

Las preguntas establecidas en el cuestionario, individualmente se les practicaron los siguientes análisis:

Descriptivo: por medio de la presentación de los resultados obtenidos a través de tablas y gráficos.

Inferencial: de la información de los análisis descriptivos, se generalizó la población, según los resultados obtenidos de la muestra.

2.7 DIAGNÓSTICOS DE LA INVESTIGACIÓN.

Esta investigación está basada en dos grandes unidades de análisis: las firmas de contaduría pública y las agencias de viajes del municipio de San Salvador, por lo cual se elaboró un diagnóstico general y dos específicos para cada unidad.

2.7.1 **Diagnóstico General.**

Los profesionales en contaduría pública y auditoría con personería jurídica, actualmente ofrecen en su mayoría servicios de auditoría financiera. Muy pocas veces las agencias les han hecho requerimientos sobre trabajos específicos. Para los ellos, pocos de sus clientes han implementado procedimientos para detección, prevención y corrección de datos, mientras que las agencias argumentan haber implementado dichos procedimientos. En ese caso, las firmas determinan evaluar la efectividad de estos procesos, limitándose en la evaluación por medio de procedimientos de cumplimiento.

Sin embargo, se identifica cierto grado de inefectividad en los controles, porque las agencias experimentan problemas que afectan la integridad de la información que manejan, como la pérdida o hurto de datos confidenciales de los clientes, exponiéndose a niveles de riesgo bastante altos.

Las agencias desconocen que al tener bien establecidos los procedimientos de control, el nivel de exposición del riesgo informático y los problemas inherentes se verían reducidos. Esto significa una

oportunidad para las firmas de ampliar sus servicios profesionales al diseñar a la medida, los controles que requiere la agencia.

Por último, ambas unidades de análisis consideran de utilidad que la creación de un modelo de control interno informático, les brindaría la guía para establecer controles más efectivos que gestionen el riesgo informático de forma optimizada.

2.7.2 **Diagnóstico firmas de contaduría pública.**

De acuerdo a la muestra de la población, se afirma que el 31.71% de las firmas han prestado servicios a las agencias de viajes, de las cuales el 84.62% fueron por auditorías financieras, seguidas por 38.46% en consultorías y 38.45% en contabilidad. Se concluye que las firmas enfocan más sus servicios en auditoría que en el ofrecimiento de servicios de consultoría.

Nº Pregunta Relacionada	**Resultado**	**Frecuencia**	
		Absoluta	Relativa
1	Contadores públicos que han prestado sus servicios a las agencias de viaje	13	31.17%
2	Tipo de servicios prestados a las agencias (Auditoría)	11	84.62%

Las firmas comentan que la mayoría de sus clientes no maneja procedimientos de control interno informático (60.98%), Por esta razón, determinan que el mayor indicio de fraude se lo proporciona la detección de operaciones ficticias (80.49%)

Nº Pregunta Relacionada	**Resultado**	**Frecuencia**	
		Absoluta	Relativa
3	Nadie de su cartera de clientes maneja procedimientos de control interno informático	25	60.98%
4	El mayor indicio de fraude lo proporciona el registro de operaciones ficticias	33	80.49%

Ellos manifiestan que si tienen la oportunidad de evaluar el control interno de una agencia de viajes, consideran que el área que tiene mayor riesgo es Ventas (68.29%), por lo que recurrirían al uso de matrices de riesgo y control (63.41%); otro aspecto importante que aplicarían es la evaluación de los controles, midiendo su efectividad a través de procedimientos de verificación y cumplimiento. Esto demuestra que los contadores poseen el conocimiento y habilidades necesarios para realizar este tipo de trabajo especializado.

Nº Pregunta Relacionada	**Resultado**	**Frecuencia**	
		Absoluta	Relativa
5	Para verificar la efectividad de los controles realizan procedimientos de verificación de cumplimiento	29	70.73%
7	La herramienta que mayor información le brinda para evaluar riesgos son las matrices de riesgo y control	26	63.41%
8	el elemento más importante para evaluar los riesgos informáticos es la evaluación de los controles	26	63.41%
9	Si tuviera la oportunidad de evaluar una agencia de viaje, el área que tiene mayor riesgo es la de ventas	28	68.29%

Las firmas no han tenido la oportunidad de aceptar solicitudes de diseño de controles internos informáticos a las agencias de viajes (68.29%), pero la mayoría muestra interés en realizar su diseño (65.85%); estos lo desarrollarían bajo el enfoque de COBIT 5 porque es el más adecuado para este tipo de requerimiento (63.41%) y agregan que la experiencia que se posee en la evaluación de los riesgos (65.85%), es factible realizarlo.

Mientras que las firmas que no están interesadas en el desarrollo de los controles, comentaron que la principal razón por la que no la aceptan es debido a que es un trabajo especializado.

Nº Pregunta Relacionada	Resultado	Frecuencia	
		Absoluta	Relativa
6	El enfoque de riesgo que tomaría para el diseño de control interno es COBIT 5	26	63.41%
10	Las firmas no han tenido la oportunidad de diseñar un sistema de control interno informático a este tipo de entidades	28	68.29%
11	Las firmas están dispuestas a aceptar una solicitud de diseño de control interno informático	27	65.85%
12	Las firmas que no están dispuestas a aceptar a proponer una oferta debido a que es un área especializada	11	78.57%
14	Un sistema de control interno informático es factible diseñarlo por el conocimiento que posee el contador público para evaluar riesgos.	27	65.85%

Finalmente, las firmas de contaduría pública opinaron que la creación de modelo de control interno informático aportaría como una guía para la evaluación y desarrollo de este tipo de controles, no únicamente a las agencias, sino también los demás sectores económicos en donde poseen participación.

Nº Pregunta Relacionada	Resultado	Frecuencia	
		Absoluta	Relativa
13	La creación de un modelo de control interno informático puede aportar como base para la evaluación de los controles interno informáticos	29	70.73%

2.7.3 **Diagnóstico de las agencias de viajes.**

La actividad comercial de las agencias de viajes está expuesta a riesgos muy complejos, todo en beneficio de la satisfacción total de los clientes que buscan los servicios de asesoría de viajes y reservas que ofrecen. El presente diagnóstico muestra la situación actual del control interno informático.

En esta unidad de análisis, se determinó que la venta de sus servicios se promueven mayormente por el uso del correo electrónico (100%) y páginas web (100%). Esto los motivó a establecer contratos de garantía con sus proveedores del exterior (61.11%), con el objetivo de asegurarse que las reservas se prestaran tal como lo requiere el cliente. Con ello se demuestra la importancia que ha conseguido la tecnología de información en las actividades comerciales de las agencias.

Nº Pregunta Relacionada	Resultado	Frecuencia	
		Absoluta	Relativa
1	Firma de contrato de garantía con el proveedor.	11	61.11%
4	Uso de correos electrónicos para promocionar productos.	18	100.00%
4	Empleo de página web para publicar sus servicios.	18	100.00%

También afirman que poseen procedimientos para la detección, prevención y corrección de datos contra códigos maliciosos (88.89%); sin embargo, han presentado problemas de pérdidas de registros por no realizar respaldos periódicos a la información que manejan, accesos no autorizados de equipos ajenos a la red corporativa, modificación no restringida a la base de datos y el robo de información por publicidad falsa en la web, lo que indica que dichos procedimientos no están diseñados de acuerdo a las necesidades de seguridad informática que demanda la compañía y no se encuentra protegida adecuadamente contra terceros.

Nº Pregunta Relacionada	Resultado	Frecuencia	
		Absoluta	Relativa
2	Si existen procedimientos para detección, prevención y corrección de datos contra códigos maliciosos.	16	88.89%
5	Frecuentemente se conectan equipos no autorizados a la red corporativa.	9	50.00%

5	Sufren perdida de datos por ausencia de respaldos de información.	6	33.33%
6	en el tema de autenticidad el problema más común es la modificación no autorizada de la información	11	61.11%
7	Si sufren robo de información por uso de publicidad falsa en la web.	5	62.50%

Las agencias han establecido procedimientos para el intercambio de información con terceros y aseguran que a la fecha no se han generado problemas de pérdida de información. Esta afirmación es contradictoria, debido a los problemas que ha presentado dentro de su organización, por lo tanto, es posible que sus procedimientos también estén deficientes.

Otros problemas que los encuestados comentan, es que poseen dificultades para el acceso remoto a sus sistemas de información y periódicamente en los reportes que ellos generan se reflejan distorsionados, con respecto al procesado. Se concluye que no han establecido un protocolo para este tipo de enlaces y no se monitorea la información que se ingresa.

Nº Pregunta Relacionada	**Resultado**	**Frecuencia**	
		Absoluta	Relativa
8	Tienen problema de disponibilidad de la información remotamente.	13	72.22%
9	Los reportes que se generan son distintos a la información procesada.	6	33.33%

Ellos consideran que las causas de los problemas descritos, son ocasionados principalmente por el uso de sistemas obsoletos y ausencia de mantenimiento de los equipos existentes; opinan que para resolverlos se limitarían en la adquisición de nuevos equipos y brindar el mantenimiento respectivo a los que puedan ser considerados rescatables, concluyendo que desconocen que la aplicación de controles internos pudieran facilitar la solución a los inconvenientes generados y minimizar las inversiones que se requieren al realizar ese tipo de adquisiciones.

Nº Pregunta Relacionada	Resultado	Frecuencia	
		Absoluta	Relativa
10	La unidad de análisis considera que los problemas se generan por falta de mantenimiento a los equipos utilizados.	6	33.33%
10	Se generan por uso de equipos obsoletos.	8	44.44%
11	Se pueden solucionar comprando equipos más recientes.	8	44.44%
11	Se solucionan brindándoles mantenimiento a los equipos.	6	33.33%

Finalmente, los encuestados muestran su interés en la creación de un modelo de control interno informático dirigido a su sector, que les brindaría elementos de control a la información que se utiliza dentro de su actividad.

CAPÍTULO III DESARROLLO DE CASO PRÁCTICO: DISEÑO DE SISTEMA DE CONTROL INTERNO INFORMÁTICO BASADO EN RIESGO DE TI PARA LAS AGENCIAS DE VIAJES.

La Agencia de Viajes Perico, presentó un problema de fraude por parte de dos de sus asesores de viaje, lo cual fue detectado al momento de solicitar el pago a un proveedor que no existía. El asesor falsificaba las ventas para aumentar su comisión, creaba estados de cuenta falsos del supuesto proveedor del exterior, y de esta forma solicitaba el pago a favor de otro beneficiario, desviando los fondos. Esta operación la realizaron por cinco meses generando pérdidas de USD$20,000.00, aparte de gastos procesales y de investigación. Es de mencionar que estas operaciones ficticias afectaron la razonabilidad en los estados financieros, exponiendo a la empresa a una fiscalización por parte del Ministerio de Hacienda.

En vista de la amenaza, la gerencia general le ha hecho el requerimiento a CG Consultores, para que asesore en materia de control interno informático. En una primera entrevista, se detectó que los problemas se vinculaban al uso de la tecnología de información, por el empleo de correo electrónico, internet, gestores de reservas y software aplicativo para realizar las operaciones. Por lo que se determinó entre ambas partes la realización de un Sistema de Control Interno Informático basado en riesgos, el cual ayudará a reducir los riesgos en las operaciones y garantizar la razonabilidad de las cifras que presentan los estados financieros de la entidad.

3.1 DISEÑO DEL SISTEMA DE CONTROL INTERNO INFORMÁTICO.

Para la creación de un sistema de control interno informático se requiere seguir los siguientes parámetros:

1. Conocimiento de la entidad a través de su planeación estratégica y áreas operativas, e identificar las medidas de control interno informático aplicados: para esto se usaran cuestionarios los cuales están enfocados a obtener el conocimiento general de la entidad, su entorno, actividad económica, áreas de operaciones en las que está dividida, uso de tecnologías de información y factor humano. Así mismo servirán para examinar los controles ya existentes y tener un panorama de los riesgos a los que enfrenta.
2. Identificación de la normativa legal relacionada a la actividad y la TI. Es esencial el conocimiento de la leyes aplicables, se enfocara en aéreas puntuales, lo cual no indica que las no mencionadas son inaplicables, para efectos de este caso se trató de enmarcar únicamente las leyes que relaciona a las TI y a la agencia de viaje.

3. Elaboración de cuestionarios por áreas para identificar los riesgos. Luego de identificadas las aéreas operativas de la empresa y el conocimiento general, se construyen cuestionarios por unidades de operación, esto para tener claro el panorama de las actividades y detectar riesgos.
4. Evaluar los riesgos identificados, luego de identificar los riesgos informáticos se procede a construir la matriz de riesgos, donde se refleja el riesgo total que surge de valorar la probabilidad versus el impacto. Lo cual permitirá por medio del mapa de calor generado en la valuación detectar aquellos riesgos que necesitaran especial atención para optimizarlos.
5. Establecer los controles internos informáticos. Luego de la gestión del riesgo se crean los controles de acuerdo al resultado de la valuación. Estos controles se dividen en generales y de aplicación.
6. Elaboración de la matriz de control interno informático por área examinada. Seguido de crear los controles, es necesario aplicar el método de la matriz de control interno, lo cual servirá para identificar con mayor rapidez la forma de optimizar un determinado riesgo para un explícito activo o recurso.

3.2 DESARROLLO DEL REQUERIMIENTO:

3.2.1 Conocimiento de la entidad y medidas de control interno informático aplicados.

Para el conocimiento de la entidad se concertó una cita con el gerente general de la agencia, de la cual se obtuvieron los siguientes apuntes:

Sumaria A-1 Conocimiento preliminar

CLIENTE: Agencia Perico, S.A. de C.V.	**Elaborado por AC**
TIPO DE TRABAJO: Diseño de un sistema de control interno informático basado en riesgos.	
AREA A EXAMINAR: Conocimiento preliminar.	
CEDÚLA NARRATIVA DE LA PLANEACIÓN GLOBAL DE LA COMPAÑÍA	

Para conocer de manera general la planeación global de la compañía, fue necesaria la concertación de una cita con el gerente general de la agencia, para obtener de primera mano dicha información. También se requirió la realización de una inspección visual sobre cada departamento de la entidad, para asegurar que la descripción obtenida tiene concordancia por lo comentado por gerencia general

Visión

Promover con liderazgo los mercados turísticos, a través de la creación de las oportunidades de negocio, por medio de procesos de mejora continua; favoreciendo a nuestros clientes y a la empresa.

Misión

Brindar soluciones de viaje con la amabilidad, eficiencia y compromiso, a través de una atención de calidad hacia nuestros clientes.

Objetivo General: Brindar un servicio de calidad a nuestro clientes, generando de esta forma la confianza y satisfacción.

Los departamentos de la empresa son los siguientes, descritos en orden alfabético:

BSP: es el encargado de realizar la verificación de los boletos emitidos a través de los GDS, cuya liquidación final corresponde de la agencia a IATA. Supervisa que hayan sido emitidos de acuerdo a las reglas establecidas.

Caja y facturación; son responsables de la emisión de la documentación fiscal requerida por el cliente y por el fisco. Se encargan de la custodia del efectivo que ingresa a la entidad, y con ello liquidan las facturas. También son las responsables de la custodia de la caja chica.

Contabilidad: este departamento pilar en la compañía, mantiene el control de las operaciones, validando que las operaciones de pago se hagan de manera razonable, cuidando los recursos de la compañía y haciendo el registro correspondiente de las actividades diarias que se realizan. También validan las operaciones de ingresos, a través de la revisión de las reservas que se generan y se facturan a los clientes.

Créditos y Cobros: su función principal es realizar los análisis crediticios suficientes para determinar si el cliente es apto para otorgarle financiamiento, así como realizar la gestión de cobro de las facturas pendiente de pago.

Finanzas: son los responsables de custodiar y registrar todo lo relacionado a las cifras de la compañía, la asignación de los pagos, realización, registro y almacenamiento de las operaciones y la presentación de los estados financieros.

Gerencia General: el responsable de las riendas del negocio. Su función principal es velar por el buen funcionamiento de todas las áreas de la entidad. Tomar decisiones de acuerdo a los lineamientos que establece Junta Directiva y marcar el liderazgo que necesita la entidad para la obtención de mayores beneficios económicos.

Informática: son los encargados del buen funcionamiento de los sistemas y hardware que comprenden a la entidad. Responsables de la custodia de las bases de datos que se generan por las operaciones diarias de la entidad.

Mercadeo: se dedica a la creación de todo lo relacionado a la publicidad y promoción de los servicios que se ofrecen a la agencia.

Reservas: este departamento es el que se encarga generar los ingresos a la compañía, por medio de la venta de los servicios que esta ofrece. Responsables de brindar calidad de servicio y la atención hacia los clientes que consumen los productos promovidos. Constituyen también los intermediarios entre los proveedores, pues ellos buscan los proveedores necesarios y realizan negociaciones con ellos con el único fin de obtener el mejor precio y servicios, de acuerdo a los requerimientos brindados por el cliente.

Siguiendo con el procedimiento, se ejecuta un cuestionario de conocimiento preliminar dividido en cinco partes, la primera que es la actividad económica de la entidad, luego el gobierno corporativo, tocando temas generales de tecnología, factor humano y riesgos y fraudes. Donde se puedan detectar los vacios y construir los siguientes cuestionarios para obtener los riesgos informáticos.

Cuestionario A-1 Conocimiento Preliminar

CLIENTE: Agencia Perico, S.A. de C.V. Hecho por: KG

TIPO DE TRABAJO: Diseño de un sistema de control interno informático basado en riesgos.

AREA A EXAMINAR: Conocimiento preliminar.

CUESTIONARIO DE CONOCIMIENTO PRELIMINAR

No.	PREGUNTAS	RESPUESTA			
		SI	NO	N/A	COMENTARIOS
	ACTIVIDAD ECONÓMICA				
1	¿Cual es la fuente de los ingresos?				Venta de reservas de boletos aéreos y paquetes turísticos.
2	¿Obtiene otros ingresos y de que actividad?		X		
3	¿Cual es el monto promedio de los ingresos anuales de los últimos cinco años?				Desde el año 2010 al 2014 asciende a $600,000.00
4	Indique el número de establecimientos.			X	Solo tiene un establecimiento.
5	Canal que utiliza para vender sus servicios.				Venta directa, a mayoristas y a detallistas.
	GOBIERNO				
6	¿El gobierno de la empresa se reúne periódicamente para reflexionar sobre el futuro de la empresa (a 3 ó 5 años) y definir la estrategia a seguir?	X			Dos veces al año.
7	¿Se elaboran presupuestos que integran los objetivos de la empresa y los medios para alcanzarlos?	X			
8	¿Se dispone de un cuadro de mando mensual con la evolución de las variables clave (ventas, gastos, flujo de caja)?	X			Se tienen metas de ventas mensuales contempladas en el presupuesto anual y se controlan para su cumplimiento. En cuanto al flujo de caja se preocupan por tener la disponibilidad para pagar la IATA y demás obligaciones. Los gastos se revisan mensualmente, pero no establecen estrategias para reducirlas.
9	¿Se controlan oportunamente dichas variables clave?	X			
10	¿Se elaboran de forma continua previsiones de caja a 1 año como mínimo?	X			
11	¿Se obtienen estados financieros a los pocos días de la finalización de cada mes?	X			Después de los primeros diez días hábiles de cada mes se emiten los definitivos.
12	¿Se conocen los márgenes por producto?	X			
13	¿La estructura jurídica es la más conveniente?	X			
14	¿Se cumple la legislación vigente en todas las áreas de la empresa?	X			
15	¿Existe un manual de normas que, de acuerdo con los objetivos de la empresa, define todas las funciones y las relaciones entre los distintos puestos de trabajo?		X		
16	¿La entidad posee organigrama?	X			
17	¿A que fecha esta actualizado el organigrama?				Se encuentra actualizado al 2013, sin embargo no han ocurrido modificaciones significativas en su estructura.
18	¿Existe un control interno adecuado para verificar que se cumplen los procedimientos previstos y para proteger los activos de la empresa?		X		
19	¿Existe una adecuada descentralización y delegación de funciones?		X		
	TECNOLOGÍA				
20	¿La edad media del equipo de oficina es inferior a 7 años?		X		Hay equipo de computo que usa software desfasado
21	¿El equipo de oficina está en buen estado?		X		
22	¿La superficie destinada a la producción del servicio es la correcta?	X			
23	¿Los sistemas de información son correctos en cuanto a volumen, precisión y puntualidad?	X			
24	¿Se utilizan convenientemente las posibilidades de la informática?		X		
25	¿Que tipo de sistema de información posee actualmente?				ERP, diseñado a la medida
26	¿Existen contratos de mantenimiento para el sistema aplicativo?	X			
27	¿Utiliza sitios web como parte del negocio?	X			
28	¿Utiliza correos electrónicos como parte del negocio?	X			
29	¿Se destinan recursos suficientes a las actividades de investigación y desarrollo?		X		

Cuestionario A-1 Conocimiento Preliminar

CLIENTE: Agencia Perico, S.A. de C.V. Hecho por: KG

TIPO DE TRABAJO: Diseño de un sistema de control interno informático basado en riesgos.

AREA A EXAMINAR: Conocimiento preliminar.

CUESTIONARIO DE CONOCIMIENTO PRELIMINAR

No.	PREGUNTAS	RESPUESTA			
		SI	NO	N/A	COMENTARIOS
	FACTOR HUMANO				
30	¿Tiene la empresa un líder indiscutible?	X			
31	¿La selección de dirigentes y cuadros se hace en función de su competencia?		X		
32	¿Los puestos de trabajo están correctamente definidos y se les atribuyen objetivos personales?	X			
33	¿El clima organizacional en general es bueno?	X			
34	¿Se utilizan círculos de calidad o similares?		X		Se reúne el comité para evaluar el rendimiento de las áreas.
35	¿Cual es la cantidad de empleados laborando a la fecha?				30 empleados
36	¿La pirámide de edades por categorías de personal es normal?	X			
37	¿La antigüedad media del personal en la empresa es inferior a 14 años?	X			
38	¿La tasa de absentismo (faltas) es normal?	X			
39	¿Los sueldos, salarios y otras remuneraciones son correctos en relación al sector?	X			
40	¿La promoción interna y la formación profesional son suficientemente cuidadas?		X		
41	¿Se ha previsto un plan de sucesión en caso de que algún directivo clave se retire de la empresa?	X			
	RIESGOS Y FRAUDES				
42	¿Dispone la empresa de cobertura suficiente en los seguros para salvaguarda de activos y para hacer frente a todo tipo de responsabilidades?	X			
43	¿Es auditada la empresa por profesionales externos?	X			
44	¿Se ha registrado evento de fraude o robo en los últimos cinco años?	X			
45	¿Se tienen planes y controles internos para la detección de fraudes en la empresa?		X		
46	¿En general, se hacen evaluaciones de los riesgos del negocio?	X			Si se evalúa el riesgo pero no se contemplan medidas para optimizarlos.

El siguiente cuestionario es para identificar controles internos informáticos que la agencia aplica, debido a que manifestaron no tenerlos por escrito.

Con el resultado de este examen, se podrán verificar los vacíos que existen en cuanto a controles que optimicen riesgos.

Cuestionario A-2 Medidas de control interno informático

CLIENTE: Agencia Perico, S.A. de C.V.
TIPO DE TRABAJO: Diseño de un sistema de control interno informático basado en riesgos.
AREA A EXAMINAR: Identificación de medidas de control interno informático.

CUESTIONARIO PARA IDENTIFICAR MEDIDAS DE CONTROL INTERNO INFORMATICO

No.	PREGUNTAS	SI	NO	N/A	COMENTARIOS
	HARDWARE				
1	¿Posee la entidad un inventario de equipo informático.?		X		
2	¿La infraestructura de la entidad proporciona seguridad al equipo informático?	X			
3	¿Existe seguridad en el voltaje y cableado en las instalaciones eléctricas en la entidad?	X			Verificación a nivel de servidor y equipos existente del voltaje, ups y cableado.
4	¿Existe plan de mantenimiento para el equipo informático?		X		Les dan mantenimiento cuando presentan problemas.
5	¿El personal que provee el mantenimiento es externo o interno?				Interno.
6	¿Se cuenta con el equipo apropiado para la protección de las computadoras y terminales?	X			
7	¿Se cuenta con vectores de errores para evaluar el buen funcionamiento del hardware (identificar principales fallas)?		X		Si el problema no puede ser solucionado por el personal interno, se solicitan servicios externos.
8	Indique la frecuencia del mantenimiento del equipo informático.			X	
	SOFTWARE				
9	¿El aplicativo instalado posee la respectiva licencia?	X			El ERP lo tiene dado que es construcción propia. El resto de aplicaciones como el de ofimática, de 20 equipos solo 12 cuentan con su respectiva licencia.
10	¿Se efectúan pruebas a los sistemas antes de instalarlos?	X			El departamento de informática lo instala y verifica su funcionamiento antes de notificar al usuario que dispone de la aplicación.
11	¿Se documentan las pruebas efectuadas a los sistemas?	X			
12	¿Cuando se adquirió el sistema aplicativo, se documentó el requerimiento apropiadamente?	X			
13	¿Las modificaciones al sistema aplicativo son autorizadas por la alta gerencia?	X			
14	¿Las modificaciones al sistema aplicativo son documentadas?	X			
15	¿Existe software de seguridad para los sistemas instalados (firewall, antivirus, administración, acceso)?	X			
	PROCESAMIENTO DE DATOS				
16	¿Se controla la captura de datos?		X		
1	¿Se evalúa la autenticidad de los datos o de la información capturada?		X		
17	¿Existen controles para verificar la exactitud de los datos?		X		
18	¿Se evalúa la totalidad de los datos?		X		
19	¿Existen controles para evitar la redundancia de los datos?		X		Se ha pagado a proveedores dos veces.
20	¿Se controla la periocidad de cambios de acceso al sistema?		X		No se reestructuran password ni perfiles ni roles.
21	¿Existen políticas y procedimientos aplicados al control interno del procesamiento de datos?		X		
22	¿El sistema genera informe de excepciones?		X		
23	¿Se transfiere la información de forma oportuna entre los diversos módulos?		X		En ocasiones la tarifa del boleto no coincide con el dato que refleja el sistema. Aun después de realizarse la interfaz.
24	¿Existe plan de capacitación al personal en cuanto al procesamiento de datos?		X		
25	¿Cómo es la captura de datos?				Por lotes.
26	¿Existen fallos en el procesamiento?	X			
27	¿Se mantienen registros de esas fallas?		X		

Cuestionario A2 Medidas de control interno informático

CLIENTE: Agencia Perico, S.A. de C.V.
TIPO DE TRABAJO: Diseño de un sistema de control interno informático basado en riesgos.
AREA A EXAMINAR: Identificación de medidas de control interno informático.

