UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

"MODELO DE SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA PROFESIONALES DE LA CONTADURÍA PÚBLICA QUE EJERCEN LA AUDITORÍA EXTERNA EN EL SALVADOR"

Trabajo de Investigación presentado por:

HENRÍQUEZ DE GUZMÁN, LAURA DEL CARMEN

HERRERA RIVERA, GUADALUPE YAMILETH

LEMUS CAMPOS, FLOR DE MARÍA

Para optar al grado de

LICENCIATURA EN CONTADURÍA PÚBLICA

SEPTIEMBRE 2016

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

AUTORIDADES UNIVERSITARIAS

Rector	:	Lic. José Luis Argueta Antillón
Secretaria	:	Dra. Ana Leticia Zavaleta de Amaya
Decano de la Facultad de Ciencias Económicas	:	Lic. Nixón Rogelio Hernández Vásquez
Secretario de la Facultad de Ciencias Económicas	:	Licda. Vilma Marisol Mejía Trujillo
Directora de la Escuela de Contaduría Pública	:	Licda. María Margarita de Jesús Martínez Mendoza de Hernández
Coordinador general de Procesos de graduación Facultad De ciencias económicas	:	Lic. Mauricio Ernesto Magaña Martínez
Coordinador de Seminario	:	Licenciado Daniel Nehemías Reyes López
Docente Director	:	Licda. María Elena Vidal de Serpas
Jurado Examinador	:	Lic. Henry Amílcar Marroquín
	:	Lic. Daniel Nehemías Reyes López
	:	Licda. María Elena Vidal de Serpas

SEPTIEMBRE DE 2016

San Salvador, El Salvador, Centro América

Agradecimientos

Agradezco primeramente a Dios que me dio vida y me ha permitido llegar hasta acá; a mis padres que me han dado la mejor de las herencias, mi estudio y mi carrera; a mis hermana Iris y Evelyn Henríquez, que siempre me han apoyado y ayudado en todo momento; gracias a mi esposo por toda la paciencia, ayuda y ánimos que me ha dado durante este proceso; a mi Jacob por acompañarme en las noches de desvelo y finalmente pero no menos importante a mis compañeras Florcita y Lupis, gracias por todo chicas.

Laura del Carmen Henríquez de Guzmán

Agradezco a Dios principalmente por ser mi guía y mi fortaleza, seguido a mi madre y a mi hermana por apoyarme incondicionalmente y comprenderme en todos los aspectos, a mi padre por apoyarme y encaminarme a mi carrera, a Marbely Álvarez por acompañarme en todos mis altos y bajos, a mi paiqui por hacerme reír en el momento más oportuno, a Graciela por creer en mí y a toda mi familia en general por apoyarme sin límites, y a mis compañeras Lau y Florcita por no pelearnos en ningún momento y no perder las esperanzas. Con todo mi corazón, gracias a todos.

Guadalupe Yamileth Herrera Rivera

A Dios Todopoderoso, por haberme dado siempre la sabiduría y fuerzas necesarias en toda la realización de mi carrera. a mi madre, por haberme forjado en el buen camino, por sus sacrificios y apoyo incondicional en mi formación profesional, a mi padre y hermanas por animarme en seguir adelante y por supuesto a mis compañeras Laura y Lupita por ser pacientes, comprensivas y tolerantes, muchas gracias por todo.

Flor de María Lemus Campos

ÍNDICE

PÁGINA Nº

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN EJECUTIVO

En vista de la problemática de la seguridad de la información que enfrentan las firmas de auditoría, estas se ven en la necesidad de buscar las herramientas necesarias para implementar un sistema que garantice el resguardo de los datos proporcionados por el cliente, y así poder prestar un mejor servicio a las empresas auditadas, que confiarán más en los integrantes del encargo.