CUESTIONARIO PARA IDENTIFICAR MEDIDAS DE CONTROL INTERNO INFORMATICO

No.	PREGUNTAS	SI	NO	N/A	COMENTARIOS
28	**SEGURIDAD FISICA**				
29	¿Existe una política de seguridad física en la empresa y está actualizada?		X		
30	¿Existen y se difunden los planes de contingencia/emergencia?	X			Existen pero no se difunden, no están escritos.
31	¿Tiene todo el personal disponible un listado con los números de teléfono de emergencia?		X		
32	¿Tiene la empresa contratos de seguros generales?	X			
33	¿Realizan capacitación sobre uso de extintores contra incendios?		X		
34	¿Existen alarmas contra robo o asalto en las instalaciones?	X			
35	¿Realizan capacitaciones sobre primeros auxilios?	X			
36	¿Existen procedimientos de evacuación del personal ante desastres naturales?		X		
37	¿Existe un comité de salud ocupacional?	X			
38	¿Se ha realizado un estudio de los riesgos de incendio que cubra tanto la prevención como la protección?		X		
39	¿Se ha hecho un estudio acerca de la posibilidad de inundaciones en la zona?		X		Es innecesario según la administración.
40	¿Existe un sistema de vigilancia de la calidad y continuidad del suministro eléctrico?	X			Se adquieren UPS de alta potencia para los equipos.
41	¿Existe un sistema de control de acceso a las salas de los equipos informáticos?	X			Los servidores se encuentran aislados y protegidos.
42	¿Existen procedimientos específicos de control de acceso para el personal ajeno a la empresa?	X			Solicitud de documento y entrega de carnet de visitante.
43	¿Las oficinas se cierran con llave y se verifica su cierre al terminar la jornada laboral?	X			Se tiene alarma de seguridad.
	SEGURIDAD LOGICA				
44	¿Existe una política de seguridad de la información en la empresa y está actualizada?		X		
45	¿Se cuenta con un back up de la información?	X			Se hace el back up diariamente.
46	¿Existen copias de la información procesada por el sistema, y éstas están resguardadas?	X			En servidor privado en la nube.
47	¿La entidad posee contraseñas adecuadas para el ingreso a los diferentes sistemas de información?	X			Se define contraseña de acuerdo a parámetros y uso de caracteres.
48	¿Se cuenta con grupos de usuarios con derechos de acceso al sistema?		X		
49	¿Se cuenta con cambios de contraseñas por defecto?		X		La contraseña la mantienen constante.
50	¿El sistema de información, está protegido ante la amenaza de virus?	X			Se tiene el antivirus.
51	¿El personal nuevo, es capacitado sobre como debe de utilizar el sistema?	X			
52	¿El personal es capacitado continuamente, sobre como debe de operar el sistema?		X		
53	¿Se mantiene una vigilancia constante de las personas, que accesan a los servidores?	X			El área está totalmente restringida a toda hora.
	RECURSO HUMANO				
54	¿Se tiene política definida para cada Perfil de usuario?	X			Se establecen roles, autorizaciones y perfiles de acuerdo con los requerimientos de la jefatura.
55	¿Se cuenta con grupos de usuarios con derechos de acceso al sistema?		X		
56	¿Se cuenta con cambios de contraseñas por defecto?		X		
57	¿Se tiene un Plan de inducción y capacitación inicial?	X			La capacitación inicial es de acuerdo a la función a desempeñar.
58	¿Existen tareas definidas para cada usuario?	X			
59	¿Con que periocidad se rota el personal?				El personal administrativo y de sistema es constante.
60	¿Todo el personal posee usuario y contraseña?	X			
61	¿Existen y se utilizan Manual de puestos?				No existen.
62	¿A que fecha están actualizados los manuales de puestos?			X	No existen manuales.
63	¿Realizan evaluación de cumplimiento de actividades asignadas?		X		No se realiza.
64	¿Se realiza capacitación por los cambios realizados en los sistemas?	X			
65	¿Se considera de forma explícita la confidencialidad?	X			Al contratar y terminar relaciones laborales se firma carta de confidencialidad.

3.2.2 **Identificación de la normativa legal relacionada a la actividad y la TI.**

Es necesario verificar la normativa legal a la que está sujeta la entidad, para identificar riesgos a los que pueda estar expuesta. Revisando la legislación aplicable a la entidad, se identificaron, listaron y explicaron cuáles son las que están sujetas, detalladas a continuación.

Cuadro B-1 Legislación aplicable

No.	LEGISLACIÓN	COMENTARIO
1	Constitución de la Republica de El Salvador, principio: "Habeas Data"	La manipulación de bases de datos de clientes, proveedores e intermediarios, muestra vulnerabilidad al riesgo de hurto de información. Es necesario revisar el cumplimiento de políticas de divulgación y manipulación de datos, además de procedimientos de registro y control, que garanticen la seguridad lógica dentro de la organización.
2	Ley de propiedad Intelectual.	Debido al manejo de *software* de aplicación, es necesaria la verificación de controles que reduzcan el riesgo de alteración no autorizada al sistema, así mismo resguardar los dispositivos de *backups* y *usb* utilizados en la instalación de programas.
3	Código Tributario y Reglamento aplicación del Código Tributario.	Al utilizar los servicios que el Ministerio de Hacienda ofrece on line, es precisa la adopción de medidas para el envío o presentación de obligaciones formales, para evitar el espionaje cibernético, malware, robo de información, descarga de virus, publicar dirección IP, riesgo de entrar en sistemas operativos no cifrados, entre otros. Si adquiere intangibles considerar las obligaciones tributarias, debido a la importancia de conservar la información del proveedor y todo lo relacionado a la instalación legal.
5	Ley de turismo.	Constatar si la contribución del 5% (hotel) y $7.00 (aerolínea) son recaudadas al momento de la realización del pago de los servicios, en su caso la liquidación a la empresa turística (hotel y aerolínea), al prestar el servicio de intermediación, la agencia de viaje debe captar la contribución y trasladarla al momento del pago a su proveedor quien es el responsable de enterarlos al Fondo General del Estado.
6	Ley contra el lavado de dinero y de activos.	Es de interés verificar la adecuación de los controles de gestión, selección de proveedores, manejo de fondos en cuentas del extranjero, selección de personal honesto y responsable, protección de información de clientes y proveedores, entre otros. Para facilitar la detección de cualquier operación, transacción, acción u omisión encaminada a ocultar el origen ilícito de valores provenientes de actividades delictivas cometidas dentro o fuera del territorio salvadoreño.
7	Ley de impuesto a la transferencia de bienes muebles y a la prestación de servicios.	Evidenciar la sustentación del servicio de intermediación, desde el momento de la solicitud, cotización, negociación hasta la facturación y cobro.
8	Ley de impuesto a las operaciones financieras.	El adecuado control de las operaciones financieras contempladas en la ley, disminuirá el riesgo al incumplimiento del pago del impuesto respectivo.
9	Ley de protección al consumidor.	Las agencias de viajes tienen la responsabilidad de responder ante cualquier insatisfacción, reclamo o denuncia de un cliente, es necesario tener procedimientos que guíen al gestor de ventas y demás personal involucrado para responder con eficiencia y eficacia.
10	Código Penal.	Para prevenir los delitos que se cometen en el manejo inadecuado de datos, deben existir controles para garantizar la seguridad física y lógica de los mismos.

3.2.3 **Elaboración de cuestionarios por áreas para identificar los riesgos.**

Cuestionario C-1 Gerencia General

CLIENTE: Agencia Perico, S.A. de C.V.
TIPO DE TRABAJO: Diseño de un sistema de control interno informático basado en riesgos.
AREA A EXAMINAR: Conocimiento de las operaciones y procedimientos del área.

CUESTIONARIO PARA GERENCIA GENERAL

No	PREGUNTAS	RESPUESTA			
		SI	NO	NO APLICA	COMENTARIOS
1	¿Existe una planificación estratégica para la agencia de viajes?	X			
2	¿Tiene establecido objetivos para la agencia?	X			
3	¿Existen políticas preestablecidas para el manejo de la agencia?		X		
4	¿Realiza reuniones con los socios para temas estratégicos?	X			
5	¿Manejan presupuestos generales?	X			
6	¿Manejan presupuestos por aéreas?	X			
7	¿Existe una duplicidad de funciones en la administración?		X		
8	¿Realizan reuniones periódicas con el personal?	X			Gerencia se reúne con los jefes cada mes. Con el resto de personal solo cuando ocurre un problema y es necesario.
9	¿Se da seguimiento a las decisiones tomadas en esas reuniones?		X		No se presentan informes de rendimiento.
10	¿Se envían las decisiones por escrito?		X		
11	¿Realizan reuniones periódicas con los socios?	X			
12	¿Están establecidos equipos de trabajo?	X			
13	¿Existe una anticipada coordinación con el personal?		X		
14	¿Se programan actividades recreacionales con el personal?	X			Dos veces al año: para el aniversario y para fiesta de fin de año y navidad.
15	¿Se ha definido procedimientos para otorgar autorizaciones?	X			
16	¿Las autorizaciones pueden ser otorgadas por otros puestos?	X			Ante la ausencia de gerencia, se delega la responsabilidad a dos personas de confianza dentro de la agencia quienes son el contador y el gerente de ventas, pero son limitadas. Los créditos a clientes solo son autorizados por el gerente.
17	¿Existen requisitos que se deban cumplir para permisos al personal?	X			Solo para tramites personales y emergencias familiares. Se debe pasar la acción de personal con dos días de anticipación, la cual es evaluada por el jefe inmediato.
18	¿Se han definido requisitos para autorizaciones en lo referente a cobros y pagos?		X		
19	¿Existe un departamento de recursos humanos?	X			
20	¿Se han establecido procedimientos para contratación de personal?		X		
21	¿Han definido procedimientos para capacitar al personal?		X		
22	¿Con que regularidad se capacitan y brinda educación continua a los empleados de la organización?				Solo se capacitan al ser contratados para utilizar el sistema aplicativo. No hay seguimiento ni retroalimentación.
23	¿Se brindan incentivos al personal?	X			Bonos por cumplimiento para jefes, obsequios para el resto del personal, precios especiales de paquetes turísticos para empleados.
24	¿Se ha implementado un sistema de promoción dentro de la compañía?		X		No existe la posibilidad de crecimiento profesional.
25	¿Se da tratamiento a las quejas y sugerencias?	X			
26	¿Existe reportes de quejas y sugerencias?		X		Se trasladan verbalmente.
27	¿Se da seguimiento a las quejas y errores del personal?	X			
28	¿Existen políticas de autorización gerencial para definir e implementar nuevos métodos de procesamiento de información?		X		
29	¿Existen procedimientos disciplinarios para empleados que han cometido una violación a la seguridad?		X		
30	¿Se encuentran documentados los procedimientos de operación de cada área?		X		

Cuestionario C-2 Administración

CLIENTE: Agencia Perico, S.A. de C.V.
TIPO DE TRABAJO: Diseño de un sistema de control interno informático basado en riesgos.
AREA A EXAMINAR: Conocimiento de las operaciones y procedimientos del área.

CUESTIONARIO PARA DEPARTAMENTOS ADMINISTRATIVOS

No	PREGUNTAS	RESPUESTA			
		SI	NO	NO APLICA	COMENTARIOS
	CONTABILIDAD				
1	¿Existe un manual de procedimientos en el área de contabilidad?		X		
2	¿Las funciones están determinadas dentro del área?	X			No están escritas
3	¿Se ha establecido un proceso de registro de las transacciones?	X			No están escritas
4	¿Se posee un control de las cuentas por cobrar?	X			La conciliación se hace una vez al terminar el mes.
5	¿Se posee un control de las cuentas por pagar?	X			La conciliación se hace una vez al mes
6	¿Se posee un control de los anticipos de clientes?		X		Se ha presentado el problema de la no liquidación de anticipos.
7	¿Se ha definido un proceso de control de registro de transacciones?	X			Por partidas fijas, variables y provisiones.
8	¿Existe un manual de archivo adecuado para los documentos contables.?		X		No hay gestión en el control del archivo.
9	¿Se registran diariamente los ingresos recibidos?	X			
10	¿Se practican arqueos de caja periódicamente?	X			Una o dos veces al mes.
11	¿Los arqueos de caja son sorpresivos?	X			
12	¿Se ha definido un proceso de capacitación en el área?		X		
13	¿En que áreas capacitan a los empleados del departamento?			X	
14	¿Se realiza revisiones de los servicios vendidos?	X			La revisión se limita a que los valores coincidan.
15	¿Se conoce los procedimientos de IATA?	X			
16	¿Se realizan conciliaciones bancarias mensuales?	X			
17	¿Se da seguimiento a las diferencias entre la contabilidad y estados de cuenta bancarias?	X			
18	¿Se da seguimiento a las diferencias entre la contabilidad y estados de cuenta de proveedores?		X		
19	¿Cantidad promedio de partidas de diario contabilizadas en el mes?				Un promedio de 1,000
20	¿Realiza operaciones exentas de IVA, no grabadas, no sujetas?	X			
21	¿Realiza transacciones con no domiciliados?	X			
22	¿Posee archivos de documentos de IVA?	X			
23	¿Concilia cuentas contables de IVA contra libros?	X			
24	¿Efectúa retenciones o percepciones?				Retenciones de IVA y de Renta
25	¿Se tiene control de las liquidaciones de tarjetas de crédito?		X		
	TESORERÍA				
26	¿Se ha diseñado un proceso de pago?		X		
27	¿Se han definido las autorizaciones correspondientes para pago en efectivo?	X			El monto máximo autorizado es de $50.00, pero si se presenta una emergencia se puede autorizar mas.
28	¿Utilizan firmas mancomunadas para las cuentas bancarias?	X			
29	¿Se realizan disponibilidades bancarias diarias?	X			
30	¿Numero promedio de cheques emitidos en el mes?				200 cheques
31	¿Cantidad promedio de pagos electrónicos en el mes?				250
32	¿Existe un procedimiento para pagos con cheque?	X			El asesor presenta el estado de cuenta y facturas para la liquidación y solicitar el pago. No se verifica la veracidad de los documentos.
	FACTURACIÓN Y CAJA				
33	¿Se ha definido un control de las facturas emitidas?	X			El control es por correlativo pre impreso
34	¿Se realizan las remesas al siguiente día laborable?		X		
35	¿Se realizan cuadres de caja diarios?		X		
	CRÉDITOS Y COBROS				
36	¿Se solicitan autorizaciones para concesión de crédito?	X			
37	¿Hay mas de una persona que autoriza financiamiento a clientes?		X		
38	¿Existe un procedimiento para conceder crédito?	X			No esta escrito
39	¿Obtienen información de otras instituciones para conceder crédito?	X			
40	¿Tienen clasificación de clientes por tiempo de pago?	X			
41	¿Identifican y separan a los clientes de mala paga?		X		
42	¿Existen procedimientos para los clientes de mala paga?	X			Después de 30 de vencido el plazo, llaman al cliente, y si no se recibe pago alguno pasa a jurídico.
43	¿Existen seguros de deuda?	X			
44	¿Posee registros con detalle para las cuentas por cobrar?	X			
45	¿Tiene políticas para las cuentas incobrables?	X			Se utilizan estimaciones
46	¿El plazo de cobro de los clientes es lo más corto posible?		X		Si el cliente es frecuente se le otorgan plazos especiales
47	¿Recibe anticipos de clientes?	X			
48	¿Se concilian las remesas o notas de abono con la facturación?		X		

Cuestionario C-3 Ventas (Reservas)

CLIENTE: Agencia Perico, S.A. de C.V.
TIPO DE TRABAJO: Diseño de un sistema de control interno informático basado en riesgos.
AREA A EXAMINAR: Conocimiento de las operaciones y procedimientos del área.

CUESTIONARIO PARA DEPARTAMENTOS VENTAS (RESERVAS)

No	PREGUNTAS	RESPUESTA			
		SI	NO	NO APLICA	COMENTARIOS
1	¿Existe un manual en el área de reservas?		X		
2	¿Se realizan reservas para todo los clientes que solicitan los servicios?		X		Algunos solo piden cotizaciones.
3	¿Se dispone de todos los datos del cliente en las reservas?		X		El asesor no completa la información
4	¿Existe un control acerca de la transcripción de los datos del cliente a la base de datos?		X		El asesor crea el código del cliente y nadie revisa la base de datos.
5	¿Existe una base de datos solida de los principales clientes?	X			Existe una cartera especial de clientes
6	¿Se tiene conocimiento acerca de la oferta de productos por parte de los proveedores?	X			Los proveedores renuevan ofertas de paquetes una vez al año.
7	¿Cuenta con un plan de capacitación para el personal sobre los sistemas de información y aplicaciones?		X		
8	documentos tales como reservas, boletos, tiquetes?		X		
9	¿Existe una correcta capacitación sobre atención al cliente?		X		
10	¿Se conoce el procedimiento para pagos con tarjetas de crédito?	X			Es necesario que el asesor sepa y aplique el procedimiento, ya que los fines de semana no se encuentra finanzas laborando.
11	¿Los asesores conocen el procedimiento para el otorgamiento de crédito.?	X			
12	¿Existen políticas de crédito para determinadas empresas?	X			Si, porque la cartera de clientes esta compuesta también por otras agencias minoristas, y grupos empresariales.
13	¿Se han definidos periodos de tiempo anticipado para realizar las reservas de los servicios?		X		Existen pero no se respetan, en el sentido que si el cliente urge del servicio y existe disponibilidad puede reservar, si no se pierde la venta.
14	¿Se conoce el procedimiento para facturación y manejo de facturas?	X			No se encuentra escrito
15	¿Existen procedimientos para las reservas de servicios?		X		
16	¿Se solicitan anticipos a los clientes para garantizar las reservas?	X			
17	¿Existe un procedimiento para el manejo de los anticipos y es conocido en el área?	X			
18	¿Se brinda asesoría sobre los requerimientos migratorios a los pasajeros con respecto al destino que visitan?	X			El asesor explica las tarifas, impuestos y tasas, entre otros requerimientos migratorios.
19	¿Se establece comunicación por escrito de las condiciones de viaje entre los proveedores y la agencia?	X			Con Reconfirmación de servicios
20	¿Se tiene establecidos procedimientos automatizados para la emisión de boletos aéreos?	X			Por el gestor de reservas Amadeus y Sabre
21	¿Existe procedimientos de quejas y sugerencias?		X		
22	¿Se posee un manual de ventas por internet y la capacidad adecuada?		X		
23	¿Se conocen los procedimientos IATA?	X			En lo que respecta a la emisión de los boletos
24	¿Existe duplicidad de funciones en la agencia?	X			Un asesor puede apoyar a otro para agilizar servicios.

Cuestionario C-3 Ventas (Reservas)

CLIENTE: Agencia Perico, S.A. de C.V.
TIPO DE TRABAJO: Diseño de un sistema de control interno informático basado en riesgos.
AREA A EXAMINAR: Conocimiento de las operaciones y procedimientos del área.

CUESTIONARIO PARA DEPARTAMENTOS VENTAS (RESERVAS)

25	¿Se firman algún documento de exoneración de responsabilidad migratoria.?		X		No es responsabilidad de la agencia.
26	¿La información requerida por el cliente se entrega oportunamente?		X		Se han dado casos que por redes sociales piden las reservas y no les envían la información.
27	¿La red de ventas está suficientemente motivada?	X			Reciben comisiones sobre las ventas.
28	¿Existe una revisión de la documentación por otra persona diferente al gestor que realizo el servicio?		X		
29	¿Reconfirmaciones previas a la salida del cliente?	X			No se encuentran documentadas.
30	¿Confirmación de servicio a la llegada del cliente?		X		
31	¿Hacen consultas con el cliente a su regreso, para conocer la calidad del servicio que prestó el proveedor?		X		
32	¿Existe procedimiento para cuando el proveedor ha hecho un cambio en la prestación del servicio?	X			No se encuentran escritos. El agente resuelve según experiencia.
33	¿Existe un manual para la organización y venta de tours privados?		X		
34	¿Se posee una planificación previa para los tours en privado?	X			
35	¿Existe procedimiento para la organización y venta?		X		
36	¿Existe el personal adecuado para la venta de este servicio?	X			
37	¿Las cotizaciones están acorde a las emitidas por los proveedores?	X			Son tarifas especiales
38	¿Existe supervisión por el área contable en lo referente a la cotización?		X		
39	¿Existen procedimientos de cobros?		X		No pasa a créditos y cobros, el asesor gestiona los depósitos.
40	¿Existen procedimientos de publicidad y promoción?	X			
41	¿Existe colaboración en equipo?	X			
42	¿Existen procedimientos establecidos para la elección de los clientes?		X		
43	¿Existe una base de datos de los clientes de tours anteriores?	X			
44	¿Existen procedimientos para corroborar el precio a cobrar a los clientes?		X		No se verifica la veracidad de la tarifa
45	¿Existe tiempo limite para la entrega de la organización y para la venta?	X			
46	¿Existe un convenio firmado por los proveedores para la venta de tours en privado?	X			Firman acuerdos de servicios
47	¿Se realizan listado de los posibles clientes ?		X		
48	¿Se realizan listado de los clientes confirmados?	X			

Cuestionario C-4 Mercadeo

CLIENTE: Agencia Perico, S.A. de C.V.
TIPO DE TRABAJO: Diseño de un sistema de control interno informático basado en riesgos.
AREA A EXAMINAR: Conocimiento de las operaciones y procedimientos del área.

CUESTIONARIO PARA DEPARTAMENTO DE MERCADEO Y PUBLICIDAD

No	PREGUNTAS	RESPUESTA			
		SI	NO	NO APLICA	COMENTARIOS
1	¿Existe una planificación anual para el manejo de la publicidad?	X			
2	¿Se realizan estudio de costo beneficio para el contrato de publicidad?	X			
3	¿Se realizan canjes para cubrir costos de publicidad?	X			Alquileres de espacios se compensan con servicios (boletos, reservas de hotel, entre otros)
4	¿Existe un departamento de publicidad?	X			Diseña los afiches y administra las redes sociales y pagina web.
5	¿Se actualiza la publicidad diariamente?	X			
6	¿Se revisan las ofertas recibidas por los proveedores?	X			Pasa por la encargada de desarrollo de productos
7	¿Se utilizan las redes sociales para la publicidad?	X			
8	¿Se realizan convenios con otros coorganizadores para realizar eventos?	X			Con proveedores
9	¿Existe control para los premios otorgados en esos eventos?	X			Se facturan como atenciones a clientes y se calcula su respectivo impuesto.
10	¿Se cuenta con suficiente capacitación para el personal que participa en esos eventos?	X			
11	¿Existe un cronograma de eventos en los que participa la compañía?	X			
12	¿Se han preestablecido contratos para la publicidad de esos eventos?	X			
13	¿Se maneja publicidad con mas de un medio de comunicación?	X			
14	¿Existen reglamentos para la contratación de espacios publicitarios?		X		
15	¿Se elaboran de forma periódica estudios de mercado?	X			Una vez al año.
16	¿Para introducirse en los mercados en que opera la empresa se precisan fuertes inversiones técnicas, comerciales o humanas?		X		
17	¿Los productos o servicios que ofrece la empresa presentan una ventaja diferencial conocida por la clientela?	X			
18	¿Se dispone de un plan de marketing (precio, plaza, producto, publicidad) coherente?	X			
19	¿Se analiza continuamente la evolución de los principales competidores?		X		
20	¿Existen políticas de protección y control de la información que es expuesta al público?		X		

3.2.4 **Evaluación de riesgos.**

Se procede a realizar la evaluación con el único objetivo de establecer respuestas a los riesgos que se identifican. Para ello se establecieron diferentes riesgos por cada área, de acuerdo a los siguientes catalizadores de COBIT: la información; los servicios, infraestructura y aplicaciones y; el personal, habilidades y competencias.

Riesgo Total	1	2	3	4	6	8	9	12	14	16

Cuadro D-1-1 análisis de riesgo datos e Información. (Criminalidad y motivación política).