En tal sentido el objetivo final fue crear un "modelo de sistema de gestión de seguridad de la información para profesionales de la contaduría pública que ejercen la auditoría externa en El Salvador" para que como propósito principal sea mantener e impulsar la eficacia y la eficiencia de la disponibilidad, integridad y confidencialidad de la información de terceros, y de la misma entidad como tal.

Por consiguiente, para la adopción de este término innovador e internacional, la gerencia de cada compañía de profesionales de contaduría pública deberá cumplir con normas de protocolo donde avalen el compromiso de adquirir el modelo antes mencionado, y dar paso a la verificación y modificación de algunos datos y documentos importantes que puedan impulsar de forma más ágil la implementación de este proyecto.

El sistema garantiza ventajas muy identificadas como la reducción de costos, la mejor táctica para la atracción de clientes altamente competentes, así mismo se motiva a los colaboradores de la firma para el desarrollo de cada encargo que adquieren, entre otros beneficios notables que impulsen a visiones de estrategias empresariales.

Por lo cual para el desarrollo de la investigación se utilizó la encuesta y sistematización bibliográfica como herramientas para obtener un diagnóstico certero de la problemática. Los resultados obtenidos con las encuestas demostraron que las firmas de auditoría no poseen controles adecuados para almacenar y resguardar la información, por lo que resulta un compromiso y una responsabilidad hacia con los clientes y con la rentabilidad de sus servicios.

Muchos de ellos consideran que la inversión tecnológica y la protección de estos, crean un costo elevado y dejan de buscar recursos para informarse más sobre el tema y como resultado de esto se busca ayudar a tener acceso a este tipo de herramientas que colaboren y ayuden a cumplir con el propósito individual de cada firma.

En esta propuesta, las entidades podrán adherirse abiertamente por ser basada en un estándar internacional, con una serie de formularios y pasos con sus respectivas fases para que puedan implementar controles de seguridad para la información y los activos relacionados directa o indirectamente a ella.

En consecuencia de lo antes expuesto, se pretende de forma figurativa, mostrar la incidencia y la relevancia a través de un caso hipotético que selecciona y cubre los aspectos generales para efectos de mayor comprensión y visualización de la conveniencia de este elemento, garantizando la confidencialidad, integridad y disponibilidad de la información.

INTRODUCCIÓN

El período de innovación tecnológica en el cual actualmente se vive está lleno de retos y oportunidades, diferentes intereses, además, puntualmente de profesionales en contaduría buscando el alcance de una solución que beneficie a todos para crear valor agregado a los servicios que ofrecen.

Producto de la necesidad de proteger la información, en el siguiente documento se presenta una propuesta de Sistema de Gestión que tiene por objetivo garantizar el adecuado manejo de la misma bajo estrictas medidas de seguridad.

En el primer capítulo se mencionan- las generalidades de las firmas de auditoría, todo lo relacionado a las funciones y manipulación de datos por la misma, además de la seguridad de la información, la importancia y ventajas de protegerla de manera eficiente y eficaz. También sobre la normativa técnica y legal en la que se apoyan los profesionales para aplicarla en el proceso de los encargos.

En el segundo capítulo se describe la metodología empleada para ejecutar la investigación, detallando el tipo de estudio realizado, la forma como se determinó la muestra, las unidades objeto de análisis, las técnicas e instrumentos utilizados y el diagnóstico de los datos recolectados en la investigación de campo; en el cual se muestra mediante cuadros de resumen, la información y análisis de los resultados obtenidos en torno a la problemática en estudio.

En el tercer capítulo se desarrolla la propuesta, el modelo de sistema de gestión de la seguridad de la información el cuál se puede implementar en cualquier firma de auditoría en base a la ISO 27001 y 27003. Finalmente se presenta la bibliografía que fue utilizada en el desarrollo de la investigación.

CAPÍTULO I: MARCO TEÓRICO, TÉCNICO Y LEGAL.