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]											
Datos e Información	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Actos originados por la criminalidad común y motivación política											
	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material, imagen,		Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Violación a derechos de autor
					2	2	1	3	3	2	4	3	4	3	3	3	4
Documentos institucionales (proyectos, presupuesto anual, evaluaciones de rendimiento, informes contables, documentación legal)	x	x	x	4	8	8	4	12	12	8	16	12	16	12	12	12	16
Finanzas	x	x	x	4	8	8	4	12	12	8	16	12	16	12	12	12	16
Servicios bancarios	x			2	4	4	2	6	6	4	8	6	8	6	6	6	8
Documentación contable	x	x	x	4	8	8	4	12	12	8	16	12	16	12	12	12	16
Directorio de Contactos (Ejecutivos de líneas aéreas, gerentes de otras agencias de viajes, ejecutivos de cuentas bancarias, proveedores de seguros, entre otros)	x			2	4	4	2	6	6	4	8	6	8	6	6	6	8
Tarifario (Folletos, Fotos, entre otros)	x			3	6	6	3	9	9	6	12	9	12	9	9	9	12
Bases de datos clientes	x	x	x	4	8	8	4	12	12	8	16	12	16	12	12	12	16
Bases de datos proveedores	x	x		2	4	4	2	6	6	4	8	6	8	6	6	6	8
Bases de datos colaborativos	x	x		2	4	4	2	6	6	4	8	6	8	6	6	6	8
Página Web interna (Intranet)	x			3	6	6	3	9	9	6	12	9	12	9	9	9	12
Página Web externa			x	2	4	4	2	6	6	4	8	6	8	6	6	6	8
Respaldos	x		x	3	6	6	3	9	9	6	12	9	12	9	9	9	12
Infraestructura (Planos, Documentación legal)	x			3	6	6	3	9	9	6	12	9	12	9	9	9	12
Informática (Planos de redes, Documentación legal)	x	x		2	4	4	2	6	6	4	8	6	8	6	6	6	8
Base de datos de Contraseñas	x	x	x	3	6	6	3	9	9	6	12	9	12	9	9	9	12
Navegación en Internet	x			2	4	4	2	6	6	4	8	6	8	6	6	6	8
Chat interno	x			1	2	2	1	3	3	2	4	3	4	3	3	3	4
Chat externo	x		x	3	6	6	3	9	9	6	12	9	12	9	9	9	12
Llamadas telefónicas internas	x			1	2	2	1	3	3	2	4	3	4	3	3	3	4
Llamadas telefónicas externas	x		x	3	6	6	3	9	9	6	12	9	12	9	9	9	12

Cuadro D-1-2 análisis de riesgo datos e información (origen físico).

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta								
Datos e Información	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Sucesos de origen físico								
	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material, imagen,		Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
					2	1	2	1	1	1	2	3	2
Documentos institucionales (proyectos, presupuesto anual, evaluaciones de rendimiento, informes contables, documentación legal)	x	x	x	4	8	4	8	4	4	4	8	12	8
Finanzas	x	x	x	4	8	4	8	4	4	4	8	12	8
Servicios bancarios	x			2	4	2	4	2	2	2	4	6	4
Documentación contable	x	x	x	4	8	4	8	4	4	4	8	12	8
Directorio de Contactos (Ejecutivos de líneas aéreas, gerentes de otras agencias de viajes, ejecutivos de cuentas bancarias, proveedores de seguros, entre otros)	x			2	4	2	4	2	2	2	4	6	4
Tarifario (Folletos, Fotos, entre otros)	x			3	6	3	6	3	3	3	6	9	6
Bases de datos clientes	x	x	x	4	8	4	8	4	4	4	8	12	8
Bases de datos proveedores	x	x		2	4	2	4	2	2	2	4	6	4
Bases de datos colaborativos	x	x		2	4	2	4	2	2	2	4	6	4
Página Web interna (Intranet)	x			3	6	3	6	3	3	3	6	9	6
Página Web externa			x	2	4	2	4	2	2	2	4	6	4
Respaldos	x		x	3	6	3	6	3	3	3	6	9	6
Infraestructura (Planos, Documentación legal)	x			3	6	3	6	3	3	3	6	9	6
Informática (Planos de redes, Documentación legal)	x	x		2	4	2	4	2	2	2	4	6	4
Base de datos de Contraseñas	x	x	x	3	6	3	6	3	3	3	6	9	6
Navegación en Internet	x			2	4	2	4	2	2	2	4	6	4
Chat interno	x			1	2	1	2	1	1	1	2	3	2
Chat externo	x		x	3	6	3	6	3	3	3	6	9	6
Llamadas telefónicas internas	x			1	2	1	2	1	1	1	2	3	2
Llamadas telefónicas externas	x		x	3	6	3	6	3	3	3	6	9	6

Cuadro D-1-3 Análisis de riesgos datos e información (decisiones institucionales).

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]											
	Clasificación				Sucesos derivados de la impericia, negligencia de usuarios y decisiones institucionales											
Datos e Información	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material, imagen,	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software "pirateado"	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas,	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, entre
					2	3	4	1	4	3	2	3	2	3	3	3	2
Documentos institucionales (proyectos, presupuesto anual, evaluaciones de rendimiento, informes contables, documentación legal)	x	x	x	4	8	12	16	4	16	12	8	12	8	12	12	12	8
Finanzas	x	x	x	4	8	12	16	4	16	12	8	12	8	12	12	12	8
Servicios bancarios	x			2	4	6	8	2	8	6	4	6	4	6	6	6	4
Documentación contable	x	x	x	4	8	12	16	4	16	12	8	12	8	12	12	12	8
Directorio de Contactos (Ejecutivos de líneas aéreas, gerentes de otras agencias de viajes, ejecutivos de cuentas bancarias, proveedores de seguros, entre otros)	x			2	4	6	8	2	8	6	4	6	4	6	6	6	4
Tarifario (Folletos, Fotos, entre otros)	x			3	6	9	12	3	12	9	6	9	6	9	9	9	6
Bases de datos clientes	x	x	x	4	8	12	16	4	16	12	8	12	8	12	12	12	8
Bases de datos proveedores	x	x		2	4	6	8	2	8	6	4	6	4	6	6	6	4
Bases de datos colaborativos	x	x		2	4	6	8	2	8	6	4	6	4	6	6	6	4
Página Web interna (Intranet)	x			3	6	9	12	3	12	9	6	9	6	9	9	9	6
Página Web externa			x	2	4	6	8	2	8	6	4	6	4	6	6	6	4
Respaldos	x		x	3	6	9	12	3	12	9	6	9	6	9	9	9	6
Infraestructura (Planos, Documentación legal)	x			3	6	9	12	3	12	9	6	9	6	9	9	9	6
Informática (Planos de redes, Documentación legal)	x	x		2	4	6	8	2	8	6	4	6	4	6	6	6	4
Base de datos de Contraseñas	x	x	x	3	6	9	12	3	12	9	6	9	6	9	9	9	6
Navegación en Internet	x			2	4	6	8	2	8	6	4	6	4	6	6	6	4
Chat interno	x			1	2	3	4	1	4	3	2	3	2	3	3	3	2
Chat externo	x		x	3	6	9	12	3	12	9	6	9	6	9	9	9	6
Llamadas telefónicas internas	x			1	2	3	4	1	4	3	2	3	2	3	3	3	2
Llamadas telefónicas externas	x		x	3	6	9	12	3	12	9	6	9	6	9	9	9	6

Cuadro D-1-3 Análisis de riesgos datos e información (decisiones institucionales).

Matriz de Análisis de Riesgo																		
Datos e Información	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Sucesos derivados de la impericia, negligencia de usuarios y decisiones institucionales													
	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material, imagen,		Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los	Falta de mecanismos de verificación de normas y reglas / Análisis	Ausencia de documentación
					3	3	2	4	2	2	2	2	3	3	4	3	2	
Documentos institucionales (proyectos, presupuesto anual, evaluaciones de rendimiento, informes contables, documentación legal)	x	x	x	4	12	12	8	16	8	8	8	8	12	12	16	12	8	
Finanzas	x	x	x	4	12	12	8	16	8	8	8	8	12	12	16	12	8	
Servicios bancarios	x			2	6	6	4	8	4	4	4	4	6	6	8	6	4	
Documentación contable	x	x	x	4	12	12	8	16	8	8	8	8	12	12	16	12	8	
Directorio de Contactos (Ejecutivos de líneas aéreas, gerentes de otras agencias de viajes, ejecutivos de cuentas bancarias, proveedores de seguros, entre otros)	x			2	6	6	4	8	4	4	4	4	6	6	8	6	4	
Tarifario (Folletos, Fotos, entre otros)	x			3	9	9	6	12	6	6	6	6	9	9	12	9	6	
Bases de datos clientes	x	x	x	4	12	12	8	16	8	8	8	8	12	12	16	12	8	
Bases de datos proveedores	x	x		2	6	6	4	8	4	4	4	4	6	6	8	6	4	
Bases de datos colaborativos	x	x		2	6	6	4	8	4	4	4	4	6	6	8	6	4	
Página Web interna (Intranet)	x			3	9	9	6	12	6	6	6	6	9	9	12	9	6	
Página Web externa			x	2	6	6	4	8	4	4	4	4	6	6	8	6	4	
Respaldos	x		x	3	9	9	6	12	6	6	6	6	9	9	12	9	6	
Infraestructura (Planos, Documentación legal)	x			3	9	9	6	12	6	6	6	6	9	9	12	9	6	
Informática (Planos de redes, Documentación legal)	x	x		2	6	6	4	8	4	4	4	4	6	6	8	6	4	
Base de datos de Contraseñas	x	x	x	3	9	9	6	12	6	6	6	6	9	9	12	9	6	
Navegación en Internet	x			2	6	6	4	8	4	4	4	4	6	6	8	6	4	
Chat interno	x			1	3	3	2	4	2	2	2	2	3	3	4	3	2	
Chat externo	x		x	3	9	9	6	12	6	6	6	6	9	9	12	9	6	
Llamadas telefónicas internas	x			1	3	3	2	4	2	2	2	2	3	3	4	3	2	
Llamadas telefónicas externas	x		x	3	9	9	6	12	6	6	6	6	9	9	12	9	6	

Cuadro D-2-1 análisis de riesgos sistemas (criminalidad común).

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]											
Sistemas e Infraestructura	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Actos originados por la criminalidad común y motivación política											
	Acceso exclusivo	Acceso ilimitado	Costo de recuperación (tiempo, económico, material, imagen,		Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Violación a derechos de autor
					2	2	1	3	3	2	4	3	4	3	3	3	4
Equipos de la red cableada (router, switch)	x	x		4	8	8	4	12	12	8	16	12	16	12	12	12	16
Equipos de la red inalámbrica (router, punto de acceso)	x	x		4	8	8	4	12	12	8	16	12	16	12	12	12	16
Cortafuego	x		x	4	8	8	4	12	12	8	16	12	16	12	12	12	16
Servidores	x		x	4	8	8	4	12	12	8	16	12	16	12	12	12	16
Computadoras	x		x	3	6	6	3	9	9	6	12	9	12	9	9	9	12
Portátiles	x		x	3	6	6	3	9	9	6	12	9	12	9	9	9	12
Programas de administración (contabilidad, manejo de personal)	x		x	4	8	8	4	12	12	8	16	12	16	12	12	12	16
Programas de producción de datos (ERP y GDS)	x		x	4	8	8	4	12	12	8	16	12	16	12	12	12	16
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, redes sociales)	x	x	x	3	6	6	3	9	9	6	12	9	12	9	9	9	12
Impresoras	x	x	x	2	4	4	2	6	6	4	8	6	8	6	6	6	8
Memorias portátiles	x	x		1	2	2	1	3	3	2	4	3	4	3	3	3	4
PBX (Sistema de telefonía convencional)	x	x	x	2	4	4	2	6	6	4	8	6	8	6	6	6	8
Celulares	x		x	2	4	4	2	6	6	4	8	6	8	6	6	6	8
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, entre otros)	x		x	2	4	4	2	6	6	4	8	6	8	6	6	6	8

Cuadro D-2-2 análisis de riesgos sistemas (origen físico).

Matriz de Análisis de Riesgo	Clasificación				Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta								
					Sucesos de origen físico								
Sistemas e Infraestructura	Acceso exclusivo	Acceso ilimitado	Costo de recuperación (tiempo, económico, material, imagen,	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
					2	1	2	1	1	1	2	3	2
Equipos de la red cableada (router, switch)	x	x		4	8	4	8	4	4	4	8	12	8
Equipos de la red inalámbrica (router, punto de acceso)	x	x		4	8	4	8	4	4	4	8	12	8
Cortafuego	x		x	4	8	4	8	4	4	4	8	12	8
Servidores	x		x	4	8	4	8	4	4	4	8	12	8
Computadoras	x		x	3	6	3	6	3	3	3	6	9	6
Portátiles	x		x	3	6	3	6	3	3	3	6	9	6
Programas de administración (contabilidad, manejo de personal)	x		x	4	8	4	8	4	4	4	8	12	8
Programas de producción de datos (ERP y GDS)	x		x	4	8	4	8	4	4	4	8	12	8
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, redes sociales)	x	x	x	3	6	3	6	3	3	3	6	9	6
Impresoras	x	x	x	2	4	2	4	2	2	2	4	6	4
Memorias portátiles	x	x		1	2	1	2	1	1	1	2	3	2
PBX (Sistema de telefonía convencional)	x	x	x	2	4	2	4	2	2	2	4	6	4
Celulares	x		x	2	4	2	4	2	2	2	4	6	4
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, entre otros)	x		x	2	4	2	4	2	2	2	4	6	4

Cuadro D-2-3 análisis de riesgos sistemas. (Decisiones institucionales).

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]												
	Clasificación				Sucesos derivados de la impericia, negligencia de usuarios y decisiones institucionales												
Sistemas e Infraestructura	Acceso exclusivo	Acceso ilimitado	Costo de recuperación (tiempo, económico, material, imagen,	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software "pirateado"	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento,
					2	3	4	1	4	3	2	3	2	3	3	3	2
Equipos de la red cableada (router, switch)	x	x		4	8	12	16	4	16	12	8	12	8	12	12	12	8
Equipos de la red inalámbrica (router, punto de acceso)	x	x		4	8	12	16	4	16	12	8	12	8	12	12	12	8
Cortafuego	x		x	4	8	12	16	4	16	12	8	12	8	12	12	12	8
Servidores	x		x	4	8	12	16	4	16	12	8	12	8	12	12	12	8
Computadoras	x		x	3	6	9	12	3	12	9	6	9	6	9	9	9	6
Portátiles	x		x	3	6	9	12	3	12	9	6	9	6	9	9	9	6
Programas de administración (contabilidad, manejo de personal)	x		x	4	8	12	16	4	16	12	8	12	8	12	12	12	8
Programas de producción de datos (ERP y GDS)	x		x	4	8	12	16	4	16	12	8	12	8	12	12	12	8
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, redes sociales)	x	x	x	3	6	9	12	3	12	9	6	9	6	9	9	9	6
Impresoras	x	x	x	2	4	6	8	2	8	6	4	6	4	6	6	6	4
Memorias portátiles	x	x		1	2	3	4	1	4	3	2	3	2	3	3	3	2
PBX (Sistema de telefonía convencional)	x	x	x	2	4	6	8	2	8	6	4	6	4	6	6	6	4
Celulares	x		x	2	4	6	8	2	8	6	4	6	4	6	6	6	4
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, entre otros)	x		x	2	4	6	8	2	8	6	4	6	4	6	6	6	4

Cuadro D-2-3 análisis de riesgos sistemas. (Decisiones institucionales).

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]												
Sistemas e Infraestructura	Clasificación				Sucesos derivados de la impericia, negligencia de usuarios y decisiones institucionales												
	Acceso exclusivo	Acceso ilimitado	Costo de recuperación (tiempo, económico, material, imagen,	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de	Falta de mecanismos de verificación de normas y reglas /	Ausencia de documentación
					3	3	2	4	2	2	2	2	3	3	4	3	2
Equipos de la red cableada (router, switch)	x	x		4	12	12	8	16	8	8	8	8	12	12	16	12	8
Equipos de la red inalámbrica (router, punto de acceso)	x	x		4	12	12	8	16	8	8	8	8	12	12	16	12	8
Cortafuego	x		x	4	12	12	8	16	8	8	8	8	12	12	16	12	8
Servidores	x		x	4	12	12	8	16	8	8	8	8	12	12	16	12	8
Computadoras	x		x	3	9	9	6	12	6	6	6	6	9	9	12	9	6
Portátiles	x		x	3	9	9	6	12	6	6	6	6	9	9	12	9	6
Programas de administración (contabilidad, manejo de personal)	x		x	4	12	12	8	16	8	8	8	8	12	12	16	12	8
Programas de producción de datos (ERP y GDS)	x		x	4	12	12	8	16	8	8	8	8	12	12	16	12	8
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, redes sociales)	x	x	x	3	9	9	6	12	6	6	6	6	9	9	12	9	6
Impresoras	x	x	x	2	6	6	4	8	4	4	4	4	6	6	8	6	4
Memorias portátiles	x	x		1	3	3	2	4	2	2	2	2	3	3	4	3	2
PBX (Sistema de telefonía convencional)	x	x	x	2	6	6	4	8	4	4	4	4	6	6	8	6	4
Celulares	x		x	2	6	6	4	8	4	4	4	4	6	6	8	6	4
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, entre otros)	x		x	2	6	6	4	8	4	4	4	4	6	6	8	6	4

Cuadro D-3-1 análisis de riesgo personal (criminalidad común).

Matriz de Análisis de Riesgo	Clasificación				Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]												
					Actos originados por la criminalidad común y motivación política												
Personal	Imagen pública de alto perfil, indispensable para funcionamiento	Perfil medio, experto en su área	Perfil bajo, no indispensable para funcionamiento institucional	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Violación a derechos de autor
					2	2	1	3	3	2	4	3	4	3	3	3	4
Junta Directiva	x			4	8	8	4	12	12	8	16	12	16	12	12	12	16
Gerencia General	x			3	6	6	3	9	9	6	12	9	12	9	9	9	12
Administración		x		3	6	6	3	9	9	6	12	9	12	9	9	9	12
Personal técnico (asesor de ventas)		x		4	8	8	4	12	12	8	16	12	16	12	12	12	16
Recepción			x	2	4	4	2	6	6	4	8	6	8	6	6	6	8
Informática / Soporte técnico interno		x		3	6	6	3	9	9	6	12	9	12	9	9	9	12
Soporte técnico externo		x		3	6	6	3	9	9	6	12	9	12	9	9	9	12
Servicio de limpieza externo			x	2	4	4	2	6	6	4	8	6	8	6	6	6	8
Servicio de mensajería externo		x		3	6	6	3	9	9	6	12	9	12	9	9	9	12

Cuadro D-3-2 análisis de riesgos personal (sucesos origen físico).

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta								
	Clasificación				Sucesos de origen físico								
Personal	Imagen pública de alto perfil, indispensable para funcionamiento	Perfil medio, experto en su área	Perfil bajo, no indispensable para funcionamiento institucional	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
					2	1	2	1	1	1	2	3	2
Junta Directiva	x			4	8	4	8	4	4	4	8	12	8
Gerencia General	x			3	6	3	6	3	3	3	6	9	6
Administración		x		3	6	3	6	3	3	3	6	9	6
Personal técnico (asesor de ventas)		x		4	8	4	8	4	4	4	8	12	8
Recepción			x	2	4	2	4	2	2	2	4	6	4
Informática / Soporte técnico interno		x		3	6	3	6	3	3	3	6	9	6
Soporte técnico externo		x		3	6	3	6	3	3	3	6	9	6
Servicio de limpieza externo			x	2	4	2	4	2	2	2	4	6	4
Servicio de mensajería externo		x		3	6	3	6	3	3	3	6	9	6

Cuadro D-3-3 análisis de riesgos personal (decisiones institucionales).

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]												
Personal	Clasificación				Sucesos derivados de la impericia, negligencia de usuarios y decisiones institucionales												
	Imagen pública de alto perfil, indispensable para funcionamiento	Perfil medio, experto en su área	Perfil bajo, no indispensable para funcionamiento institucional	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software "pirateado"	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento,
					2	3	4	1	4	3	2	3	2	3	3	3	2
Junta Directiva	x			4	8	12	16	4	16	12	8	12	8	12	12	12	8
Gerencia General	x			3	6	9	12	3	12	9	6	9	6	9	9	9	6
Administración		x		3	6	9	12	3	12	9	6	9	6	9	9	9	6
Personal técnico (asesor de ventas)		x		4	8	12	16	4	16	12	8	12	8	12	12	12	8
Recepción			x	2	4	6	8	2	8	6	4	6	4	6	6	6	4
Informática / Soporte técnico interno		x		3	6	9	12	3	12	9	6	9	6	9	9	9	6
Soporte técnico externo		x		3	6	9	12	3	12	9	6	9	6	9	9	9	6
Servicio de limpieza externo			x	2	4	6	8	2	8	6	4	6	4	6	6	6	4
Servicio de mensajería externo		x		3	6	9	12	3	12	9	6	9	6	9	9	9	6

Cuadro D-3-3 análisis de riesgos personal (decisiones institucionales).

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]												
Personal	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Sucesos derivados de la impericia, negligencia de usuarios y decisiones institucionales												
	Imagen pública de alto perfil, indispensable para funcionamiento	Perfil medio, experto en su área	Perfil bajo, no indispensable para funcionamiento institucional		Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de	Falta de mecanismos de verificación de normas y reglas /	Ausencia de documentación
					3	3	2	4	2	2	2	2	3	3	4	3	2
Junta Directiva	x			4	12	12	8	16	8	8	8	8	12	12	16	12	8
Gerencia General	x			3	9	9	6	12	6	6	6	6	9	9	12	9	6
Administración		x		3	9	9	6	12	6	6	6	6	9	9	12	9	6
Personal técnico (asesor de ventas)		x		4	12	12	8	16	8	8	8	8	12	12	16	12	8
Recepción			x	2	6	6	4	8	4	4	4	4	6	6	8	6	4
Informática / Soporte técnico interno		x		3	9	9	6	12	6	6	6	6	9	9	12	9	6
Soporte técnico externo		x		3	9	9	6	12	6	6	6	6	9	9	12	9	6
Servicio de limpieza externo			x	2	6	6	4	8	4	4	4	4	6	6	8	6	4
Servicio de mensajería externo		x		3	9	9	6	12	6	6	6	6	9	9	12	9	6

En cuanto a la matriz que analiza el riesgo al que se expone los datos y la información, se refleja que dicho recurso se encuentra muy vulnerable a riesgos de criminalidad y motivación política, tales como el sabotaje, el fraude, robo, hurto e intrusiones a la red interna donde se transmiten los datos; los equipos en donde se trabajan están expuestos a fallas en el suministro eléctrico y esto supone a la exposición de riesgos institucionales por dependencia del servicio técnico para la resolución de problemas que surgen del sistema, ausencia de actualizaciones importantes y normas y reglas claras para el manejo de los datos. Con respecto a los riesgos del sistema e infraestructura, se detecta fuerte riesgo de pérdida por vandalismos, fraude, robo y hurto, fallas en el suministro eléctrico, mal manejo de los sistemas y herramientas, robo de contraseñas, infección de virus, perfiles no definidos con sus respectivos roles

Por último, el personal que tiene acceso a la información, está expuesta a riesgos tales como daños por vandalismo, fraude, robo y hurto de información electrónica y por consiguiente, perdida de datos. Se concluye, que los controles implementados no formalmente por la administración no optimizan adecuadamente los riesgos detectados en el sistema de información, por lo que requiere el establecimiento de controles internos informáticos más específicos.

3.2.5 **Establecer los controles.**

Procede a la elaboración de los controles los cuales se dividen en generales y de aplicación, con sus respectivas sub divisiones.

Se detallan a continuación:

Controles generales.

a. Plan de organización general.

1) Asegurar que exista una separación de deberes adecuada entre los usuarios operadores, los programadores de aplicación, los programadores del sistema y los analistas de sistemas. Si alguien ingresa al área del servidor central, además de los usuarios operadores, asegurar que se posee controles externos apropiados para que los usuarios estén informados ante la situación especial.
2) Al implementarse nuevos controles es necesario programar reuniones donde se discutan y aclaren dudas, determinar planes de inducción. También se pueden tocar los controles ya existentes y discutir sus mejoras. Las reuniones deben ser periódicas e incluir a todas las áreas de trabajo.
3) Cuando se corra un programa crítico o delicado, usar dos o más usuarios operadores durante la impresión del trabajo.
4) Si es factible, realizar rotación periódica de los operadores de la computadora entre diferentes funciones del trabajo.
5) Organizar de forma independiente a la función de proceso de datos de otros departamentos, especialmente separada de las operaciones financieras.
6) Asegurarse de la existencia de un plan para las operaciones de procesos de datos en caso de desastre total.
7) Asegurar que exista una autorización formal del sistema para los cambios o modificaciones del mismo.
8) Establecer políticas y realizar educación y entrenamiento continuo al usuario, en áreas de seguridad y eficiencia del trabajo.
9) Insistir en que todo el personal tome como un mínimo de cinco días consecutivos de vacaciones, a razón que alguien más pueda ejecutar funciones específicas de un puesto determinado.

10) Asegurar que exista un manual de descripción de puestos de trabajo.
11) Asegurar que haya un reporte de utilización de máquina para identificar el trabajo que está corriendo el operador.
12) Asegurar que la gerencia del departamento revise los reportes de control y resuelva las excepciones que ocurran.
13) Cerciorar que se posea un seguro adecuado que cubra la pérdida del equipo de computación, medios de proceso de datos y posiblemente las interrupciones por negocio y costo extra, que haya política de errores y omisiones.
14) Realizar análisis de riesgos periódicamente para identificar programas críticos (debido a su alta exposición al fraude) y controlar fuertemente estos programas. Transmitir contantemente a los usuarios las consecuencias negativas del no mitigar los riesgos con los controles ya establecidos.
15) Formar un grupo de control operacional que relacione a los usuarios y las operaciones de la computadora con el fin de controlar las entradas, salidas y resolver las excepciones.
16) Procurar que un grupo de prueba de sistemas que examine adecuadamente todas las modificaciones a los sistemas, así como los nuevos que se estén desarrollando.
17) Desarrollar una política que permita el cese inmediato de empleados no adecuados. La cual considere multas por degradación de imagen de la organización. O procedimientos legales para demandar en caso de ser grave el problema.
18) Asegurar que haya una apropiada separación de deberes dentro del área de usuario que este siendo auditada.
19) Revisar los organigramas para asegurar que la organización es funcional y que puede operar exitosamente dentro de los confines de la organización.
20) Interrelacionar los organigramas totales con los organigramas departamentales para asegurar que exista una relación adecuada de trabajo.
21) Revisar las políticas generales dadas por la gerencia con respecto a las operaciones de proceso de datos.
22) Revisar los procedimientos del departamento de proceso de datos para verificar si llevan a cabo adecuadamente las políticas básicas tal como fueron esbozadas por el gobierno corporativo.
23) Revisar el manual de descripción de puestos dentro del departamento de proceso de datos con el fin de asegurar que existe una separación de las funciones laborales.

24) Procurar procedimientos escritos para horarios de trabajo dentro de las operaciones de proceso de datos.

25) Procurar un área separada de almacenamiento de respaldos, con respecto al departamento de proceso de datos.

26) Asegurarse que exista un procedimiento especial para reportar dificultades y problemas de documentación

27) Proporcionar un estándar con respecto al cual se desarrolle el ciclo de vida del sistema PED.

28) Procurar un estándar separado con respecto a la administración de la base de datos.

29) Asegurarse que existe la documentación adecuada para todos los sistemas y programas.

30) Garantizar que cualquier información concerniente a individuos o relaciones públicas quede a disposición de las fuentes públicas solamente a través del personal específicamente designado o departamentos específicos.

31) Asegurar que cualquier información que se pueda identificar directamente con un individuo se libere solamente bajo la autorización escrita de tal individuo.

32) Asegurar que todos los reportes importante generados por la computadora lleven un encabezado tal que establezca claramente que el reporte es privado y es propiedad confidencial, también que lleve establecido como se debe disponer de los reportes cuando no se necesiten más.

33) Asegurar que exista una política específica respecto a quien dentro de la organización tiene el derecho al acceso a la información específica. Esta debe definir cualesquiera limitaciones en el uso de esta información por los que tenga acceso autorizado a ella.

34) Establecer un política específica para los registros de la organización , que defina quien mantendrá los registros , el medio ambiente en el cual deban mantenerse, y que procuren un tiempo límite claro y un plan de disposición en el caso de registros antiguos.

35) Clasificar las políticas acerca de quién tiene las bases de datos y la información contenida en ellos así como quien tiene la autoridad para originar, modificar o borrar datos existentes dentro de las bases de datos específicos.

36) Proporcionar un programa de entrenamiento a lo amplio de la organización para la seguridad y privacidad. Este programa toma un área específica y también puede incluir un semanario sobre la seguridad y privacidad.

37) Asegurar que haya un comité de auditoría formado por los directores externos de la empresa, que interactúen con la función de auditoría.

b. Controles propios del equipo.

38) Mantener un inventario actualizado del hardware de la organización.

39) Verificar la edad de los equipos y programar cambios en las unidades desfasadas u obsoletas.

40) Capacitar a los usuarios para el uso de nuevos equipos.

41) Contrato de seguros para salvaguardar el equipo.

42) Verificar que las cláusulas de los seguros contratados cubran los equipos.

43) El desplazamiento de los equipos solo puede ser ejecutado por personal técnico cualificado.

44) Programar jornadas de mantenimiento periódico al equipo.

45) El personal de mantenimiento tenga los conocimientos y la pericia necesaria para solventar la demanda inmediata.

46) Establecer un procedimiento para reportar fallas al personal técnico.

47) Mantener un inventario adecuado de repuestos para reparaciones inmediatas.

48) Establecer procedimientos para adquisiciones de nuevos equipos.

49) Hacer estudios del rendimiento del equipo actual.

50) Realizar capacitaciones constantes al personal sobre el uso del software

51) Establecer atributos de usuarios, jerarquías y contraseñas en el software que se emplean, incluyendo correo electrónico y uso de redes sociales.

52) Realizar mantenimientos al software a través de la instalación de las actualizaciones que dispone el fabricante.

53) Establecer procedimientos de instalación de software, que regule la instalación de códigos no autorizados.

54) Llevar un inventario de licencias de software, actualizado periódicamente.

55) Realizar pruebas de nuevas versiones de software que proporcione mejoras en estabilidad, rendimiento y seguridad.

c. Controles de acceso.

56) Verifique que son seguras las tablas que autorizan las contraseñas de usuarios o restringen a otro usuarios

57) Revise los controles de usuario respecto a la seguridad física y lógica de la información.

58) Contrólese convenientemente el acceso a la base de datos y los programas de aplicación, utilería y cualquier otro recurso.

59) Designar oficialmente a una persona como la encargada de la oficina de control de la información para toda la organización. Esta persona es responsable de la seguridad de todo el proceso de datos, tanto físicamente como de la información.

60) Hacer que el personal use gafetes o insignias en áreas restringidas. Los visitantes deben usar un gafete de color diferente, deben firmar registro y ser escoltados.

61) No dejar impreso el nombre de la compañía en los gafetes de visita.

d. Seguridad física.

62) Determinar si la construcción del edificio, incluyendo las paredes, techos y pisos, son de materiales no combustibles, con el fin de reducir la posibilidad de incendio.

63) Ver que las paredes adyacentes inmediatas a los archivos o al equipo critico son de ladrillo, de marera que no sean penetradas fácilmente.

64) Observar que las paredes se extiendan desde la estructura del piso a la del techo del edificio y no desde pisos elevados a techos falsos, con el fin de impedir una entrada furtiva.

65) Separar físicamente el servidor central de los otros departamentos.

66) En edificios de varios pisos, situar el servicio de proceso de datos en el piso más alto, para reducir el riesgo de penetración externa o inundaciones. Asegurarse que no haya goteras.

67) Separar el área de servidor central, con respecto al área de almacenamiento de back ups, con paredes sólidas y no de materiales inflamables.

68) No permitir visitas al servidor central.

69) Sellar las paredes y los pisos de cemento con pintura resistente al polvo.

70) Verificar que los techos estén a prueba de agua y que no fluya hacia los pisos.

71) Procurar que el servicio de drenaje adecuado bajo pisos elevados, debido a que los cables de corriente eléctrica pasan debajo de ellos.

72) Verificar que solo haya una entrada y salida que sea usada por el personal de operación del servidor central. Todas las puertas deben de estar provistas de aberturas, para poder romperlas en caso de emergencia.

73) Instalar un sistema automático de supresión de fuego en el área del servidor central, especialmente en el cuarto de respaldos.

74) Instalar detectores de fuego y humo tanto en el área del techo del cuarto de la computadora, así como en el piso falso.

75) Instalar dos tipos de detectores de fuego y humo; detectores de ionización para dar alerta rápida del humo y los de fuego para liberar los mecanismos de supresión de fuego.

76) Tener un interruptor manual en caso de ser falsa alarma, el personal autorizado pueda cortar la liberación automática de los supresores.

77) Colocar estratégicamente extintores cerca del servidor central.

78) Comprobar que las cortinas, tapetes, muebles, piso falso, cielo falso, filtros de aire acondicionado, materiales aislantes eléctricos y acústicos, estén elaborados de materiales no combustibles o con retardantes de fuego.

79) Prohibir el fumar, comer y beber dentro área del servidor central.

80) Instalar apagadores automáticos de incendios en los ductos de aire acondicionado en cuarto de la computadora, para cortar el flujo de aire en caso de incendio.

81) Cerciorarse que el sistema de alarma contra incendios tiene capacidad de transmitir a un punto remoto que sea supervisado las 24 horas.

82) Almacenar el papel y otros suministros combustibles fuera del área del servidor central, a excepción de los que se usaran inmediatamente.

83) Conservar en pequeñas cantidades los materiales inflamables usados en el área del servidor central, tales como los líquidos limpiadores.

84) Brindar el adecuado mantenimiento al sistema contra incendios.

85) Eliminar continuamente las acumulaciones de basura combustible.

86) Capacitar al personal para la lucha contra el fuego y la evacuación ordenada del servicio de proceso de datos en caso se active la alarma contra incendios o de terremoto.

87) Proteger de las variaciones de voltaje a toda la potencia eléctrica que sirve al servidor central, al equipo relacionado y al equipo de comunicación, empleando un transformador.

88) Proteger los circuitos de la computadora contra el vandalismo que se puede originar por abrir los tableros y cortar la energía.

89) Comprobar que el panel de distribución del sistema eléctrico y red de cableado del servidor se encuentra en un área segura inaccesible a personas no autorizadas.

90) Marcar apropiadamente los tableros de circuito de manera que si se les brinda servicio al equipo se encuentre de manera rápida.

91) Instalar luces de emergencia accionadas por baterías al servidor central.

92) Procurar dar mantenimiento preventivo a la planta generadora de energía de emergencia.

93) Brindar mantenimiento preventivo y verificación mensual del sistema de aire acondicionado.

94) Proteger las conexiones eléctricas y las cajas de circuitos que alimentan los aires acondicionados.

95) Considerar el uso de gafetes de identificación, por todo el personal

96) Utilizar alguna clase de trampas en las entradas, video vigilancia, identificación del personal por supervisores volantes, u otros procedimientos positivos de control que restrinjan al personal no autorizado al ingreso de áreas sensibles.

97) No permitir a los programadores y analistas de sistemas entrar al cuarto del servidor central. Tampoco que el personal de operación ingrese al cuarto donde se almacenan los respaldos. Caso contrario se debe contar con autorización.

98) No se indique con signos, planos o directorios el lugar donde está el servidor central.

99) Utilizar un servicio de vigilancia para todo el edificio, y con especial atención las áreas de mayor flujo de información. Al contratar la empresa de vigilancia firmar un contrato de responsabilidad.

100) Establecer estándares, documentos de seguridad, procedimientos y guías de servicio de computadora.

101) Establecer el puesto de administrador de seguridad de la computadora.

102) Desarrollar un plan que cubra las acciones a ser tomadas durante una emergencia temporal tal como atentados por bombas, inundación, incendio pequeño o fallo temporal del sistema de cómputo

103) Comprobar que haya una protección física oportuna contra el fuego, humo, calor, penetración física de personas y otros factores, en lugar donde se almacenan los respaldos.

104) Ratificar que el plan para casos de desastre en PED determine quién debe tomar las decisiones durante la recuperación del desastre, y establezca la disponibilidad y entrenamiento del personal suficientemente experimentado.

105) Certificar que la gerencia refuerce las políticas y procedimientos con respecto a la seguridad física.

106) Ratificar que la gerencia ha considerado a la seguridad como una línea en el presupuesto, preste su asistencia a los esfuerzos de entrenamiento con respecto a la seguridad física.

107) Determinar que los empleados deben firmar un convenio reconociendo el hecho de que no deben vender programas de computadoras o usar la máquina para asuntos particulares, así mismo no compartir contraseñas o permisos.

108) Revisar las coberturas de los seguros, sobre los medios de proceso de datos, el equipo y sobre interrupciones de transacciones comerciales que generen gastos extras a la organización.

e. Seguridad lógica y control de procesamiento de datos.

109) Mantener conteo de verificación de la cantidad de bits de los paquetes de software, para prevenir modificaciones en los programas.

110) Cuando un software sensitivo es utilizado en lugares remotos, considere el hacer una carga especial de software desde el lugar central. Esto daría seguridad de que no han sido hechos cambios ilegales en los programas en lugar remoto.

111) Utilizar software de auditoría generalizado para las diversas funciones de los paquetes de software del sistema.

112) Revisar regularmente las bitácoras de reinicio del sistema y de los conteos de tiempo de reproceso por causa de mal funcionamiento del sistema.

113) Verificar la existencia de una bitácora donde se registren los problemas del software, que posea el diagnóstico del problema y que el usuario, los componentes del software o el dispositivo que lo haya causado se pueda aislar.

114) Determine si están programados claramente y se han definido bien las interfaces entre los paquetes de software y los sistemas operativos, el software de comunicación de datos, los gestores de bases de datos.

115) Hacer que los programadores del software del sistema enumeren todas las irregularidades conocidas en cualquier de los software, definan el grado de riesgo individualmente y que hagan posibles las correcciones.

116) Revisar las salvaguardas con respecto a que el operador de la consola reinicie ilegalmente el reloj interno de la computadora y verificar que no se pueda hacer esto y que se tengan los controles secundarios adecuados para detectar quien y cuando realizo esta acción.

117) Ratificar que se registren las fallas repetidas y que se tome alguna clase de acción positiva, tal como desechar la terminal infractora y contratar personal de seguridad oportuno.

118) Comprobar que los comandos del software del sistema se pueden ejecutar desde una terminar maestra y no de un conjunto de terminales.

119) Verificar que el sistema administrativo de la base de datos da protección contra coincidencias y desacuerdos, registrándolos en una bitácora.

120) Considerar que el software de sistema verifique sus propias tablas internas sensitivas y que revalide periódicamente esta verificación con el fin de prevenirse contra una penetración sofisticada que pueda cambiar una tabla, violar la seguridad y restaurar la tabla en su configuración original.

121) Asegurarse que está guardada seguramente toda la documentación relativa al software del sistema y programas de utilería.

122) Verificar si se ha delegado un responsable en verificar las bitácoras de auditoría.

123) Verificar que haya el apoyo apropiado de mantenimiento y del proveedor para el software.

124) Verificar que los proveedores que hagan cualquier clase de servicio de mantenimiento al software son absolutamente confiables. Así también los de servicio de mensajería externa y limpieza. Controlar sus accesos y sus salidas del área. En caso de ocurrir una falta establecer los términos de negociación según sea el caso.

125) Controlar el uso de los programas de diagnósticos.

126) Verificar que el sistema operativo es lo suficientemente sofisticado como para conservar una pista de la proporción de asignaciones de espacio permitidas a los usos reales de un programa y entonces, eficientemente sin comprometer la seguridad, borrar solamente esa porción de la memoria.

127) Verificar el acceso a los archivos.

128) Verificar el escudriñamiento de la información residual.

129) Verificar el acceso remoto.

130) Verificar las intrusiones de virus tipo caballo de Troya, atacando y protegiendo las computadoras.

131) Verificar la sobrecarga del sistema.

132) Verificar la detección de intrusión y bloquear con cortafuegos.

133) Verificar los recursos compartidos.

134) Verificar la integridad del usuario.

135) Compruebe que el administrador de la base de datos (ABD) es responsable de la instrucción del usuario y personal técnico en los conceptos y procedimientos de trabajo de la base de datos.

136) Verifique que el ABD supervisa el uso de la base de datos.

137) Verifique que el ABD tiene autoridad de realizar modificaciones a la base de datos.

138) No se permita que el ABD tenga acceso no supervisado al área de operación y opere las computadoras.

139) No se permita que el ABD iniciar transacciones sin la aprobación del departamento usuario.

140) Solicite al ABD establezca procedimientos escritos para la recuperación de la base de datos para el caso de una pérdida parcial o total.

141) Haga que el ABD establezca procedimientos escritos acerca de la seguridad de la información.

142) Haga que el ABD documente el contenido de la base de datos, defina entidades y atributos y defina completamente las interrelaciones.

143) Verifique que el ABD tiene el control del contenido, organización, integridad y privacidad de la base de datos.

144) Compruebe que el ABD tiene el control del medio físico de almacenamiento de la base de datos.

145) Ratifique que la base de datos se separa de la usada para programas de prueba.

146) Determine si los programas de utilería escritos especialmente por el proveedor están bajo control del administrador de la base de datos.

147) Contrólese convenientemente el acceso a la base de datos y los programas de aplicación, utilería y cualquier otro recurso.

148) Revisar los dispositivos de entrada y salida situados en la computadora, con el fin de cerciorarse que están controlados apropiadamente.

149) Asegurarse que existen manuales de procedimientos e instrucciones de operación para todos los programas aplicativos que acceden a la base de datos.

150) Provéase un programa especial de software que revise periódicamente la base de datos y busque agujeros en la estructura física o lógica de ella.

151) Procúrese un diccionario de datos para un control simple y efectivo sobre todas las definiciones y para el rastreo de los datos a través del mismo sistema.

152) Establézcase una función humana titulada Administrador de la base de datos (ABD), quien será el responsable de toda la base de datos.

153) Revise los controles de los archivos de la base de datos con respecto a la seguridad.

154) Mantener restringidas por límite de tiempo las llamadas telefónicas al exterior.

155) Establecer un sistema de escucha telefónica para las áreas que manejan información sensible.

Controles de Aplicación.

a. Controles de entrada.

156) Es necesario etiquetar los dispositivos de entrada ya sea USB o discos de almacenamiento, para su identificación. Además deben ser escaneados por antivirus antes de ejecutarlos.

157) Cuando los documentos fuente pasan a través de varios departamentos para su procesamiento manual, llevar un registro en cuanto a la hora recibida y de quien se recibieron.

158) Realizar una verificación manual de los documentos fuente, como las cifras de control, firma de autorización, nombre del solicitante y fecha de solicitud, cuentas contables o códigos utilizados, entre otros.

159) Asegurar que la función responsable de la alimentación de las transacciones verifica las firmas de autorización comparándolas con el registro de firmas autorizadas.

160) Cuando los archivos deban convertirse a otros formatos para su lectura, verificar la correcta conversión para dar fiabilidad en los datos.

161) Utilizar palabras clave para abrir los archivos de información delicada y confidencial.

162) Utilizar restricciones para evitar la modificación de información sensible, como protección de hojas de edición.

163) Segregar la responsabilidad de las funciones de generación de transacciones, registros y la custodia de la misma.

164) Establecer controles de paquetes de documentación con el fin de prevenir la introducción de una entrada no autorizada.

165) Archivar los documentos fuente en un lugar seguro para prevenir modificaciones no autorizadas, o el uso no autorizado de los datos antes de su entrada al sistema. El método de archivo debe procurar un acceso rápido a los mismos.

166) Controlar los documentos confidenciales usando métodos de custodia cajas de seguridad, custodia dual.

167) Registrar los datos de una forma pre impresa o utilizar sellos que den seguridad contra errores u omisiones.

168) Verificar que el personal que ingresa los datos coloca su firma o cualquier señal que lo identifique de alguna forma en los datos que prepara.

169) Utilizar un formato estándar para cada tipo de transacción que se realiza con la posibilidad de numerarlos para evitar la duplicidad, especificando los requisitos mínimos para su verificación y registro.

170) Escanear la documentación que soporta los pagos a proveedores para su consulta.

171) Verificar que los proveedores estén autorizados. Si no lo está debe crearse primero en la base de datos para autorizar el pago, donde debe contener la identificación, dirección y número de contacto.

172) Mantener un ciclo de proceso establecido y publicarlo para permitir a los usuarios el control de las fechas de corte.

173) Centralizar la operación de respaldos para asegurar la información ante la pérdida de los datos fuente.

174) Asignar un tiempo límite para la retención de cada documento, para que la fluidez de la información no se detenga y se acumule el trabajo.

175) Utilizar un documento que controle la transmisión del papeleo entre los diversos usuarios y la función de entrada de datos.

176) Desarrollar procedimientos escritos para el manejo de errores con el fin de proporcionar al personal usuario instrucciones comprensivas para la detección de errores en los documentos fuente, de errores en las correcciones, y de retorno de los datos corregidos. Así mismo identificar los errores que se den al ingresar los datos al sistema y consultar el soporte técnico.

177) Asegurar que el personal recibe la capacitación adecuada y constante.

178) Rotar periódicamente los deberes entre el personal de una misma área.

b. Controles de salida.

179) La información debe ser revisada antes de llevarla fuera del proceso de datos. Los departamentos que la utilizan detectan errores en el empleo de información.

180) Producir únicamente la cantidad requerida de reportes de salida.

181) Revisar siempre todos los errores ya las razones de su ocurrencia con el fin de determinar si los problemas son de programa o de entrada.

182) Controlar la distribución de los reportes de manera que se envíen únicamente al personal autorizado.

183) Conservar en un área todos los reportes confidenciales de manera que el personal no autorizado no pueda obtener copias.

184) Si la información se almacena digital, ya sea en dispositivos de almacenamiento o en una “nube”, es necesario protegerla con contraseñas o en su caso resguardar las unidades en caja fuerte o archivos protegidos.

185) En el caso de documentos confidenciales, si las salidas son abortadas, deben destruirse con una trituradora de papel. Si la generación fue digital, los archivos deben borrarse también de la papelera de reciclaje de la computadora.

186) Revisar periódicamente los mensajes de error dados por la computadora y los mensajes de control de las salidas del sistema con el fin de determinar si hay fallas en el programa.

187) Elaborar un programa de análisis global de reportes con el fin de determinar si deben ser eliminados, combinados, reagrupados, simplificados, o si se requieren de nuevos reportes.

188) Asignar a un responsable del control de la calidad de los reportes.

189) Los reportes deben ser bien identificados incluyendo: la fecha de preparación, periodo cubierto de proceso, titulo descriptivo del reporte, departamento, usuario, identificación del programa que lo generó, como se debe disponer del reporte y determinar su carácter de confidencialidad.

190) Los reportes deben ser numerados identificando la finalización del mismo.

191) Si el reporte no ha sido generado por un sistema, el creador debe considerar dos pasos anteriores en lo que respecta, además identificarse como creador del mismo, y el origen de los datos proporcionados.

192) El ADB que construya los reportes debe estar accesible ante cualquier cambio que se quiera hacer, o en caso de error en el mismo.

193) Si los reportes son convertidos del sistema a aplicaciones ofimáticas, es necesario comparar la información y verificar el correcto traslado de los datos, para poder ser manipulados. Es necesaria la eliminación de los archivos que ya no se utilicen, y resguardar los reportes.

194) Los archivos de reportes definitivos deben ser etiquetados y almacenados de acuerdo al grado de su confidencialidad.

c. Controles de proceso.

195) Verificar que el sistema envíe mensajes de error al usuario, cuando este se equivoque en algún paso, o al introducir algún dato.

196) Hacer que los programas comparen el conteo de las transacciones de entrada, con las procesadas y con las salidas.

197) Establecer que los programas busquen asientos duplicados y erróneos.

198) Definir los perfiles de cada usuario delimitado a las funciones propias de cada uno.

199) Mantener un programa que controle las diversas bibliotecas de programas de computador y que muestre cualesquiera modificaciones que hayan sido hechas a estas bibliotecas.

200) Definir que solamente los ADB pueden modificar y programar los distintos sistemas operativos y de aplicación.

201) Verificar que el sistema mantenga un registro de los usuarios que acceden y modifican las transacciones, fecha y hora.

202) Si las transacciones son modificadas por los usuarios programar que el sistema les pregunte la razón de que se esté modificando, para futuras consultas.

203) Ver que el sistema genere reportes que puedan usarse para identificar todas las transacciones alimentadas por un usuario.

204) Si los archivos de instalación y legales de los programas serán escaneados para su almacenamiento, debe almacenarse con seguridad.

205) Cuando se actualicen los programas se debe capacitar al personal de los cambios efectuados para evitar problemas en el uso.

206) Hacer que los programas acumulen datos para preparar un reporte de los intentos no autorizados de acceso al sistema, a tablas restringidas y similares.

207) Establecer restricciones de acceso a los programas de utilería del sistema que permitan la modificación y parametrización.

208) Usar una metodología de verificación para controlar o detectar cambios no autorizados en los sistemas.

209) Usar claves de protección en los programas del software con objeto de salvaguardar datos que estén en la memoria o en discos duros.

210) Utilizar técnicas criptográficas para almacenar datos.

211) Que el sistema emita un informe de discrepancias entre el sistema contable y los GDS, para controlar y corregir los errores y mostrar datos fieles.

212) Guardar bajo custodia segura las copias de los programas (de las aplicaciones y de los sistemas), de manera que no puedan ser sustraídos fácilmente de la organización.

213) Verificar que estén adecuadamente documentados todos los programas de las aplicaciones del sistema operativo suministrado por el proveedor.

3.2.6 **Elaboración de matriz de control interno informático.**

Luego de diseñar los controles, se elabora la matriz para facilitar la identificación del activo contra el riesgo. Existen unos activos y riesgos no referenciados a un control, lo cual no indica que no apliquen, sino que a lo largo de la lectura de ellos podrán ser identificados implícitamente.

Siempre siguiendo con el establecimiento de controles en las tres áreas citadas: datos, sistemas y personal, procede a relacionar los controles para cada área.

En los siguientes cuadros se coloca la referencia de controles a los que obtuvieron un riesgo total de 8 a 16, y otros que aunque su riesgo total fue menor se les coloco referencia.

Las cuales se entenderán de la siguiente manera:

Para el activo “Documentos institucionales” se presenta el riesgo de “Robo / hurto de información electrónica”, los documentos pueden comprender escrituras, contratos, información contable, manuales de instalación de software, correos electrónicos, entre otros, que deben estar debidamente almacenados y protegidos, para ello la entidad puede optar por seguir los siguientes controles:

162. Utilizar restricciones para evitar la modificación y extracción de información sensible, como protección de hojas de edición.

163. Segregar la responsabilidad de las funciones de generación de transacciones, registros y la custodia de la misma.

167. Registrar los datos de una forma pre impreso o utilizar sellos que den seguridad contra errores u omisiones, y así sucesivamente se van referenciando para cada activo su respectivo control para prevenir, detectar y corregir amenazas.

Cuadro E-1 Controles para área de datos e información (riesgo criminalidad y motivación política).