1.1. Antecedentes de la seguridad de la información

A lo largo de la historia han existido grandes compañías que se dedican al negocio de fabricar y comercializar diferentes productos y servicios, lo que creaba la necesidad de controlar y mejorar los movimientos económicos de dichas empresas a través de profesionales de contaduría pública que lleven la contabilidad y a la vez se auditara la información procesada y así mismo poder garantizar la seguridad de la información confidencial; en consecuencia de ello, existía demanda de estos servicios profesionales pero eran escasos los que tenían conocimientos y estaban certificados en ello, por lo cual fue necesario solicitar servicios provenientes de Europa, donde ya habían logrado la tecnología y desarrollo técnico que se necesitaba.

"En 1929 se solicitó los servicios de una firma de auditoría de ingleses conocida como *Layton Bennett Chiene & tait* para que auditaran la contabilidad pública en el país, los cuales se dedicaron a realizar ésta profesión como auditores independientes sin restricciones ya que no existía ninguna norma legal que regulara las actividades de las mismas." (Monge, 2006)

Posteriormente se constituye la corporación de contadores públicos, se establecen requisitos de certificación para esta actividad y servicios relacionados.

Por consiguiente debido a la necesidad de asegurar la información surgió la exigencia de no solo ejercer la auditoría, sino de conformar organizaciones denominadas firmas de auditoría que proporcionan estos servicios que por defecto se necesitan en los negocios, el prestigio de estas firmas se genera e incrementa en la medida que proporciona a sus clientes la seguridad de los archivos o información sujeta a examen.

La seguridad o resguardo de la información se convierte en un tema de interés para la empresa auditada, ya que en cierta manera la competencia y otros interesados pretenden obtener provecho de la vulnerabilidad de la protección de la misma.

Inicialmente la información proporcionada a las firmas de auditoría por parte de sus clientes se organizaba en archivos físicos usando la tecnología del momento que muchas veces se limitaba al uso de máquinas de escribir. Posteriormente con el uso de la computadora, la información es generada y almacenada en dispositivos ya de forma digital.

La integridad y disponibilidad de la información se pone en riesgo por muchos factores tales como el no generar respaldos de los archivos recolectados de terceros y de su propia compañía y la manipulación incorrecta de la misma. Actualmente con el uso más avanzado de la tecnología, estos factores se mejoraron aunque siempre existe algún tipo de vulnerabilidad que puede afectar el desarrollo eficiente y eficaz de las actividades que realizan las firmas de auditoría. En este sentido puede afirmarse que la información no es sólo una vía para llegar al conocimiento sino que además, éstas conducen directamente a la toma de decisiones oportunas que se traducen en ventaja competitiva para las organizaciones representadas en tal sentido.

Con el avance de la ciencia en la tecnología de la información, así aparecen medios y formas más prácticas de tratar la información tales como: correo, por medio de textos, videos, mensajes multimedia, en los que garantizar la integridad, la disponibilidad y la confidencialidad de la información de los clientes que confían el activo principal de sus compañías, se vuelve un aspecto al que las firmas deben prestar mucha atención.

Con el paso de los años han aparecido dispositivos y redes de comunicación que hacen mucho más fácil el trabajo de los auditores, por ejemplo los *switch, rauter*, modem, entre otros

servidores que les permiten interconectar varios ordenadores y de ésta forma mantener disponible la información, además el internet permite mantenerse en comunicación no importando la distancia aparte del intercambio de información que viene a facilitar un poco el trabajo de los profesionales, aunque si bien es cierto el desarrollo de las nuevas tecnologías ha dado un giro radical a la forma de comunicación, a la vez ha aumentado los riesgos para las empresas ya que se exponen a nuevas amenazas.

La seguridad forma parte de la creatividad que los expertos deben implementar en sus organizaciones y aunque el avance tecnológico fluye rápidamente, así mismo los profesionales deben ponerse a la vanguardia de la actualidad y suplir las necesidades para la protección y cumplimiento de discreción profesional de los servicios de auditoría, inspirado en los estándares internacionales que innova éste tipo de mejora con el objetivo de incrementar la cartera de clientes que se puedan auditar.