Datos e Información	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Violación a derechos de autor
Documentos institucionales	26, 29, 121	182		162, 163, 167	162, 163, 167	155	162, 163, 167	96, 162, 163, 167	162, 163, 167	51	59	130, 132	54, 204, 213
Finanzas	26	26		161, 166, 183, 184, 185	161, 166, 183, 184, 185	155	161, 166, 183, 184, 185	96, 161, 166, 183, 184, 185	161, 166, 183, 184, 185	51	59	130, 132	54, 204
Servicios bancarios							14,		184				
Documentación contable	26	183		162, 166, 183, 184, 185	162, 166, 183, 184, 185	9, 155	162, 166, 183, 184, 185	96, 162, 166, 183, 184, 185	162, 166, 183, 184, 185	51	56, 57, 59	130, 132	204
Directorio de Contactos													
Tarifario (Folletos, Fotos, entre otros)				162, 166, 183, 184, 185	162, 166, 183, 184, 185		58	162, 166, 183, 184, 185	162, 166, 183, 184, 185	51	59	130, 132	59
Correo electrónico				51, 56	56, 132		58	56, 132	56, 132	51, 56	56, 57, 58	130, 132	132, 134
Bases de datos clientes	58	58		28, 58, 119, 135, 137, 144	28, 58, 119, 135, 137, 144	9, 155	58	28, 58, 119, 135, 137, 144	28, 58, 119, 135, 137, 144	51	59, 60	130, 132	204
Bases de datos proveedores				28, 58, 119, 135, 137, 144, 169			58		28, 58, 119, 135, 137, 144, 169				204
Bases de datos colaborativos							58		58				204
Página Web interna (Intranet)				51, 56	51, 56		51, 56	51, 56, 96	51, 56	51	59, 60	130, 132	54, 204
Página Web externa							58		58				54, 204
Respaldos				25, 73, 103, 173	25, 73, 103, 173, 212		58	67, 96	25, 73, 103, 173, 212	51	58, 59, 60, 210	130, 132	204
Infraestructura (Planos, Documentación legal)				99	121		58	96, 99, 121	58, 204	51	58, 59, 60	130, 132	204
Informática (Planos de redes, Documentación legal)							58		58, 204				54, 204
Base de datos de Contraseñas				51, 56	51, 56		58	51, 56, 96	51, 56	51	58	130	56
Navegación en Internet							58		51				132, 134
Chat externo				51	51		58	51	51	51	198	198	132, 134
Llamadas telefónicas externas				154, 155	154, 155		154, 155	154, 155	154, 155	154, 155	154, 155	154, 155	154, 155

Cuadro E-2 Controles para área de datos e información (sucesos de origen físico).

Datos e Información	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
Documentos institucionales	72, 74, 75, 77, 78, 79, 80, 81-86.		86				87-92	87-92	88-92
Finanzas	72, 74, 75, 77, 78, 79, 80, 81-86.		86				87-92	87-92	88, 92
Servicios bancarios									
Documentación contable	72, 74, 75, 77, 78, 79, 80, 81-86.		86				87-92	87-92	88, 92
Directorio de Contactos									
Tarifario (Folletos, Fotos, entre otros)								87-92	
Correo electrónico								87-92	
Bases de datos clientes	72, 74, 75, 77, 78, 79, 80, 81-86.		86				87-92	87-92	88, 92
Bases de datos proveedores									
Bases de datos colaborativos									
Página Web interna (Intranet)								87-92	
Página Web externa									
Respaldos								87-92	
Infraestructura (Planos, Documentación legal)								87-92	
Informática (Planos de redes, Documentación legal)									
Base de datos de Contraseñas								87-92	
Navegación en Internet									
Chat externo								87-92	
Llamadas telefónicas externas								87-92	

Cuadro E-3-1 Controles para área de datos e información (sucesos derivados de la impericia, negligencia de usuarios y decisiones institucionales).

Datos e Información	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software "pirateado"	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento.
Documentos institucionales	177	40, 176, 177, 205	54, 55	173	144, 156	210	210	210	51, 56, 184	17, 107, 198, 201	17, 107, 155	17, 96, 98, 99, 107
Finanzas	177	40, 176, 177, 205	54, 55	173	144, 156	210	210	210	51, 56, 184	17, 107, 198, 201	17, 107, 155	17, 96, 98, 99, 107
Servicios bancarios			54, 55	173								
Documentación contable	177	40, 176, 177, 205	54, 55	173	144, 156	210	210	210	51, 56, 184	17, 107, 198, 201	17, 107, 155	17, 96, 98, 99, 107
Directorio de Contactos				173								
Tarifario (Folletos, Fotos, entre otros)		40, 176, 177, 205	54, 55	173	144, 156		210		51, 56, 184	17, 107, 198, 201	17, 107, 155	
Correo electrónico		40, 176, 177, 205	54, 55	173	144, 156		210		51, 56, 184	17, 107, 198, 201	17, 107, 155	
Bases de datos clientes	177	40, 176, 177, 205	54, 55	173	144, 156	210	210	210	51, 56, 184	17, 107, 198, 201	17, 107, 155	17, 96, 98, 99, 107
Bases de datos proveedores			54, 55	173		210						
Bases de datos colaborativos			54, 55	173								
Página Web interna (Intranet)		40, 176, 177, 205	54, 55	173	144, 156		210		51, 56, 184	17, 107, 198, 201	17, 107, 155	
Página Web externa			54, 55	173								
Respaldos		40, 176, 177, 205	54, 55	173	144, 156		210		51, 56, 184	17, 107, 198, 201	17, 107, 155	
Infraestructura (Planos, Documentación legal)		40, 176, 177, 205	54, 55	173	144, 156		210		51, 56, 184	17, 107, 198, 201	17, 107, 155	
Informática (Planos de redes, Documentación legal)			54, 55	173								
Base de datos de Contraseñas		40, 176, 177, 205	54, 55	173	144, 156		210		51, 56, 184	17, 107, 198, 201	17, 107, 155	
Navegación en Internet			54, 55	173								
Chat externo		40, 176, 177, 205	54, 55	173	144, 156		210		51, 56, 184	17, 107, 198, 201	17, 107, 155	
Llamadas telefónicas externas		177		173	144, 156		210		51, 56, 184	17, 107	17, 107, 155	

Cuadro E-3-2 Controles para área de datos e información (sucesos derivados de la impericia, negligencia de usuarios y decisiones institucionales).

Datos e Información	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
Documentos institucionales	35	198	44, 45, 52	52	46, 117, 186	30, 31, 36	36	89	33, 124, 129, 184, 206	99, 124	6, 14	1, 2	26, 29, 100
Finanzas	35	198	44, 45, 52	52	46, 117, 186	30, 31, 36	36	89	33, 124, 129, 184, 206	99, 124	6, 14	1, 2	26, 29, 100
Servicios bancarios				52							6, 14		
Documentación contable	35	198	44, 45, 52	52	46, 117, 186	30, 31, 36	36	89	33, 124, 129, 184, 206	99, 124	6, 14	1, 2	26, 29, 100
Directorio de Contactos				52							6, 14		
Tarifario (Folletos, Fotos, entre otros)	35	198		52					33, 124, 129, 184, 206	99, 124	6, 14	1, 2	
Correo electrónico	35	198		52					33, 124, 129, 184, 206	99, 124	6, 14	1, 2	
Bases de datos clientes	35	198	44, 45, 52	52	46, 117, 186	30, 31, 36	36	89	33, 124, 129, 184, 206	99, 124	6, 14	1, 2	26, 29, 100
Bases de datos proveedores				52							6, 14		
Bases de datos colaborativos				52							6, 14		
Página Web interna (Intranet)	35	198		52					33, 124, 129, 184, 206	99, 124	6, 14	1, 2	
Página Web externa				52							6, 14		
Respaldos	35	198		52					33, 124, 129, 184, 206	99, 124	6, 14	1, 2	
Infraestructura (Planos, Documentación legal)	35	198		52					33, 124, 129, 184, 206	99, 124	6, 14		
Informática (Planos de redes, Documentación legal)				52							6, 14		
Base de datos de Contraseñas	35	198		52					33, 124, 129, 184, 206	99, 124	6, 14	1, 2	
Navegación en Internet				52							6, 14		
Chat externo	35	198		52					33, 124, 129, 184, 206	99, 124	6, 14		
Llamadas telefónicas externas	35	198		52					33, 129	99, 124	6, 14		

Cuadro E-4 Controles para área de sistemas e infraestructura (actos originados por la criminalidad común y motivación política).

Sistemas e Infraestructura	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Violación a derechos de autor
Equipos de la red cableada (router, switch)				67, 68,72 ,74,75,88,89, 90,100,132	67, 68,72 ,74,75,88,89,90 ,100,132	95,96	51	56,63 64	96	132	132	132	132
Equipos de la red inalámbrica (router, punto de acceso)				67, 68,72 ,74,75,88,89, 90,100,132	67, 68,72 ,74,75,88,89,90 ,100,132	95,96	51	56,63 64	96	132	132	132	132
Cortafuego				132	132	95,96	51	56	132	132	132	132	54
Servidores	34	34		67, 68,72 ,74,75,88,89, 90,100,132	67, 68,72 ,74,75,88,89,90 ,100,132	95,96	51,97	56,63, 64,72	96	132	132	132	54
Computadoras				41	41		51,97	41,42	96	129	130	53	54
Portátiles				41	41		51,97	41,42	96	129	130	53	54
Programas de administración (contabilidad, manejo de personal)	33	33		132	132	132	51,97	97	96	132	57	57	54
Programas de producción de datos (ERP y GDS)	33	33		132	132	132	51,97	97	96	132	57	57	54
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, redes sociales)				51	51		51		58	132	132	53	54
Impresoras							3						
Memorias portátiles													
PBX (Sistema de telefonía convencional)									38				
Celulares									38				
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, entre otros)									38				

Cuadro E-5 Controles para área de sistemas e infraestructura (sucesos de origen físico).

Sistemas e Infraestructura	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
Equipos de la red cableada (router, switch)	73,74,75		72				88,89	87	88
Equipos de la red inalámbrica (router, punto de acceso)	73,74,75		73,	69			88,89	87	88
Cortafuego	73,74,75		73,				88,89	87	88
Servidores	73,74,75		73,	69			88,89	87	88
Computadoras				69				88	
Portátiles				69				88	
Programas de administración (contabilidad, manejo de personal)	67		73				88,89	87	87
Programas de producción de datos (ERP y GDS)	67		73				88,89	87	87
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, redes sociales)								87	
Impresoras				69					
Memorias portátiles									
PBX (Sistema de telefonía convencional)				69					
Celulares									
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, entre otros)				69					

Cuadro E-6-1 Controles para área de sistemas e infraestructura (sucesos derivados de la impericia, negligencia de usuarios y decisiones institucionales).

Sistemas e Infraestructura	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software "pirateado"	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, entre otros.
Equipos de la red cableada (router, switch)		40	53		59, 135,136,140, 144,145,146	109, 110		156, 184, 185,210	210	51	51	51	41, 42
Equipos de la red inalámbrica (router, punto de acceso)		40	53		59, 135, 136, 140, 144, 145, 146	109, 110		156, 184, 185,210	210	51	51	51, 155	41, 42
Cortafuego		132	132		132	109, 110		156, 184, 185,210	210	51	51	51, 155	41, 42
Servidores		40	53		59, 135, 136, 140, 144, 145, 146	109, 110		156, 184, 185,210	210	51	51	51, 155	41, 42
Computadoras			53		59, 135, 136, 140, 144, 145, 146								
Portátiles			53		59, 135,136,140, 144,145,146								
Programas de administración (contabilidad, manejo de personal)		40	53		59, 135,136,140, 144,145,146	109, 110		156, 184, 185,210	210	51	51	51, 155	
Programas de producción de datos (ERP y GDS)		40	53		59, 135,136,140, 144,145,146	109, 110		156, 184, 185,210	210	51	51	51, 155	
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, redes sociales)			53		59, 135,136,140, 144,145,146								
Impresoras													41, 42
Memorias portátiles													41, 42
PBX (Sistema de telefonía convencional)													41, 42
Celulares													41, 42
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, entre otros)													41, 42

Cuadro E-6-2 Controles para área de sistemas e infraestructura (sucesos derivados de la impericia, negligencia de usuarios y decisiones institucionales).

Sistemas e Infraestructura	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
Equipos de la red cableada (router, switch)	51	51	44, 45, 124	38, 52	51				33, 127, 129, 147, 201, 206	46, 47	40, 50, 86, 177, 205		
Equipos de la red inalámbrica (router, punto de acceso)	51	51	44, 45, 124	38, 52	51					46, 47	40, 50, 86, 177, 205		
Cortafuego	51	51	44, 45, 124	38, 52	51				33, 127, 129, 147,	46, 47	40, 50, 86, 177, 205		
Servidores	51	51	44, 45, 124	38, 52	51				33, 127, 129, 147, 201, 206	46, 47	40, 50, 86, 177, 205		
Computadoras					51					46, 47	40, 50, 86, 177, 205		
Portátiles					51					46, 47	40, 50, 86, 177, 205		
Programas de administración (contabilidad, manejo de personal)	201	51		38, 52	51				33, 127, 129, 147, 201, 206	46	40, 50, 86, 177, 205		
Programas de producción de datos (ERP y GDS)	201	51		38, 52	51				33, 127, 129, 147, 201, 206	46	40, 50, 86, 177, 205		
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, redes sociales)				38, 52	51					46, 47	40, 50, 86, 177, 205		
Impresoras			44, 45, 124	38, 52, 205	51					46, 47			
Memorias portátiles										46, 47			
PBX (Sistema de telefonía convencional)			44, 45, 124							46, 47			
Celulares										46, 47			
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, entre otros)			44, 45, 124	52, 55, 124						46, 47			

Cuadro E-7 Controles para área personal (actos originados por la criminalidad común y motivación política).

Personal	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Violación a derechos de autor
Junta Directiva	17, 26, 29	17		163, 167	163, 167	155	163, 167	96, 162, 163, 167	162, 163, 167	51, 66	59, 60, 96	130, 132, 134	54, 204, 213
Gerencia General				163, 167	127		124	33, 57	58, 59, 60	51, 66	59, 60, 96	130, 132, 134	142
Administración				132, 163, 167	127, 133		124, 170, 171	33, 57	58, 59, 60	51, 66	59, 60, 96	130, 132, 134	142
Personal técnico (asesor de ventas)	17, 26, 29	17		96, 99, 132, 163, 167	96, 99, 132, 163, 167	155	124, 170, 171	33, 57	58, 59, 60	51, 66	59, 60, 96	130, 132, 134	142
Recepción							124		58, 59,				142
Informática / Soporte técnico interno				96, 99	88		124	33, 57	58, 59, 60	51, 66	59, 60, 96	130, 132, 134	142
Soporte técnico externo				124	88		124	33, 57	58, 59, 60	51, 66	59, 60, 96	130, 132, 134	142
Servicio de limpieza externo							124		124				142
Servicio de mensajería externo				124	124		124	124	124	124	124	124	

Cuadro E-8 Controles para área personal (sucesos de origen físico).

Personal	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
Junta Directiva	8, 14		8, 14				8, 14	8, 14	8, 14
Gerencia General	8, 14, 86		8, 14, 86					8, 14	
Administración	86		86					8, 14	
Personal técnico (asesor de ventas)	86		86						
Recepción	86		86						
Informática / Soporte técnico interno	86		86					71, 92	
Soporte técnico externo								71	
Servicio de limpieza externo	86		86						
Servicio de mensajería externo									

Cuadro E-9-1 Controles para área personal (sucesos derivados de la impericia, negligencia de usuarios y decisiones institucionales).

Personal	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software "pirateado"	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos criticos (codificar, borrar)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, entre otros.
Junta Directiva	8, 14	40				156		210	210	1, 51	107	107, 155	17
Gerencia General		40	54, 55		13, 140	156		210		1, 51	107	107, 155	
Administración	14, 177	40	54, 55		13, 140	156		210		51	107	107, 155	
Personal técnico (asesor de ventas)	14, 177	40				156		210	210	51	107	107, 155	99
Recepción						156							
Informática / Soporte técnico interno	14, 177	40	54, 55		13, 140	156	210	210		1, 51	107	107, 155	
Soporte técnico externo						156		210			107	107, 155	
Servicio de limpieza externo													
Servicio de mensajería externo					124	156		210			107	107, 155	

Cuadro E-9-2 Controles para área personal (sucesos derivados de la impericia, negligencia de usuarios y decisiones institucionales).

Personal	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control	Ausencia de documentación
Junta Directiva	1, 4	198									6, 14	1, 2	
Gerencia General	1, 4	198			46, 117, 186						6, 14	1, 2	26, 29, 100
Administración	1, 4	198			46, 117, 186						6, 14	1, 2	
Personal técnico (asesor de ventas)	1, 4	198			46, 117, 186	46, 117, 186	46, 117, 186	46, 117, 186		99, 124	14,	2,	26, 29, 100
Recepción											14,		
Informática / Soporte técnico interno		198	44, 45, 52	52	46, 117, 186	46, 117, 186	46, 117, 186	46, 117, 186			14,	2,	
Soporte técnico externo		198							89	99, 124	14,		
Servicio de limpieza externo										99, 124	14,		
Servicio de mensajería externo		198								99, 124	14,		

CAPÍTULO IV CONCLUSIONES Y RECOMENDACIONES.

4.1 Conclusiones

a) Para el diseño de un sistema de control interno informático basado en riesgos es necesario identificar los activos o recursos que posee la entidad, luego realizar la gestión de los riesgos informáticos a los que están expuestos.

b) Una adecuada gestión de riesgos ayuda en el diseño adecuado de controles preventivos, detectivos y correctivos que actúen sobre la causa de los riesgos para disminuir la probabilidad de ocurrencia.

c) El concepto de optimización sugerido por COBIT 5 *For Risk* sugiere una gestión de riesgos adecuada que no permita superar el nivel aceptable establecido por el gobierno, y que el impacto del riesgo inherente es tratado, además el incumplimiento de leyes es minimizado. Lo cual es aplicable para cualquier entidad que desee salvaguardar sus activos.

d) En cuanto a la decisión de cuales controles internos informáticos son requeridos para optimizar su exposición al riesgo, depende de la pericia del profesional en contaduría pública y del conocimiento técnico que posea.

e) Si los controles propuestos se implementan con éxito en los riesgos identificados, se logra obtener el resguardo y la seguridad en la información que maneja la compañía, reduciendo en gran medida la pérdida de datos y recursos ante cualquier eventualidad.

4.2 Recomendaciones

a) Debido a la actividad que desempeñan, las agencias de viajes podrían considerar que sus controles internos se enfoquen en prevenir, detectar, y corregir riesgos que amenacen sus activos.

b) Toda entidad que hace uso de la tecnología de información como parte usual en sus operaciones diarias, se recomienda el establecimiento de controles internos informáticos que faciliten la optimización de los riesgos inherentes al uso de estas tecnologías.

c) Es importante que los profesionales en contaduría pública, como parte de su educación continua, amplíen su conocimiento del uso de tecnologías de información para definir el perfil ideal trazado en IEPS y expandir su oferta de servicios de auditoría o consultoría.

BIBLIOGRAFÍA

Benítez, M.R., Lara, G.A., Menjívar, M.A. (2003) *El control financiero como una herramienta para la toma de decisiones de las agencias de viajes del área metropolitana de San Salvador.* Tesis. UTEC, San Salvador, El Salvador.

COBIT 5 *For Risk* ISACA.

Controles Internos para sistemas de computación, Jerry Fitzgerald, Editorial Limuza, México.

Fonseca, Oswaldo (2011) *Sistemas de control interno para organizaciones.* Perú: Instituto de Investigación en Accountibility y Control.

Guías para la gestión de la seguridad de TI /TEC TR 13335-1, 1996

Introducción a Riesgo Informático, FCEA, Agosto de 2004, L. Sena, S.M. Tenzer.

ISACA, información. Disponible en World wide web: http://www.isaca.org/spanish/Pages/default.aspx

Muñoz de Escalona y Lafuente, F. (2003). *El Turismo explicado con claridad.* Libros en Red.

Poch Ramón (1997), *Manual de control interno: los circuitos informativos en la administración empresarial.* Ediciones Gestión 2000, S.A. Barcelona.

Solano, O.J. (2012) *Referencias teóricas para la construcción de un marco Teórico en el estudio del sistema de control interno Informático en ambiente computacional en la organización*. Universidad del Valle.

Solarte Francisco Nicolás Javier, Universidad Modular Abierta y a la Distancia, Colombia, Disponible en: http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_5_matrices_y_mapas_de_riesgo.html.

ANEXOS

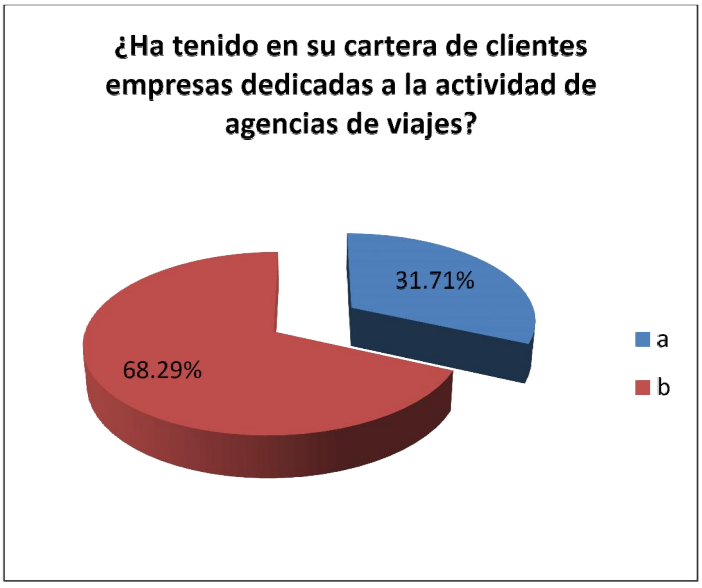
ÍNDICE DE ANEXOS

ANEXO 1 TABULACIÓN DE UNIDAD DE ANALISIS PROFESIONALES EN CONTADURÍA PÚBLICA DEL MUNICIPIO DE SAN SALVADOR.

A continuación la interpretación de los resultados del cuestionario efectuado a la muestra de 41 profesionales en contaduría pública con personería jurídica del municipio de San Salvador, en el departamento de San Salvador.

1. ¿Ha tenido en su cartera de clientes empresas dedicadas a la actividad de agencias de viajes?

Literal	Respuesta	Frecuencia	Porcentaje
a	Si	13	31.71%
b	No	28	68.29%
TOTAL		41	100.00%



INTERPRETACIÓN: Del 100% de los encuestados el 31.71% responde que ha tenido en su cartera de clientes empresas dedicadas a la actividad de agencias de viajes, mientras que un 68.29% manifiesta no tener.

2. ¿Qué servicios profesionales ha prestado a este tipo de entidades?

Literal	Respuesta	Frecuencia Absoluta	Frecuencia Relativa
a	Auditoría	11	84.62%
b	Consultoría	5	38.46%
c	Contabilidad	5	38.46%

INTERPRETACIÓN: El 31.71% de firmas que manifestaron haber tenido en su cartera de clientes empresas dedicadas a agencia de viajes, han prestado el servicios de auditoría con una frecuencia del 84.62%, los servicios de consultoría con un 38.46% y con el mismo porcentaje el de contabilidad.

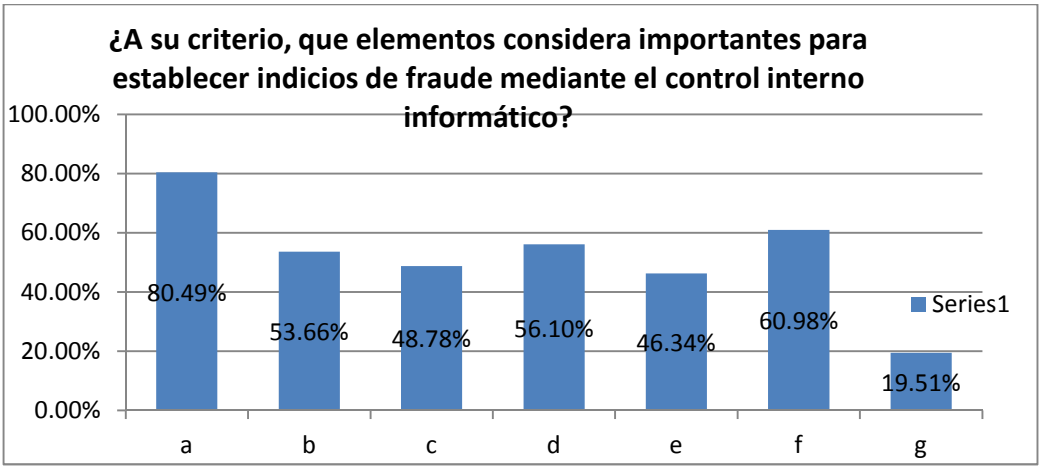
3. ¿Dentro de su cartera de clientes, aquellos que manejan tecnologías de información poseen procedimientos que controlen el riesgo informático?

Literal	Respuesta	Frecuencia	Porcentaje
a	Si	14	34.15%
b	No	25	60.98%
c	No Responde	2	4.88%
TOTAL		41	100%

INTERPRETACIÓN: Al cuestionar si los clientes poseen procedimientos que controlen el riesgo informático, solamente el 35.90% contestan positivamente, mientras que un 64.10% dicen que no los poseen, el 4.88% no responde.

4. ¿A su criterio, que elementos considera importantes para establecer indicios de fraude mediante el control interno informático? Puede seleccionar más de una opción.

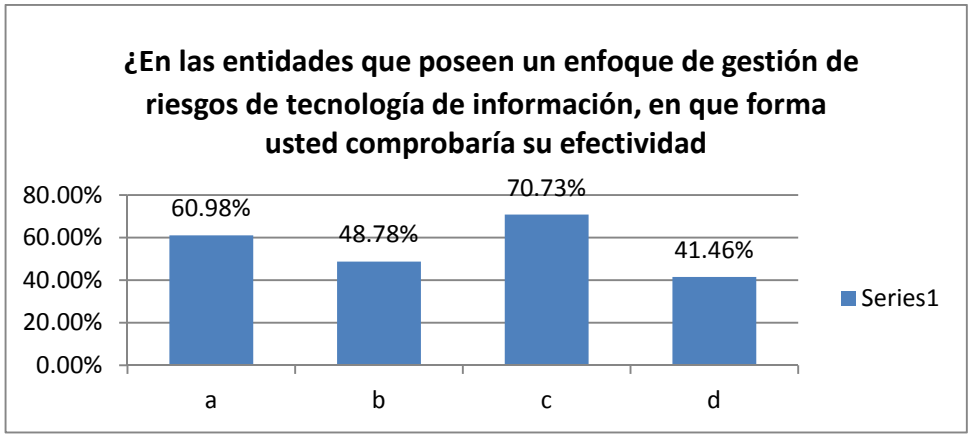
Literal	Respuesta	Frecuencia Absoluta	Frecuencia Relativa
A	Registro de operaciones ficticias.	33	80.49%
B	Omisión de registro de operaciones en el periodo correspondiente.	22	53.66%
C	No revelar hechos que pueden afectar los datos ingresados.	20	48.78%
D	Manipular resultados a través de operaciones complejas entre compañías.	23	56.10%
E	Manipulación, falsificación o alteración de registros o documentos soportes.	19	46.34%
F	Mala aplicación de políticas de control interno informático.	25	60.98%
G	Apropiación indebida o utilización irregular de activos.	8	19.51%



INTERPRETACIÓN: Los encuestados consideran los siguientes elementos importantes para establecer indicios de fraude informático, con una frecuencia de 80.49% se encuentra el registro de operaciones ficticias, con 60.98% podría encontrarse por la mal aplicación de políticas de control interno informático, con 56.10% por la manipulación de resultados a través de operaciones complejas entre compañías, con 53.66% por omisión en el registro de operaciones, un 48.78% podría surgir por la no revelación de hechos que pueden afectar los datos ingresados al sistema, con 46.34% de frecuencia la manipulación, falsificación y alteración de registros o documentos soportes, y con un 19.51% la idea de que exista apropiación o utilización irregular de activos

5. ¿En las entidades que poseen un enfoque de gestión de riesgos de tecnología de información, en qué forma usted comprobaría su efectividad? Puede seleccionar más de una opción.

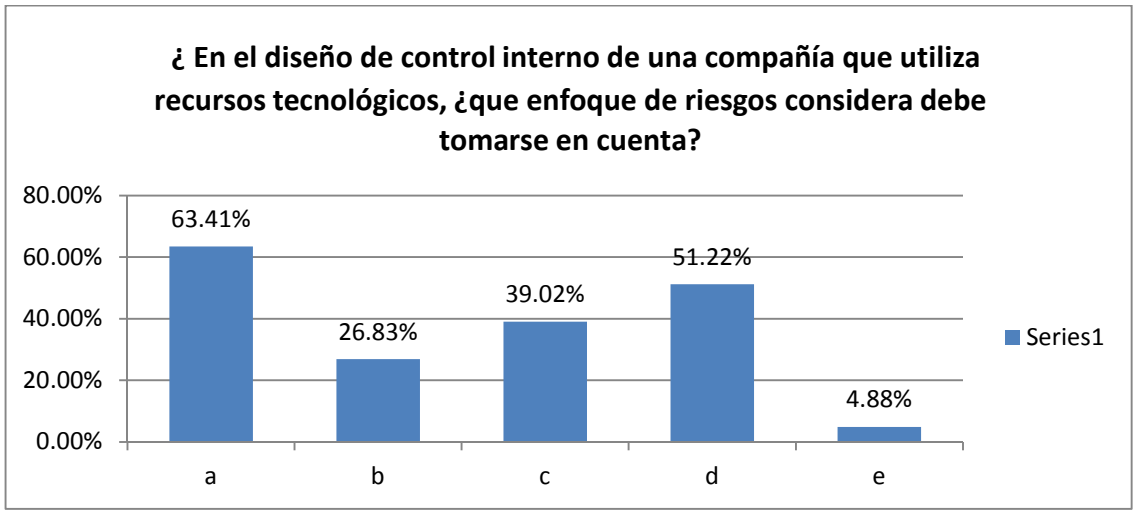
Literal	Respuesta	Frecuencia Absoluta	Frecuencia Relativa
a	Se hace un análisis de la gestión de los riesgos	25	60.98%
b	Se piden informes de revisión.	20	48.78%
c	Se realiza un procedimiento de verificación de cumplimiento.	29	70.73%
d	Se valida si la gestión de riesgos cumple con los objetivos de la entidad	17	41.46%



INTERPRETACIÓN: para comprobar la efectividad de la gestión de riesgos, los encuestados realizan una o varias de las siguientes actividades, con una frecuencia del 70.73% realizan procedimientos de verificación de cumplimiento, con una de 60.98% por medio de un análisis de la gestión de los riesgos, con un 48.78% utilizan informes de revisión, y con un 41.46% validan si la gestión de riesgos cumple con los objetivos de la entidad.

6. En el diseño de control interno de una compañía que utiliza recursos tecnológicos, ¿que enfoque de riesgos considera debe tomarse en cuenta? Puede seleccionar más de una opción.

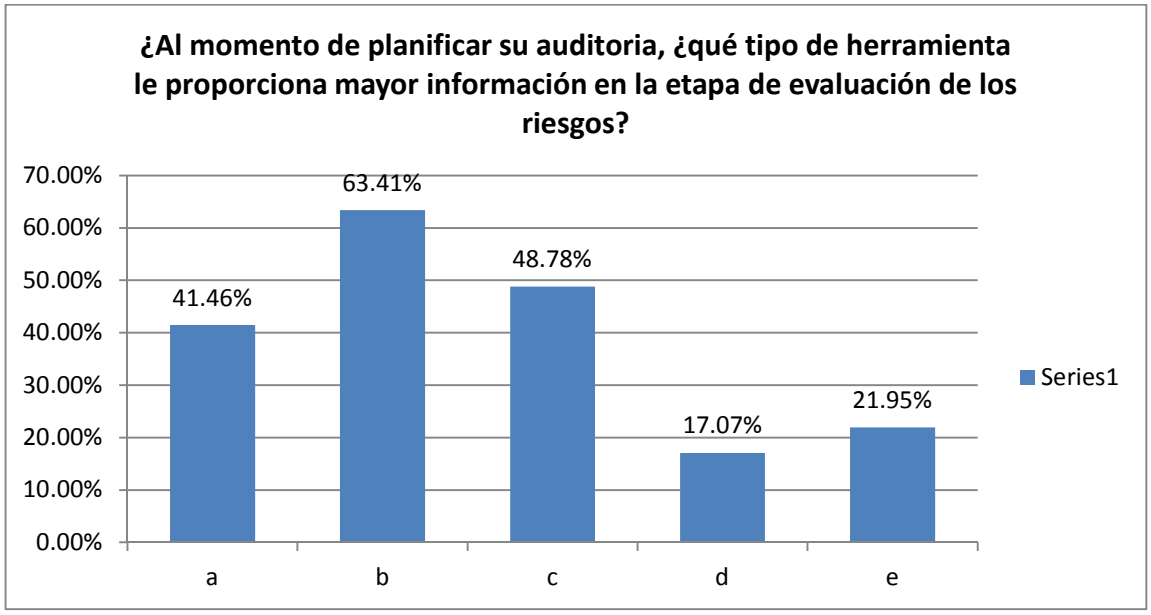
Literal	Respuesta	Frecuencia Absoluta	Frecuencia Relativa
a	COBIT (Objetivos de control para tecnología y áreas relacionadas)	26	63.41%
b	ITIL (Gestión de servicios de TI)	11	26.83%
c	COSO ERM	16	39.02%
d	ISO 27001:2013 (Sistemas de gestión para la seguridad de la información)	21	51.22%
e	No responden	2	4.88%



INTERPRETACIÓN: los marcos teóricos que las firmas utilizarían para evaluar riesgos en compañías que utilizan tecnología de información, son los siguientes: se obtuvo una frecuencia de 63.41% para COBIT, con un 51.22% la norma ISO 27001:2013, con una de 39.02% COSO ERM, con una de 26.83% la biblioteca ITIL.

7. Al momento de planificar su auditoría, ¿qué tipo de herramienta le proporciona mayor información en la etapa de evaluación de los riesgos? Puede seleccionar más de una opción.

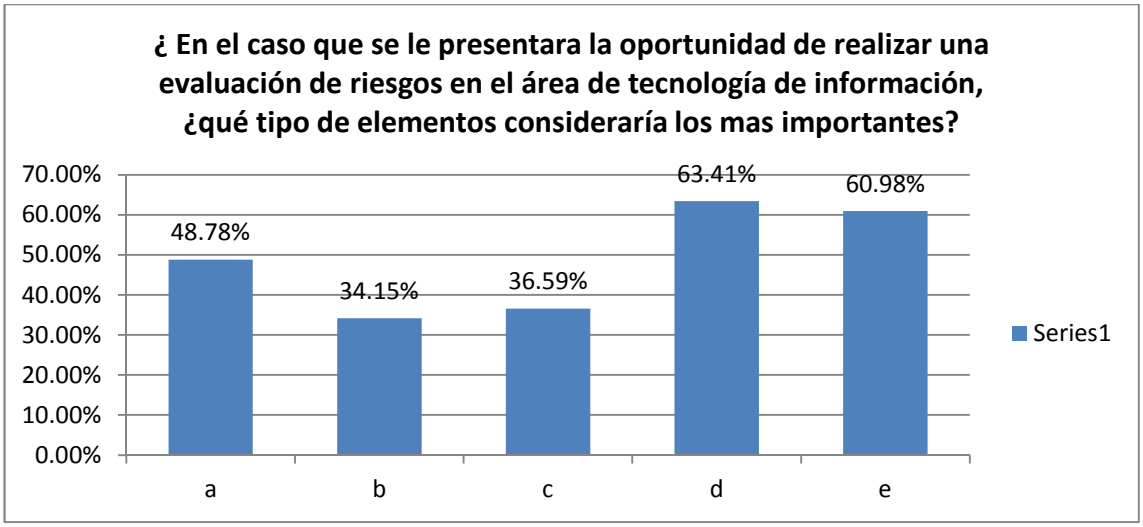
Literal	Respuesta	Frecuencia Absoluta	Frecuencia Relativa
a	Diagrama de Flujos de Procesos	17	41.46%
b	Matrices de Riesgo y Control.	26	63.41%
c	Cuestionarios.	20	48.78%
d	Software especializado.	7	17.07%
e	Software y matrices de riesgo y control	9	21.95%



INTERPRETACIÓN: Las herramientas utilizadas por los encuestados y que le brindan mayor calidad de información al momento de evaluar los riesgos, son las siguientes según su frecuencia, asi con una de 63.41% son utilizadas las matrices de riesgo y control. Con un 48.78% son usados los cuestionarios, con un 41.46% con diagramas de flujos de procesos. La combinación de software especializado con matrices de riesgo y control con 21.95%, y únicamente el uso de software especializado con un 17.07%.

8. En el caso que se le presentara la oportunidad de realizar una evaluación de riesgos en el área de tecnología de información, ¿qué tipo de elementos consideraría los más importantes? Puede seleccionar más de una opción.

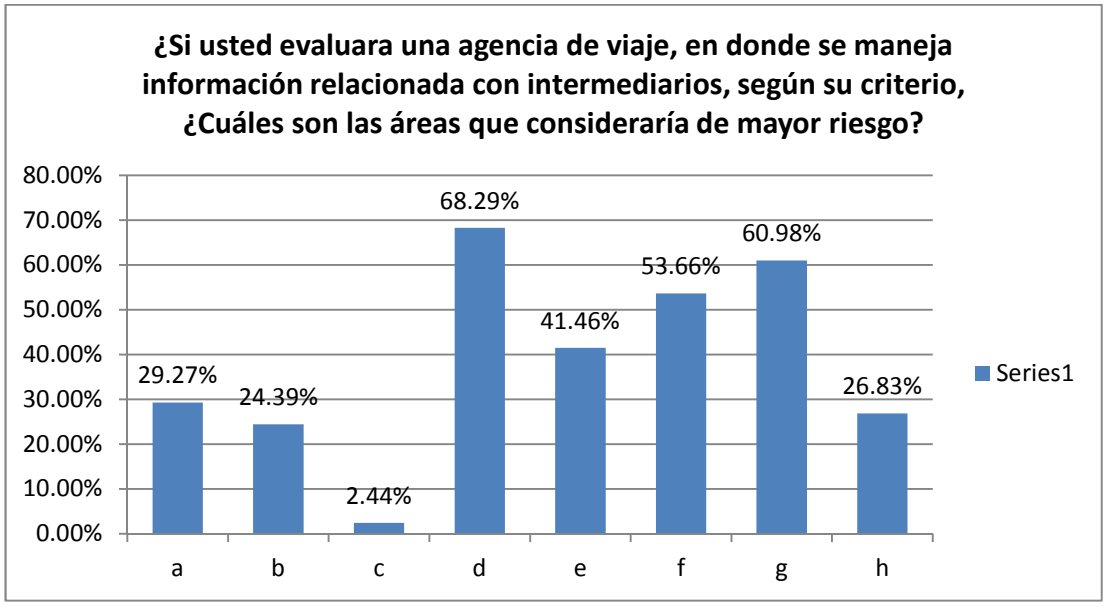
Literal	Respuesta	Frecuencia Absoluta	Frecuencia Relativa
a	Exigencia de la normativa técnica	20	48.78%
b	Indicios de fraude	14	34.15%
c	Creciente dependencia del negocio a la tecnología de información	15	36.59%
d	Carencia de controles del negocio	26	63.41%
e	Dificultades en el personal que realiza la entrada, proceso y salida de la información.	25	60.98%



INTERPRETACIÓN: En el caso que se les presente la oportunidad de evaluar riesgos en el área de tecnología de información, los encuestados respondieron que las áreas que tomarían especial atención seria en su orden por elección y frecuencia: carencia de controles del negocio con un 63.41%, las dificultades en el personal que manipula la información 60.98%, también mantienen que la exigencia técnica es de importancia con 48.78%, por otro lado sostienen que la creciente dependencia del negocio a la tecnología de información presenta riesgos, con un 36.59%, los indicios de fraude considerandos con un 34.15%.

9. Si usted evaluara una agencia de viaje, en donde se maneja información relacionada con intermediarios, según su criterio, ¿Cuáles son las áreas que consideraría de mayor riesgo?

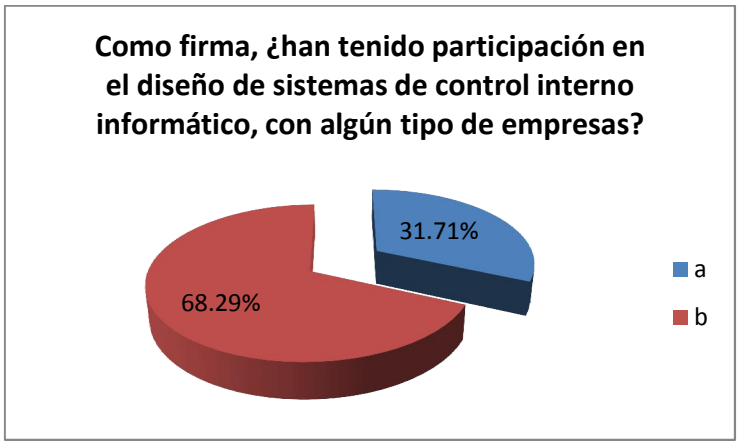
Literal	Respuesta	Frecuencia Absoluta	Frecuencia Relativa
a	Administrativa.	12	29.27%
b	Mercadeo.	10	24.39%
c	Recursos Humanos.	1	2.44%
d	Ventas	28	68.29%
e	Contabilidad	17	41.46%
f	Tecnologías de información	22	53.66%
g	Créditos y Cobros.	25	60.98%
h	Tesorería.	11	26.83%



INTERPRETACIÓN: Los encuestados opinaron que las áreas que consideran con mayor riesgo serian según su frecuencia: Ventas con un 68.29%, Créditos y Cobros un 60.98%, el área de tecnología de Información con un relativa del 53.66%, el departamento de Contabilidad con 41.46%, el área Administrativa con 29.27%, Tesorería obtuvo un 26.83%, las que a su criterio son de menor consideración son Mercadeo con 24.39% y Recursos Humanos con 2.44%.

10. Como firma, ¿han tenido participación en el diseño de sistemas de control interno informático, con algún tipo de empresas?

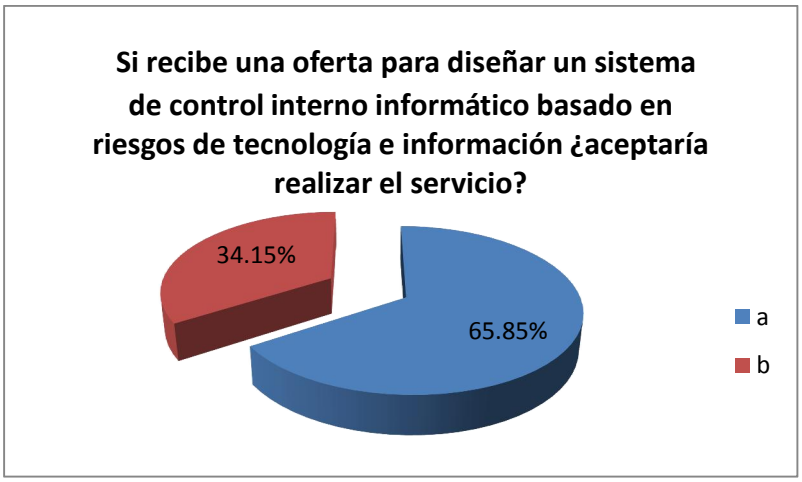
Literal	Respuesta	Frecuencia	Porcentaje
a	Si	13	31.71%
b	No	28	68.29%
TOTAL		41	100.00%



INTERPRETACIÓN: Se indago si las firmas han tenido participación en el diseño de sistemas de control interno informático, resultando solamente un 31.71% positivamente, mientras que el resto 68.29% manifiestan no haber prestado el servicio.

11. Si recibe una oferta para diseñar un sistema de control interno informático basado en riesgos de tecnología e información ¿aceptaría realizar el servicio?

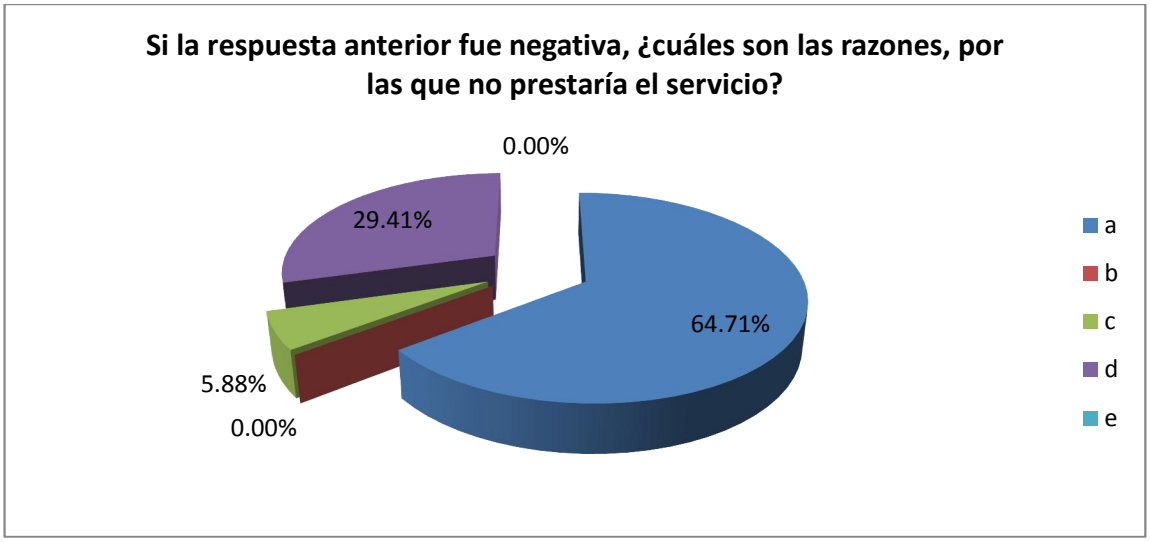
Literal	Respuesta	Frecuencia	Porcentaje
a	Si	27	65.85%
b	No	14	34.15%
TOTAL		41	100.00%



INTERPRETACIÓN: Al consultar a las firmas si tomarían en consideración prestar el servicio de diseñar un sistema de control interno informático basado en riesgos de tecnología de información, el 65.85% contestó afirmativamente, mientras que el 34.15% admite que no tomaría el trabajo.

12. Si la respuesta anterior fue negativa, ¿cuáles son las razones, por las que no prestaría el servicio? Puede seleccionar más de una opción.

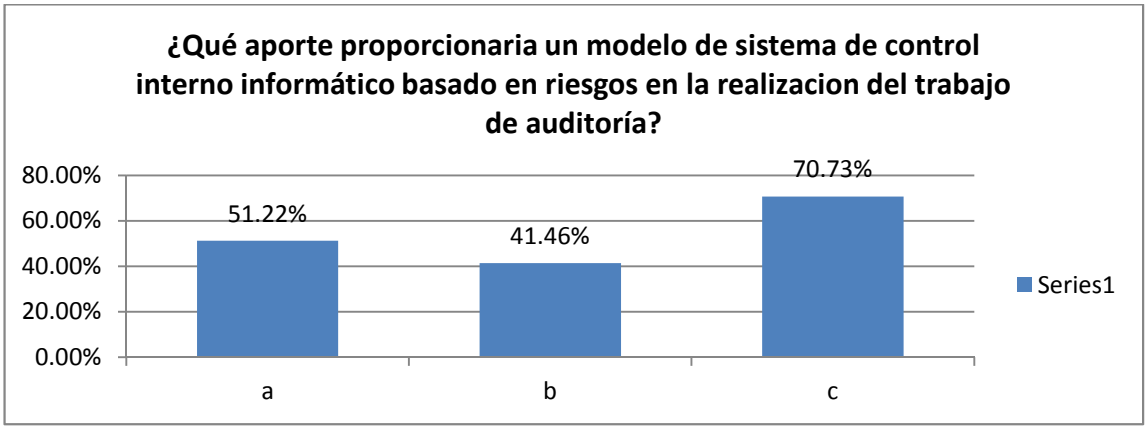
Literal	Respuesta	Frecuencia Absoluta	Frecuencia Relativa
a	Es un área especializada.	11	78.57%
b	No existe una herramienta guía para este tipo de servicio	0	0.00%
c	Complejidad del tema.	1	7.14%
d	No se encuentra un experto en tecnologías.	5	35.71%
e	No hay proceso de formación en tecnología de información.	0	0.00%



INTERPRETACIÓN: En relación a la pregunta número 11, del 34.15% que contestaron negativa la solicitud de realizar el servicio de diseño de control interno informático basado en riesgos, se les cuestiono por qué no prestarían dicho servicio, a lo cual presentaron las siguientes objeciones con su respectiva frecuencia: piensan que es un área especializada con un 78.57%, también consideran que no se encuentran expertos en tecnología que puedan apoyar sus conocimientos con un 35.711%, hubo una opinión que el tema es complejo con 7.14%. No basan sus motivos de negativa porque no exista una herramienta guía para realizarlo, ni tampoco objetan si es porque no exista un proceso de formación en tecnología de información.

13. ¿Qué aporte proporcionaria un modelo de sistema de control interno informático basado en riesgos en la realizacion del trabajo de auditoría? Puede marcar mas de una opción.

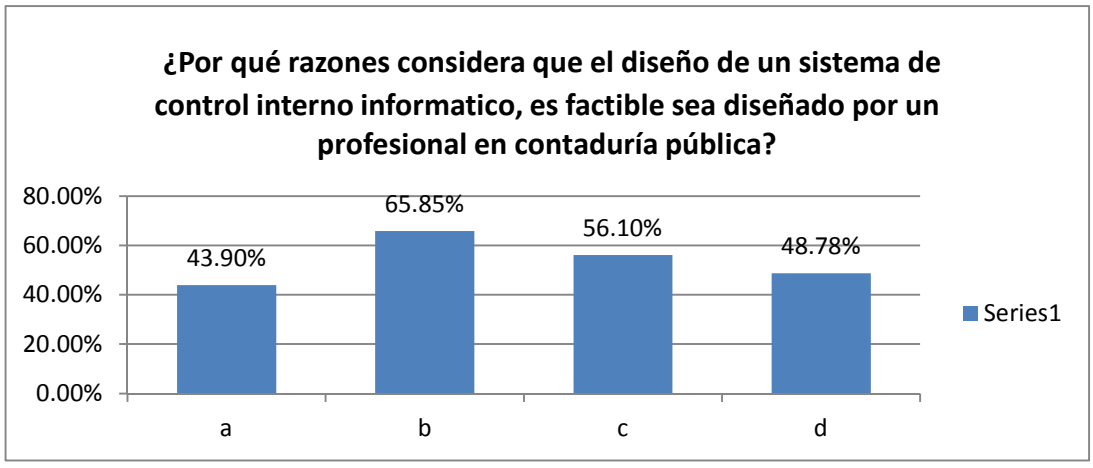
Literal	Respuesta	Frecuencia Absoluta	Frecuencia Relativa
a	Como material de consulta para recomendar mejoras en aspectos de control interno informático	21	51.22%
b	Se tomaría de base para evaluar los riesgos	17	41.46%
c	Como base para establecer procedimientos para evaluar la metodología del control interno informático	29	70.73%



INTERPRETACIÓN: Al cuestionarles sobre si existiera un modelo de sistema de control interno informático basado en riesgos, al cual pudieran obtener acceso, y en que manera lo utilizarían, contestaron según la frecuencia: como ayuda para establecer procedimientos para evaluar la metodología del control interno informático un 70.73%, como material de consulta para recomendar mejoras en aspectos de control interno informático un 51.22%, como base para evaluar riesgos un 41.46%.