A raíz de esto surge la implementación de la seguridad de la información porque ha crecido y evolucionado considerablemente en los últimos años, convirtiéndose en algo indispensable en cada empresa, ya que busca establecer y mantener programas, controles y políticas que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información.

1.2 Generalidades de las firmas de auditorías jurídicas y naturales

Las firmas de auditoría autorizadas por el Consejo de Vigilancia de la Profesión de la Contaduría Pública y Auditoría (CVPCPA) que son entidades que brindan servicios de auditoría financiera externa, auditorías especiales, consultorías, y otros servicios relacionados, poseen las siguientes características:

- Son firmas que pueden ser constituidas por una persona natural que sea capaz de responsabilizarse a cumplir las disposiciones legales y que la misma profesión exige, tal como lo menciona el Código de Comercio en el Art. 7; además podrán conformarse por dos o más socios y adoptar la figura de persona jurídica según el Art. 73 de la misma ley; así mismo se encuentra establecido los artículos del 1 al 4 de la ley Reguladora del Ejercicio de la Contaduría Pública y Auditoría donde menciona requisitos que deben cumplir los profesionales para ejercer la contaduría pública y la auditoría externa.
- Desarrollan su trabajo de una manera independiente, la imparcialidad con la que emite su opinión debe ser en base a su juicio profesional.
- Por lo menos una persona debe estar autorizada para ejercer la contaduría pública como persona natural.
- Pueden ejercer su trabajo dentro y fuera de la firma para evidenciar la información proporcionada por el cliente.

La auditoría externa es una función pública, que tiene por objeto autorizar a los comerciantes y demás personas que por ley deben llevar contabilidad formal, un adecuado y conveniente sistema contable de acuerdo a sus negocios y demás actos relacionados con el mismo, así lo establece la ley reguladora del ejercicio de la contaduría de la profesión de la contaduría pública y auditoría. (Acosta F.C., 2009)

Los profesionales de la contaduría pública que ejercen la auditoría externa son responsables de la información de sus clientes, siendo éste el activo más importante, ya que en el transcurso del encargo tendrán que almacenar datos de los cuáles depende el éxito de la auditoría.

Los responsables del encargo, suelen estar integrados por: gerente o encargado de auditoría, supervisor, asistente senior, asistente junior, entre otras categorías; es de gran relevancia poder determinar las obligaciones y funciones de cada participante en esta diligencia que requiere escepticismo profesional y así poder determinar al responsable que recibe, manipula y entrega la información y la labor realizada, para ello deben tener los procedimientos adecuados que mencionen las medidas de control para el uso de sistemas, software e inclusive instalaciones en general que tengan relación directa o indirecta con los datos o archivos de terceros.

1.2.1. Administración de la información relativa a la comunicación con el cliente

El auditor inicialmente deberá considerar aspectos importantes que le ayuden a tomar la decisión de adquirir la responsabilidad de auditar la empresa, para ello puede investigar si la entidad se encuentra libre de sospechas de fraude, si está legalizada de acuerdo a las disposiciones legales vigentes, y entonces basado en sus propios criterios podrá aceptar o rechazar el encargo. Por consiguiente ante la afirmación del compromiso de cumplir el rol de auditor externo podrá emitir una oferta que el cliente tomara en acuerdo o desacuerdo para dar el siguiente paso a la administrar de la información de los estados financieros de la entidad para que con el mismo objeto de escepticismo profesional pueda emitir una opinión razonable sobre ellos, cabe agregar que se maneja información de vital relevancia que pueden comprometer a los responsables de las entidades auditadas.