14. ¿Por qué razones considera que el diseño de un sistema de control interno informatico, es factible sea diseñado por un profesional en contaduría pública? Puede marcar mas de una opción.

Literal	Respuesta	Frecuencia Absoluta	Frecuencia Relativa
a	Porque puede realizar un análisis del entorno económico de la entidad	18	43.90%
b	Por el conocimiento que posee para evaluar los riesgos	27	65.85%
c	Por su experiencia en procedimientos contables.	23	56.10%
d	Por la oportunidad de especializarse en el área de tecnologías de información.	20	48.78%



INTERPRETACIÓN: Al consultarles las razones por las que consideran sería factible que un profesional en contaduría pública, diseñe un sistema de control interno informático, apoyaron en el siguiente orden y frecuencia: un 65.85% piensa que los conocimientos para evaluar riesgos que posee le darían un buen aporte, un 56.10% conviene en que su experiencia en procedimientos contables le ayudaría, un 48.78% considera que la oportunidad para especializarse en el área de tecnologías de información, un 43.90% mantiene que su capacidad para realizar análisis del entorno económico de la entidad sería factible.

ANEXO 2 TABULACIÓN UNIDAD DE ANÁLISIS AGENCIAS DE VIAJES DEL MUNICIPIO DE SAN SALVADOR.

A continuación la interpretación de los resultados del cuestionario efectuado a la muestra de 20 agencias de viaje del municipio de San Salvador, en el departamento de San Salvador.Hubo dos agencias con abstención de opinión, siendo efectivas solo 18 de ellas.

A continuación la interpretación de los resultados del cuestionario:

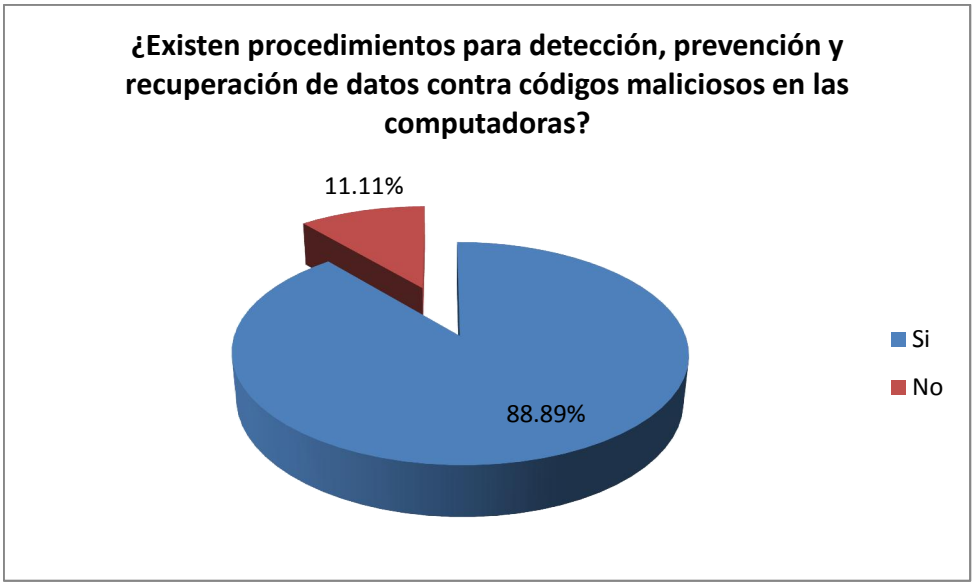
1. ¿De qué manera garantizan que será prestado por el proveedor, las reservaciones gestionadas?, puede marcar más de una opción.

Literal	Respuesta	Frecuencia Absoluta	Frecuencia Relativa
a	Con contrato de garantía con el proveedor.	11	61.11%
b	Compromiso de cumplimiento con el cliente.	3	16.67%
c	Procedimientos de monitoreo y revisión del servicio.	5	27.78%

INTERPRETACIÓN: el 61.11% de los encuestados, manifestaron que para garantizar que los servicios serán prestados por el proveedor, poseen un contrato de garantía, un 27.78% realiza procesos de monitoreo y revisión y el 16.67% restante se asegura únicamente ofreciendo un compromiso de cumplimiento con el cliente

2. ¿Existen procedimientos para detección, prevención y recuperación de datos contra códigos maliciosos en las computadoras?

Literal	Respuesta	Frecuencia	Porcentaje
a	Si	16	88.89%
b	No	2	11.11%
TOTAL		18	100.00%



INTERPRETACIÓN: del 100% de los encuestados, el 88.89% asegura poseer procedimientos para la detección, prevención y recuperación de datos contra códigos maliciosos, mientras que el 11.11% no los poseen.

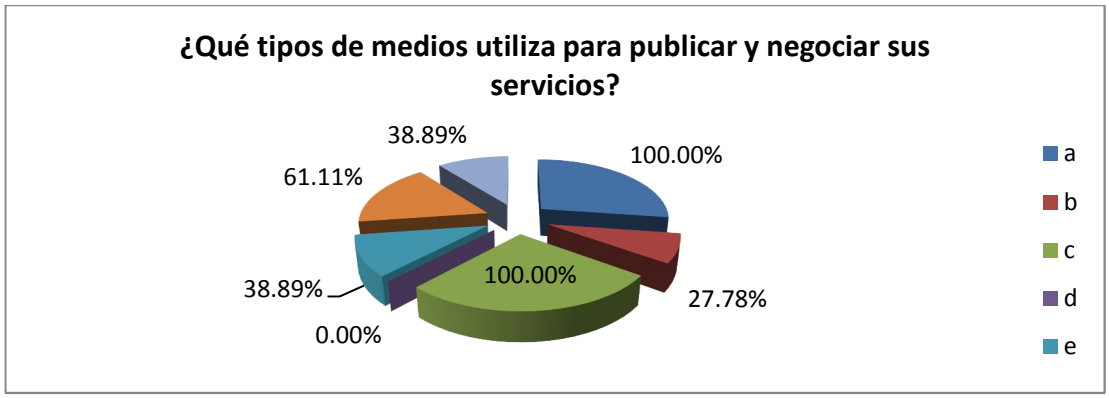
3. ¿Existen políticas y procedimientos para el intercambio de información entre la agencia y partes externas?

Literal	Respuesta	Frecuencia	Porcentaje
a	Si	18	100.00%
b	No	0	0.00%
TOTAL		18	100.00%

INTERPRETACIÓN: el 100% de los encuestados afirma que ha definido procedimientos para realizar intercambio de información entre la agencia y partes externas.

4. ¿Qué tipos de medios utiliza para publicar y negociar sus servicios? Puede marcar más de una opción

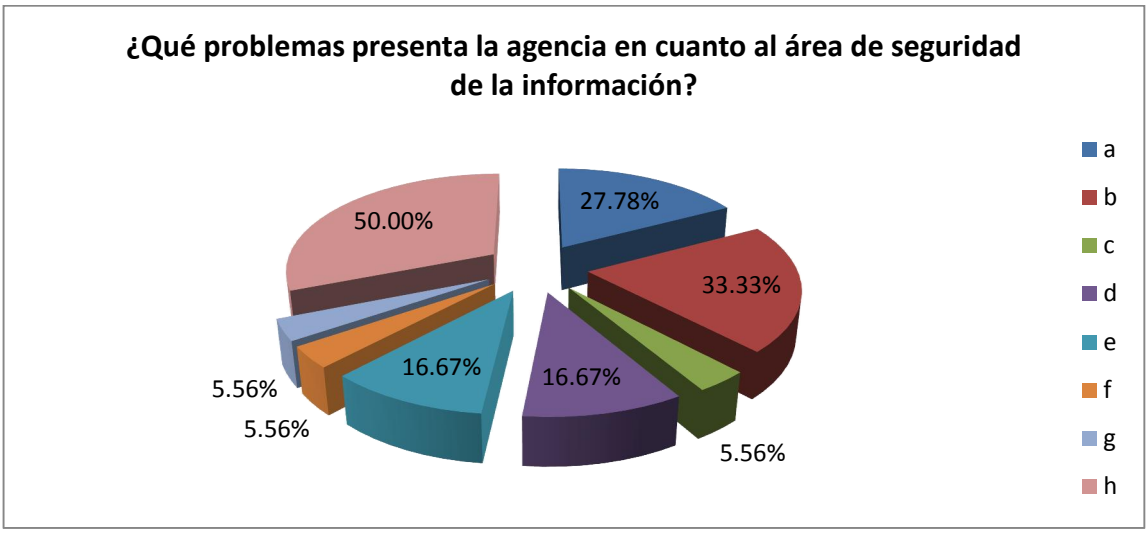
Literal	Respuesta	Frecuencia Absoluta	Frecuencia Relativa
a	Página Web	18	100.00%
b	Aplicaciones para teléfonos inteligentes	5	27.78%
c	Correos electrónicos	18	100.00%
d	Correos postales	0	0.00%
e	Revistas y periódicos	7	38.89%
f	Anuncios de radio y televisión	11	61.11%
g	Vallas publicitarias	7	38.89%



INTERPRETACIÓN: El 100% de los encuestados manifestaron que los medios que utilizan para promocionar sus servicios son el uso de páginas web y correos electrónicos, seguido de los anuncios de radio y televisión con un 61.11%. Esto indica un mayor uso de canales electrónicos para promover sus productos. Cabe recalcar, que las agencias están mostrando interés de usar aplicaciones para teléfonos inteligentes con un 27.78%. Las revistas, periódicos y vallas publicitarias también son usadas en un 38.89% ambas.

5. ¿Qué problemas presenta la agencia en cuanto al área de seguridad de la información? Puede marcar más de una opción.

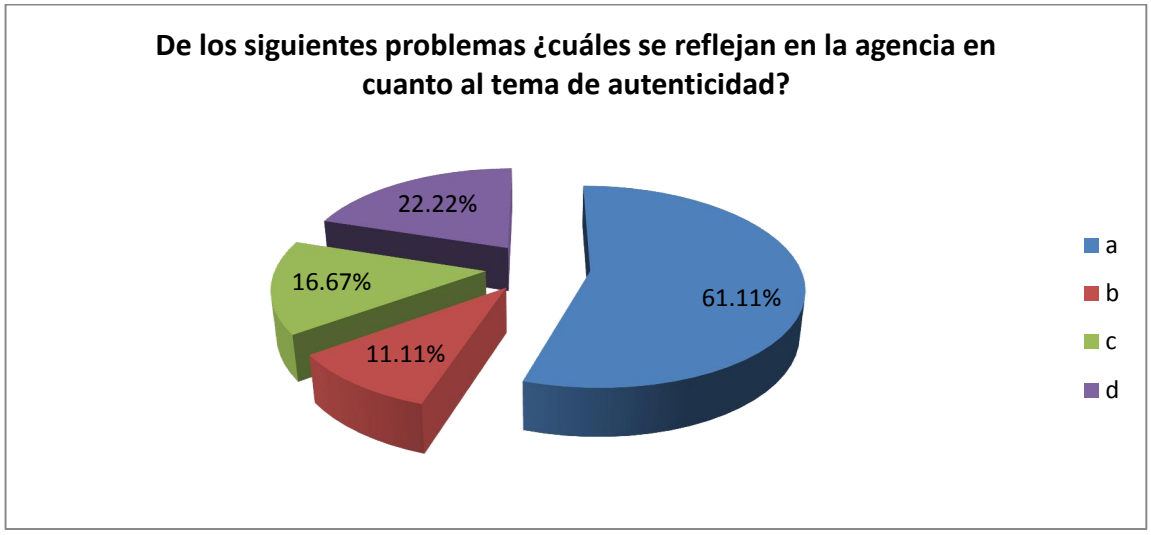
Literal	Respuesta	Frecuencia Absoluta	Frecuencia Relativa
a	Pérdida de datos por interrupción de energía eléctrica	5	27.78%
b	Pérdida de datos por ausencia de respaldos de información	6	33.33%
c	Robo de información por ausencia de métodos de protección de datos	1	5.56%
d	Ausencia de programas de antivirus	3	16.67%
e	Falta de instalaciones adecuadas para el resguardo de la información	3	16.67%
f	Fallas en la configuración de software y dispositivos de seguridad	1	5.56%
g	Aplicación de parches en forma incorrecta o incompleta	1	5.56%
h	Conexión de dispositivos no autorizados a la red corporativa	9	50.00%



INTERPRETACIÓN: los resultados reflejan que los problemas más comunes que sufren en el tema de la seguridad de la información es la conexión de equipos no autorizados a la red corporativa, presentando un 50%, seguidos por la pérdida de datos por ausencia de respaldos de información con un 33.33%, así mismo la perdida de datos por interrupción de energía eléctrica con un 27.78%, la falta de instalaciones adecuadas para el resguardo de la información y la ausencia de programas antivirus con un 16.67% en ambos, el robo de la información, fallas de instalaciones adecuadas y configuración de software en dispositivos, los tres problemas con un 5.56%.

6. De los siguientes problemas ¿cuáles se reflejan en la agencia en cuanto al tema de autenticidad? Puede marcar más de una opción.

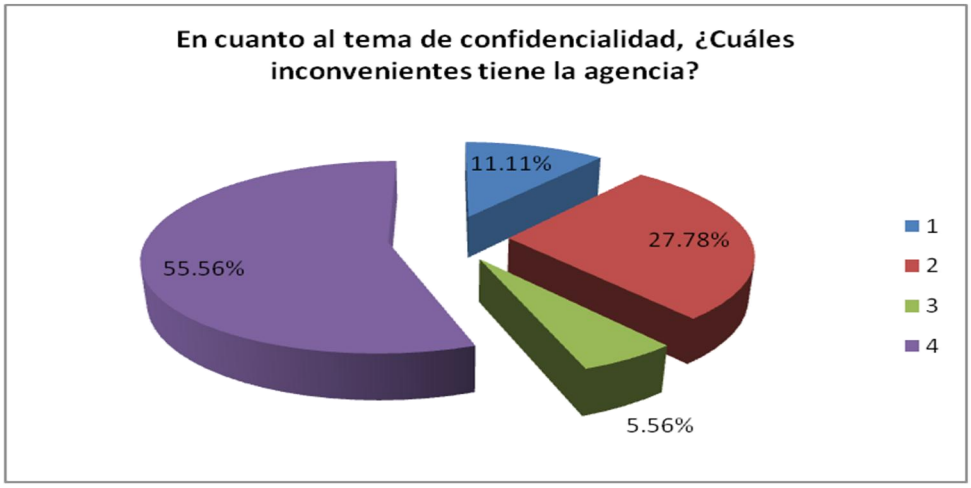
Literal	Respuesta	Frecuencia Absoluta	Frecuencia Relativa
a	Modificación no autorizada de la información	11	61.11%
b	Robo de contraseñas	2	11.11%
c	No puede identificarse el autor ni modificador de reportes y registros	3	16.67%
d	No contestan	4	22.22%



INTERPRETACIÓN: Con respecto al tema de autenticidad de la información, el 61.11% de los encuestados manifiestan que el problema principal es la modificación no autorizada de la información, seguida por la dificultad de identificar el autor de las modificaciones (16.67%). Esto indica una fuerte deficiencia en el tema de autenticidad de información, exponiéndose al riesgo de fraude y hurto de la información.

7. En cuanto al tema de confidencialidad, ¿Cuáles inconvenientes tiene la agencia? Puede marcar más de una opción.

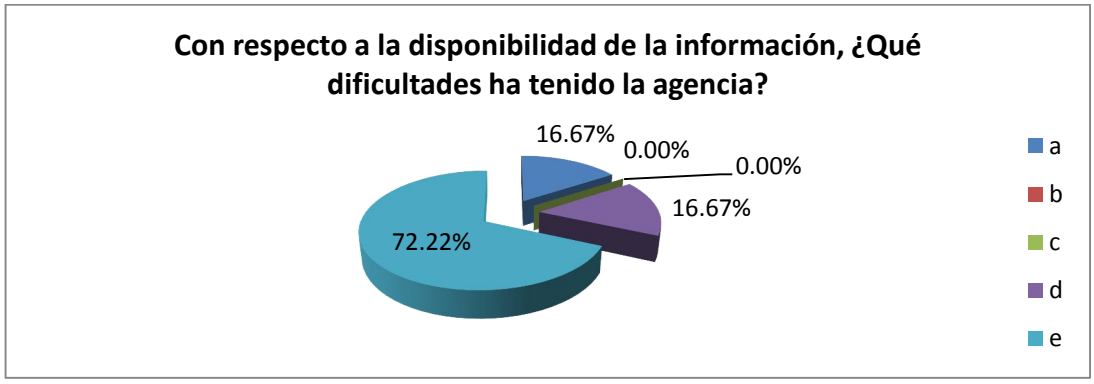
Literal	Respuesta	Frecuencia	Porcentaje
a	Robo de información operativa por partes externas (auditores, asesores informáticos, vigilancia, outsoursing).	2	11.11%
b	Robo de información por publicidad falsa en la web.	5	27.78%
c	Hurto de documentos importantes e información delicada de clientes y proveedores, se encuentran en lugares de fácil acceso para cualquier persona.	1	5.56%
d	No respondió	10	55.56%



INTERPRETACIÓN: 45% de los encuestados expresan que han sufrido inconvenientes en el tema de la confidencialidad, con mayor énfasis en el robo de la información por medio de publicidad falsa en la web, en segundo lugar, por parte de terceros que tienen acceso a la información. El 55.56% restante no emitió opinión alguna sobre la interrogante consultada.

8. Con respecto a la disponibilidad de la información, ¿Qué dificultades ha tenido la agencia? Puede marcar más de una opción.

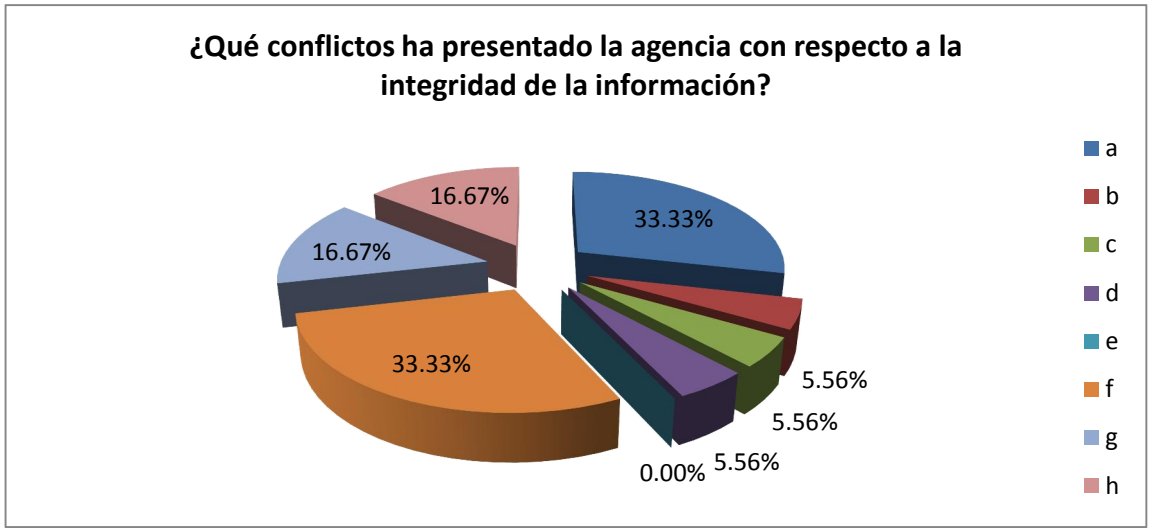
Literal	Respuesta	Frecuencia Absoluta	Frecuencia Relativa
a	No hay acceso inmediato a la información.	3	16.67%
b	El sistema aplicativo no responde con eficacia al generar reportes o procesos.	0	0.00%
c	Los sistemas de cómputo se dañan continuamente, a pesar de recibir mantenimiento adecuado.	0	0.00%
d	El servidor principal de la información no responde oportunamente.	3	16.67%
e	La información no puede accederse de forma remota cuando se requiere.	13	72.22%



INTERPRETACIÓN: para los encuestados, la dificultad que experimentan en cuanto a la disponibilidad de información, es el acceso de forma remota (72.22%), debido a que no se cuentan con los métodos y sistemas adecuados para este tipo de actividad, seguido del uso de servidores principales que no soportan la demanda de los usuarios conectados a la red corporativa con 16.67%.

9. ¿Qué conflictos ha presentado la agencia con respecto a la integridad de la información? Puede marcar más de una opción.

Literal	Respuesta	Frecuencia Absoluta	Frecuencia Relativa
a	Reportes con información distinta a la procesada.	6	33.33%
b	Modificaciones no autorizadas a la información.	1	5.56%
c	Interferencia en los sistemas de control de supervisión y adquisición de datos.	1	5.56%
d	Modificación de los permisos y privilegios de acceso.	1	5.56%
e	Imposibilidad de rastrear el uso de contraseñas privilegiadas cuando es compartido.	0	0.00%
f	Errores del usuario final que afectan los datos de producción.	6	33.33%
g	Modificación no autorizada de sistemas operativos (servidores y redes)	3	16.67%
h	Segregación de funciones inadecuada o no aplicada.	3	16.67%

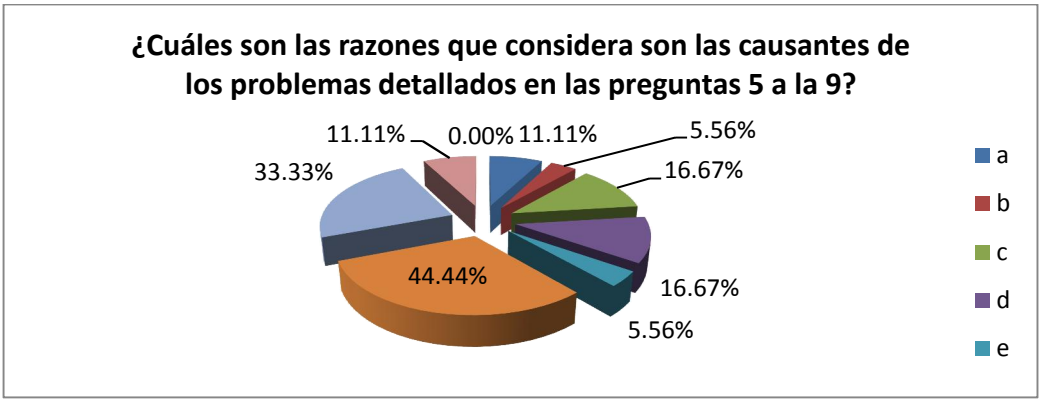


INTERPRETACIÓN: los conflictos más comunes con respecto a la integridad de la información que expresaron los encuestados fueron: los reportes con información distinta a la procesada y los errores del

usuario final, ambas con el 33.33% respectivamente; seguida por la modificación no autorizada de los sistemas operativos y segregación de funciones inadecuada, ambas con el 16.67% inclusive. Los conflictos con mayor representación indican que el factor humano al momento de ingresar la información, puede ser la causante de los errores de visualización de la información que se maneja dentro del sistema.

10. ¿Cuáles son las razones que considera son las causantes de los problemas detallados en las preguntas 5 a la 9? Puede marcar más de una opción.

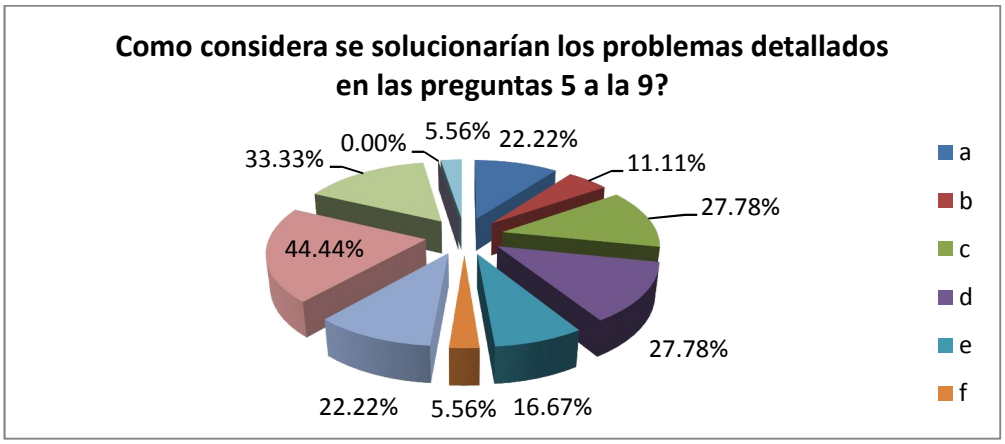
Literal	Respuesta	Frecuencia Absoluta	Frecuencia Relativa
a	Ausencia de compromiso confidencial por parte de proveedores externos.	2	11.11%
b	Ausencia de definición de perfiles de usuarios.	1	5.56%
c	Falta de métodos de protección de datos.	3	16.67%
d	Uso de software malicioso.	3	16.67%
e	Posibles alteraciones a la base de datos que generan reportes inadecuados.	1	5.56%
f	Uso de hardware obsoleto.	8	44.44%
g	Falta de mantenimiento a los equipos utilizados.	6	33.33%
h	La información no es clasificada de acuerdo al grado de confidencialidad.	2	11.11%
i	Los sistemas aplicativos no permiten dejar un rastro o pista de los usuarios.	0	0.00%



INTERPRETACIÓN: para los encuestados, las causantes de los problemas detallados en las preguntas 5 a la 9, consideran que la principal es el uso de hardware obsoleto (44.44%), seguido por la falta de mantenimiento del equipo (33.33%), falta de método de protección de datos y uso de software malicioso ambas opciones con 16.67%, la ausencia de compromiso confidencial por parte de proveedores externos y la que la información no es clasificada de acuerdo al grado de confidencialidad, ambas con 11.11%, posibles alteraciones en la base de datos que generen reportes inadecuados con 5.56%.