En consecuencia de lo anterior, la opinión del auditor deberá ser basada en la evidencia recolectada por la información proporcionada por los responsables de la entidad, que fueron comprometidos previamente para permitir el acceso ilimitado a ella, por lo que se deberán

manifestar las peticiones por escrito, para recolectar, resguardar y manipular información confidencial.

Así mismo, el auditor solicita a los superiores de la entidad, a que revelen mediante una carta sobre los cumplimientos que realizaron de acuerdo a las disposiciones legales, que se encuentran vigentes y que realizaron la entrega de la información confidencial antes mencionada y junto con estas la descripción de las responsabilidades que tiene la empresa con el auditor y sus subordinados ante la tarea, seguido por las fechas sobre la entrega de informe final y así poder esclarecer términos y evitar retrasos o eventos que provoquen desacuerdos o interpretaciones erróneas y conflictivas. La NIA 580 revela las posibles circunstancias que un auditor puede considerar para mantener la comunicación con su cliente y el intercambio de información con el objeto de prevalecer la seguridad de la misma y que el prestigio de la firma sea mantenido mediante la aplicación de un sistema de gestión de seguridad de la información

1.2.2. Administración de la información relativa al servicio proporcionado

El proceso de auditoría debe poseer políticas de control para recibir, almacenar, manipular, distribuir, respaldar o registrar la información de sus clientes. Los procedimientos pueden realizarse antes, durante o después del encargo. Las firmas tendrán la facultad de definir como serán sus técnicas de recolección de evidencia adecuada y suficiente de los clientes a los cuales se les realizará la auditoría. Cada entidad tiene diversidad de actividades económicas y a través del constante movimiento que las empresas desarrollan incrementan las auditorías que se diversifican en diferentes tipos de encargo:

Las firmas de auditoría en general comúnmente ejercen de acuerdo a lugar de aplicación (Ver tabla Nº1), ya que estas tienen la característica de verificar controles detallados de un sistema de

información que involucra activos tecnológicos, elementos del recurso humano, aspectos internos y externos que influyen en la toma de decisiones financieras y económicas en la gerencia, entre otras.

Tabla Nº1 Tipos de auditoría

Por área de aplicación	Por áreas especificas	Según lugar de aplicación
- Financieras - Administrativas - operacionales - Integral - Gubernamental - De sistemas	- Fiscal - Laboral - Ambiental - De proyectos de inversión - De sistemas	- Externa - Interna

Fuente: elaboración propia

Existen diferentes tipos de encargos, pero los que más interesan para este tipo de estudio son los relacionados con la auditoría interna y externa.

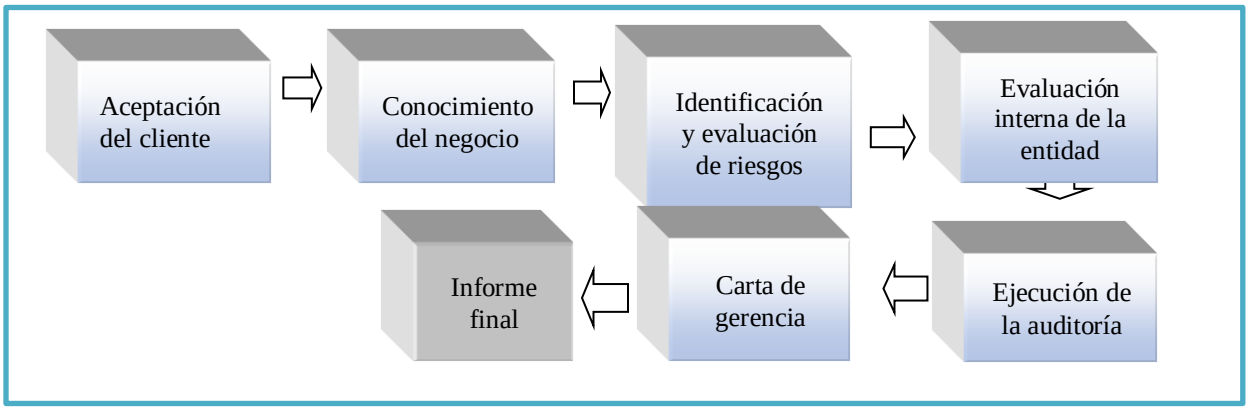
a) Auditoría interna: es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. (Interna, 2009)
b) Auditoría externa: es hacer posible que el auditor exprese una opinión sobre si los estados financieros están preparados, respecto de todo lo sustancial, de acuerdo con un marco de referencias para informes financieros identificados. (IASB (International Accounting Standars Board), 2009)