11. Como considera se solucionarían los problemas detallados en las preguntas 5 a la 9? Puede marcar más de una opción.

Literal	Respuesta	Frecuencia Absoluta	Frecuencia Relativa
a	Encriptación de datos.	4	22.22%
b	Firma de carta de confidencialidad por parte de proveedores.	2	11.11%
c	Definición de perfiles de usuarios.	5	27.78%
d	Usando programas antivirus y antimalware.	5	27.78%
e	Políticas de restricción de uso de internet.	3	16.67%
f	Restricción en la configuración de reportes.	1	5.56%
g	Restricción en la modificación de la información.	4	22.22%
h	Compra de equipos más recientes.	8	44.44%
i	Actualización de hardware y software para los equipos que aún pueden ser rescatados.	6	33.33%
j	La información debe ser clasificada de acuerdo a su grado de confidencialidad.	0	0.00%
k	Configuración del sistema aplicativo para que deje rastros o pistas de auditoría.	1	5.56%



INTERPRETACIÓN: los encuestados opinan que los problemas detallados previamente en las preguntas 5 al 9, pueden solucionarse mediante la compra de equipos más recientes (44.44%), la actualización del equipo ya existente (33.33%), definición de perfiles de usuarios y uso de programas de antivirus (ambas con el 27.78%), la aplicación de restricciones a la modificación de la información y la encriptación de datos (ambas con 22.22%). Las políticas de restricción de uso de internet con 16.67%, carta de confidencialidad por parte de proveedores con 11.11%, y la restricción de configuración de reportes con 5.56%.

12. ¿Estaría interesado en la elaboración de una guía de control interno que le ayude a minimizar el riesgo informático dentro de la agencia?

Literal	Respuesta	Frecuencia	Porcentaje
a	Si	12	66.67%
b	No	6	33.33%
TOTAL		18	100.00%

INTERPRETACIÓN: Del 100% de los encuestados un 66.67% dice estar interesado en la elaboración de una guía de control interno que les ayude a minimizar los riesgos informáticos, mientras que un 33.33% manifiesta lo contrario.

ANEXO 3 BASE DE DATOS UNIDAD DE ANÁLISIS PROFESIONALES EN CONTADURÍA PÚBLICA DEL MUNICIPIO DE SAN SALVADOR.

Listado firmas de contaduría de acuerdo al Directorio de Empresas de la DIGESTYC del 2011.

NO	MUNICIPIO	NOMBRE COMERCIAL	ACTIVIDAD
1	SAN SALVADOR	A & C QUINTANILLA Y CIA	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
2	SAN SALVADOR	A.M.C. ASOCIADOS, S.A. DE C.V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
3	SAN SALVADOR	ACONSE, S. A. DE C. V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
4	SAN SALVADOR	AFE INTERNACIONAL, S.A. DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
5	SAN SALVADOR	ALAS HERNANDEZ Y ASOCIADOS	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
6	SAN SALVADOR	ALAS LINARES Y ASOCIADOS	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
7	SAN SALVADOR	ALVARENGA BURGOS Y ASOCIADOS	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
8	SAN SALVADOR	AREVALO ALLEN Y ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
9	SAN SALVADOR	ASECONE, S. A DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
10	SAN SALVADOR	ASESORES FINANCIEROS INTEGRALES , S. A. DE C. V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
11	SAN SALVADOR	ASESORIA MERCANTIL , S.A. DE C.V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
12	SAN SALVADOR	AUD. Y CONSULTORES GUEVARA ASOCIADOS, S.A DE C.V	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
13	SAN SALVADOR	AUDICONS CHL , S.A. DE C.V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
14	SAN SALVADOR	AUDITORES Y ASESORES , S.A. DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
15	SAN SALVADOR	AUDITORES Y CONSULTORES DE NEGOCIOS, S.A. DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
16	SAN SALVADOR	AUDITORES, ASESORES, CONSULTORES S.A. DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
17	SAN SALVADOR	BMM & ASOCIADOS, S A DE C. V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
18	SAN SALVADOR	BT CONSULTORES, S. A. DE C. V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
19	SAN SALVADOR	CABRERA MARTINEZ,S.A DE C.V	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
20	SAN SALVADOR	CARRANZA Y CARRANZA Y ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
21	SAN SALVADOR	CASTELLANOS CHACON LIMITADA DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
22	SAN SALVADOR	CASTELLANOS GOMEZ CABRERA Y ASOCIADOS , S.A. DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
23	SAN SALVADOR	CASTRO ARANO & ASOCIADOS	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
24	SAN SALVADOR	CENTRO CONTABLE COMPUTARIZADO, S. A. DE C. V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
25	SAN SALVADOR	CG AUDITORES S.A. DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
26	SAN SALVADOR	CHILE MONROY, ARTEAGA Y ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
27	SAN SALVADOR	CISNEROS CASTRO Y CIA	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
28	SAN SALVADOR	CIUDAD REAL Y ASOCIADOS, S.A. DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
29	SAN SALVADOR	COLOCHO Y ASOCIADOS TECNOLOGIA , S.A. DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
30	SAN SALVADOR	CONSEJERO ROMERO BRIZUELA , S.A. DE C.V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)

31	SAN SALVADOR	CONSULTECNICA,S.A. DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
32	SAN SALVADOR	CONSULTORES PROFESIONALES TRIBUTARIOS, S.A. DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
33	SAN SALVADOR	CONTADORES PUBLICOS, QUINTANILLA & CIA. S.A DE C.V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
34	SAN SALVADOR	CONTADORES PUBLICOS AUDITORES, S.A. DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
35	SAN SALVADOR	CORNEJO & UMAÑA,LTDA DE C.V	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
36	SAN SALVADOR	CORPEÑO Y ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
37	SAN SALVADOR	DAMAS COCAR Y COMPAÑIA	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
38	SAN SALVADOR	DESPACHO ORELLANA MIXCO Y ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
39	SAN SALVADOR	DESPACHO ABREGO ESCALANTE	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
40	SAN SALVADOR	DESPACHO DE AUDITORIA AMAYA PINEDA Y ASOCIADOS	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
41	SAN SALVADOR	DESPACHO DE AUDITORIA Y CONSULTORIA DERAS ORTIZ	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
42	SAN SALVADOR	DURAN PONCE Y CIA.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
43	SAN SALVADOR	ELIAS & ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
44	SAN SALVADOR	ERNST & YOUNG EL SALVADOR, S. A. DE C. V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
45	SAN SALVADOR	ESCOBAR Y ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
46	SAN SALVADOR	FERNANDEZ Y FERNANDEZ ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
47	SAN SALVADOR	FIGUEROA JIMENEZ & CO	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
48	SAN SALVADOR	FIRMA CAÑENGUEZ	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
49	SAN SALVADOR	FREDY´S CHICAS Y COMPAÑIA	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
50	SAN SALVADOR	GARCIA CUELLAR Y ASOCIADOS	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
51	SAN SALVADOR	GONZALEZ BARAHONA ASOCIADOS S.A. DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
52	SAN SALVADOR	GONZALEZ ALAS , S.A. DE C.V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
53	SAN SALVADOR	GRUPO FLORES ASOCIADOS	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
54	SAN SALVADOR	GRUPO INTERNACIONAL DE CONSULTORIA DE EL SALVADOR, S. A. DE C. V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
55	SAN SALVADOR	GRUPO QUINBE, S. A. DE C. V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
56	SAN SALVADOR	GUTIERREZ Y BOJORQUEZ S.A DE C.V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
57	SAN SALVADOR	GVM Y ASOCIADOS ,S.A DE C.V	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
58	SAN SALVADOR	HERNANDEZ AGUIRRE & ASOCIADOS S.A DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
59	SAN SALVADOR	HERNANDEZ MARTINEZ Y ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
60	SAN SALVADOR	HERRERA ALAS Y ASOCIADOS	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
61	SAN SALVADOR	HLB EL SALVADOR, S.A. DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
62	SAN SALVADOR	INVERSIONES NOVA , S. A. DE C. V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
63	SAN SALVADOR	IZAGUIRRE MORENO Y COMPAÑIA	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
64	SAN SALVADOR	JACOBO Y ASOCIADOS ,S.A DE C.V	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)

65	SAN SALVADOR	JEREZ GONZALEZ Y ASOCIADOS	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
66	SAN SALVADOR	JOVEL JOVEL Y COMPAÑIA	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
67	SAN SALVADOR	KPMG SOCIEDAD ANONIMA	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
68	SAN SALVADOR	KPMG PEAT MARWICK.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
69	SAN SALVADOR	L.F. JOVEL Y COMPAÑIA	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
70	SAN SALVADOR	LA CENTINELA , S.A. DE C.V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
71	SAN SALVADOR	LA PONDEROSA , S.A. DE C.V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
72	SAN SALVADOR	LIRA PASASIN Y COMPAÑIA	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
73	SAN SALVADOR	LOPEZ & ASOCIADOS, LTDA DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
74	SAN SALVADOR	LOPEZ CONSULTORES Y ASOCIADOS S. A. DE C. V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
75	SAN SALVADOR	LOPEZ , SOLITO Y ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
76	SAN SALVADOR	LYBNI	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
77	SAN SALVADOR	M Y M AUDITORES, S.A. DE C.V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
78	SAN SALVADOR	MARTINEZ GARCIA Y COMPAÑIA	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
79	SAN SALVADOR	MEJIA ASOCIADOS, S.A DE C.V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
80	SAN SALVADOR	MEJIA NAVARRETER AUDITORES - CONSULTORES, S. A. DE C. V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
81	SAN SALVADOR	MEJIA VALLE Y ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
82	SAN SALVADOR	MENA RODRIGUEZ Y ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
83	SAN SALVADOR	MENDOZA VASQUEZ, S.A. DE C.V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
84	SAN SALVADOR	MGM & ASOCIADOS	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
85	SAN SALVADOR	MORALES PEREZ Y ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
86	SAN SALVADOR	MORALES TEJADA Y ASOCIADOS	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
87	SAN SALVADOR	MORALES Y MORALES ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
88	SAN SALVADOR	MORAN MENDEZ & ASOCIADOS, S.A. DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
89	SAN SALVADOR	MORENO PORTILLO Y ASOCIADOS , S.A. DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
90	SAN SALVADOR	MURCIA & MURCIA Y ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
91	SAN SALVADOR	NAVARRO GUEVARA Y ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
92	SAN SALVADOR	OMC Y ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
93	SAN SALVADOR	OMNI RESOURCES FINANCIAL GROUP ,S.A DE C.V	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
94	SAN SALVADOR	ORTEGA, CISNEROS, DOMINGUEZ Y CIA	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
95	SAN SALVADOR	OSCAR ARMANDO AGUIÑADA Y ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
96	SAN SALVADOR	PACHECO PAREDES AUDITORES CONSULTORES	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
97	SAN SALVADOR	PEREZ PORTILLO Y ASOCIADOS	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
98	SAN SALVADOR	PIMENTEL CARRANZA & ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
99	SAN SALVADOR	PRICEWATERHOUSECOOPERS , S.A. DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)

100	SAN SALVADOR	PROFESSIONAL ACCOUNTANT OFFICE , S. A. DE C. V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
101	SAN SALVADOR	QUIJANO MARTINEZ ASOCIADOS, S.A. DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
102	SAN SALVADOR	R. GALLARDO Y CIA	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
103	SAN SALVADOR	RAMOS Y RAMOS	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
104	SAN SALVADOR	RECINOS, RECINOS Y CIA	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
105	SAN SALVADOR	RIVAS NUÑEZ Y ASOCIADOS	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
106	SAN SALVADOR	RIVERA PALMA ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
107	SAN SALVADOR	RODRIGUEZ CRUZ , S.A. DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
108	SAN SALVADOR	ROJAS MENDEZ	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
109	SAN SALVADOR	ROMERO PORTILLO Y ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
110	SAN SALVADOR	ROQUE Y ROQUE ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
111	SAN SALVADOR	S. Z. CONSULTORES, S.A. DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
112	SAN SALVADOR	SAC SYSTEMS, S. A DE C. V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
113	SAN SALVADOR	SAFE VENTURE, S. A. DE C. V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
114	SAN SALVADOR	SALDAÑA , S.A. DE C.V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
115	SAN SALVADOR	SERCOA S.A DE C.V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
116	SAN SALVADOR	SERVICIOS CONTABLES Y DE CONSULTORIA , S.A. DE C.V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
117	SAN SALVADOR	SERVICONTABLES, S.A. DE C.V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
118	SAN SALVADOR	SND ELECTRONICOS, S.A DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
119	SAN SALVADOR	SOLUCIONES CONTABLES, S. A. DE C. V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
120	SAN SALVADOR	STAF . S.A DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
121	SAN SALVADOR	TANAS, S.A. DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
122	SAN SALVADOR	TMF EL SALVADOR	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
123	SAN SALVADOR	TOBIAS DE JESUS CASTRO LOVO	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
124	SAN SALVADOR	TORRES RIVAS Y ASOCIADOS , S.A. DE C.V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
125	SAN SALVADOR	TURCIOS HENRIQUEZ , S.A. DE C.V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
126	SAN SALVADOR	VALENCIA ELIAS S.A. DE C.V.	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
127	SAN SALVADOR	VALIENTE Y ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
128	SAN SALVADOR	VELASQUEZ GRANADOS Y CIA	ACTIVIDADES DE CONTABILIDAD (DESPACHOS CONTABLES)
129	SAN SALVADOR	VENTURA SOSA, S, A DE C. V.	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
130	SAN SALVADOR	VILANOVA Y ASOCIADOS	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
131	SAN SALVADOR	ZELAYA RIVAS ,S.A DE C.V	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)
132	SAN SALVADOR	ZELAYA RIVAS ASOCIADOS Y COMPAÑIA	AUDITORIA Y CONSULTORÍA (EN CONTABILIDAD)

ANEXO 4 BASE DE DATOS UNIDAD DE ANÁLISIS AGENCIA DE VIAJES DEL MUNICIPIO DE SAN SALVADOR.

Listado de empresas de acuerdo al directorio de empresas de la Dirección General de Estadística y Censos año 2011. Empresas clasificadas en el sector de transporte de personas. Dentro de ellas se encuentran las agencias de viajes, las cuales están resaltadas dentro del cuadro.

No.	DEPARTAMENTO	MUNICIPIO	NOMBRE COMERCIAL
1	SAN SALVADOR	SAN SALVADOR	PROMETUSAL (PROMOCION Y MERCADEO TURISTICO SALVADOREÑO)
2	SAN SALVADOR	SAN SALVADOR	OPENTOURS
3	SAN SALVADOR	SAN SALVADOR	**IZALCO TRAVEL BUREAU**
4	SAN SALVADOR	SAN SALVADOR	EMPRESAS TURISTICAS, S. A. DE C. V.
5	SAN SALVADOR	SAN SALVADOR	**AGENCIA DE VIAJES PREMIER**
6	SAN SALVADOR	SAN SALVADOR	**TRAVEL AND TOURS**
7	SAN SALVADOR	SAN SALVADOR	AGENCIA DE VIAJES ARIEL
8	SAN SALVADOR	SAN SALVADOR	TURIMEDIOS , S. A. DE C. V.
9	SAN SALVADOR	SAN SALVADOR	AMERICA TRAVEL SERVICE, S. A. DE C.V.
10	SAN SALVADOR	SAN SALVADOR	REPRESENTACIONES EXTRANJERAS , S.A. DE C.V.
11	SAN SALVADOR	SAN SALVADOR	**PLANET TOURS, S.A. DE C.V.**
12	SAN SALVADOR	SAN SALVADOR	GLOBAL PASSPORT, S, A DE C. V.
13	SAN SALVADOR	SAN SALVADOR	AGENCIA TRANSMUNDO ,S.A DE C.V
14	SAN SALVADOR	SAN SALVADOR	CADEJO ECO ADVENTURES , S.A. DE C.V.
15	SAN SALVADOR	SAN SALVADOR	**RINSA TOURS**
16	SAN SALVADOR	SAN SALVADOR	CORPORACION VENECIA, S.A. DE C.V.
17	SAN SALVADOR	SAN SALVADOR	AMORTUR
18	SAN SALVADOR	SAN SALVADOR	SUTTER TOURS
19	SAN SALVADOR	SAN SALVADOR	NEGOCIOS Y SERVICIOS LATINOAMERICANOS, S. A. DE C. V.
20	SAN SALVADOR	SAN SALVADOR	**AGENCIA CONTINENTAL DE VIAJES**
21	SAN SALVADOR	SAN SALVADOR	**LINDA TRAVEL AGENCY**
22	SAN SALVADOR	SAN SALVADOR	AMERICAS TOURS S.A DE C.V.
23	SAN SALVADOR	SAN SALVADOR	**AMATE TRAVEL**
24	SAN SALVADOR	SAN SALVADOR	EL JARDIN
25	SAN SALVADOR	SAN SALVADOR	PROMOCIONES TURISTICAS
26	SAN SALVADOR	SAN SALVADOR	SALVADOREAN TOURS, S. A. DE C. V.
27	SAN SALVADOR	SAN SALVADOR	AGENCIA DE VIAJES PANAMERICANA, S. A. DE C. V.
28	SAN SALVADOR	SAN SALVADOR	FLORES RIVERA & ASOCIADOS, LIMITADA DE CAPITAL VARIABLE
29	SAN SALVADOR	MEJICANOS	ROBERT'S TOURS

30	SAN SALVADOR	MEJICANOS	D Y A TOURS
31	SAN SALVADOR	SAN SALVADOR	**VISA TRAVEL, S. A. DE C. V.**
32	SAN SALVADOR	SAN SALVADOR	**ANNA´S TRAVEL SERVICE ,S.A DE C.V**
33	SAN SALVADOR	SAN SALVADOR	**AVITOURS S.A. DE C.V.**
34	SAN SALVADOR	SAN SALVADOR	**U TRAVEL SERVICE, S.A. DE C.V.**
35	SAN SALVADOR	SAN SALVADOR	MARIA DE LOS ANGELES FAGOAGA ARTIGA
36	SAN SALVADOR	SAN SALVADOR	Q C O , INVERSIONES S.A DE C.V.
37	SAN SALVADOR	SAN SALVADOR	AVIA, S.A. DE C.V.
38	SAN SALVADOR	SAN SALVADOR	QUINTANILLA AGUILA, S. A. DE C. V.
39	SAN SALVADOR	SAN SALVADOR	VIAJES INTERNACIONALES PERSONALIZADOS , S.A. DE C.V.
40	SAN SALVADOR	SAN SALVADOR	REPRES. Y PROMOCIONES COMERC., S.A. DE C.V.
41	SAN SALVADOR	SAN SALVADOR	LOPEZ ESCALANTE
42	SAN SALVADOR	SAN SALVADOR	**VIAJES EUROMUNDO ,S.A DE C.V**
43	SAN SALVADOR	SAN SALVADOR	DESARROLLOS TURISTICOS DE ORIENTE , S.A. DE C.V.
44	SAN SALVADOR	SAN SALVADOR	**INTER TOURS, S. A DE C. V.**
45	SAN SALVADOR	SAN SALVADOR	**AEROJET TRAVEL AGENCY, S.A. DE C.V.**
46	SAN SALVADOR	SAN SALVADOR	PROFESIONALES DE VIAJES ,S.A DE C.V
47	SAN SALVADOR	SAN SALVADOR	**AGENCIA DE VIAJES ESCAMILLA, S.A DE C.V.**
48	SAN SALVADOR	SAN SALVADOR	GRUPO CONTACT , S.A. DE C.V.
49	SAN SALVADOR	SAN SALVADOR	**TICKET CITY S.A DE C.V.**
50	SAN SALVADOR	SAN SALVADOR	**OSCAR RENE CHINCHILLA CISNEROS**
51	SAN SALVADOR	SAN SALVADOR	PRO SURF
52	SAN SALVADOR	SAN SALVADOR	MEGA TURISMO
53	SAN SALVADOR	SAN SALVADOR	**UNIVERSAL DE VIAJES , S.A. DE C.V.**
54	SAN SALVADOR	SAN SALVADOR	**AGENCIA DE VIAJES BETTY TOURS , S.A. DE C.V.**
55	SAN SALVADOR	SAN SALVADOR	**LATINO´S TOURS**
56	SAN SALVADOR	SAN SALVADOR	**MUNDIAL DE VIAJES, S.A. DE C.V.**
57	SAN SALVADOR	SAN SALVADOR	**AGENCIA DE VIAJES BERNAL**
58	SAN SALVADOR	SAN SALVADOR	TOUR IN EL SALVADOR
59	SAN SALVADOR	SAN SALVADOR	MUNDITOURS
60	SAN SALVADOR	SAN SALVADOR	PABLITO´S TOURS
61	SAN SALVADOR	SAN SALVADOR	**AGENCIA DE VIAJES SKY TRAVEL**
62	SAN SALVADOR	SAN SALVADOR	CORPORACION COSTERA S.A DE C.V.
63	SAN SALVADOR	SAN SALVADOR	CORPORACION PARAISO S.A DE C.V.
64	SAN SALVADOR	SAN SALVADOR	INTERNATIONAL TOUR AND RESORTS, S.A. DE C.V.
65	SAN SALVADOR	SAN SALVADOR	EL FLOR, S. A DE C. V.
66	SAN SALVADOR	SAN SALVADOR	**BLAU TRAVEL AGENCY, LINEA AZUL**

67	SAN SALVADOR	MEJICANOS	ATLAS TOURS EL SALVADOR
68	SAN SALVADOR	SAN SALVADOR	THRIVE, S, A DE C. V
69	SAN SALVADOR	SAN SALVADOR	PROTURE S.A DE C.V.
70	SAN SALVADOR	SAN SALVADOR	**DOS AMIGOS, S.A. DE C.V.**
71	SAN SALVADOR	SAN SALVADOR	DISCOVER EL SALVADOR , S.A. DE C.V.
72	SAN SALVADOR	SAN SALVADOR	INTERVAC
73	SAN SALVADOR	SAN SALVADOR	LI NIBANI, S. A. DE C. V.
74	SAN SALVADOR	SAN SALVADOR	MAYA, S.A. DE C.V.
75	SAN SALVADOR	SAN SALVADOR	**SERVI VIAJES, S.A DE C.V.**
76	SAN SALVADOR	SAN SALVADOR	**AVILES TRAVEL**
77	SAN SALVADOR	SAN SALVADOR	REPRESENTACIONES Y SERVICIOS LA CEIBA, S. A. DE C. V.
78	SAN SALVADOR	SAN SALVADOR	LYLLI'S SERVICES TRAVEL TOUR & MARKETING S.A. DE C.V.
79	SAN SALVADOR	SAN SALVADOR	**PANAMEX TRAVEL**
80	SAN SALVADOR	SAN SALVADOR	ZION AGENCIA Y SOLUCIONES DE VIAJES
81	SAN SALVADOR	MEJICANOS	HISPANOAMERICA TRAVEL, S.A. DE C.V.
82	SAN SALVADOR	SAN SALVADOR	SERVICIOS MULTIPLES Y PRODUCTOS
83	SAN SALVADOR	SAN SALVADOR	**SOPHIA TOURS , S.A. DE C.V**.
84	SAN SALVADOR	SAN SALVADOR	HISPANA DE VIAJES, S. A. DE C. V.
85	SAN SALVADOR	SAN SALVADOR	TRAVELONE SERVICES AND TOURS EL SALVADOR, S.A. DE
86	SAN SALVADOR	SAN SALVADOR	**AGENCIA DE VIAJES TURINTER**
87	SAN SALVADOR	SAN SALVADOR	OPERACIONES TURISTICAS INTERNACIONALES ,S.A DE C.V.
88	SAN SALVADOR	SAN SALVADOR	MY TRIP,S.A. DE C.V.
89	SAN SALVADOR	SAN SALVADOR	**COSMOS TRAVEL AGENCY**
90	SAN SALVADOR	SAN SALVADOR	BRISAS DEL GOLFO S.A DE C.V
91	SAN SALVADOR	SAN SALVADOR	**CTV, S.A. DE C.V.**
92	SAN SALVADOR	SAN SALVADOR	TRAVEL ONE INTERNATIONAL NETWORE EL SALVADOR , S.A. DE C.V.
93	SAN SALVADOR	SAN SALVADOR	**ALL AMERICAN TRAVEL**
94	SAN SALVADOR	SAN SALVADOR	**TRAVEL MALL**
95	SAN SALVADOR	SAN SALVADOR	OTEC TURISMO JOVEN, S. A. DE C. V.
96	SAN SALVADOR	SAN SALVADOR	EVA TOURS, S. A DE C. V.
97	SAN SALVADOR	SAN SALVADOR	**PASEO TRAVEL AGENCY**
98	SAN SALVADOR	SAN SALVADOR	IBERIA LINEAS AEREAS DE ESPAÑA , S.A.
99	SAN SALVADOR	SAN SALVADOR	VACACIONES CENTROAMERICANAS, S. A. DE C. V.