La independencia que un auditor externo ofrece, se considera como la fe pública para la emisión de una opinión certera sobre los procedimientos de la entidad ya que puede prestar este servicio hacia diferentes áreas, con la peculiar característica de que el profesional no posee ninguna tipo de relación de amistad o parentesco con el personal de trabajo de la entidad; pero como tal, existe una gran responsabilidad por estas personas naturales o jurídicas ya que el

análisis sobre los controles de los clientes auditados requiere una experiencia considerable para la emisión de sus criterios y a la vez el resguardo de la información.

El primer procedimiento de la auditoría externa es la aceptación o no del cliente, en caso de aceptar, se procede al conocimiento de la empresa lo cual implica obtener la información general de la entidad, se puede adquirir por medio de la escritura de constitución y otros documentos que ayuden a conocer más sobre el negocio, luego se hace una evaluación e identificación de riesgos, conocer las vulnerabilidades de la empresa, teniendo toda la documentación adecuada y suficiente se puede iniciar la auditoría después de obtener la carta de gerencia y por último se entrega el informe final. (Ver Figura Nº1)

Figura Nº1 Esquema de los procedimientos de la auditoría externa



Fuente: Elaboración propia

En el transcurso de la ejecución de la auditoría el equipo del encargo tendrá que documentar toda la información en tres tipos de archivos: permanente, corriente y administrativo que sirven como evidencia para el encargo a realizar. (Ver Figura Nº2)

El conocimiento oportuno de estos documentos y archivos legales permite a los auditores interpretar los hechos relacionados en toda la auditoría y asegurarse que se manifiesten de forma adecuada en los estados financieros.

Figura Nº2 Clasificación de papeles de trabajo

Fuente: NIA 230 Documentación de auditoría

Tipos de archivo de auditoría

A. Archivo corriente: este se forma con los papeles, datos y correspondencia relativos a la auditoría que se ejecuta, los cuales son:

- Información referente a la estructura organizacional de la entidad.
- Extractos o copias de documentos legales importantes.
- Información concerniente al giro de la empresa.
- Análisis de transacciones y balances.
- Detalles de procedimientos concernientes a otras auditorías.
- Cartas recibidas de la entidad.

B. Archivo administrativo: incluye la recopilación que sirve de base para realizar las pruebas que se utilizan como fuente. Contiene información relacionada con la administración del trabajo de auditoría y está limitado sólo al período sujeto a revisión, los cuales son:

    - Evidencia de que el trabajo desempeñado por los auxiliares fue supervisado y revisado.
    - Plan de auditoría y presupuesto.
    - Detalle del personal asignado.
    - Resumen del tiempo asignado.
    - Limitaciones del alcance.

C. Archivo permanente: se forma con los papeles transferidos del archivo corriente, una vez finalizado el examen; es decir, contiene la información que el auditor considera será utilizada en un periodo mayor a un año, solo debe contener información básica como:

    - Evidencia del proceso de planeación incluyendo programas de auditoría y cualquier cambio al respecto.
    - Evidencia de la comprensión del auditor de los sistemas de contabilidad.
    - Evidencia de evaluaciones de los riesgos inherentes, de control y cualquier revisión al respecto.

Riesgos y vulnerabilidades de la información

La protección de archivos implica ciertos mecanismos que pueden proteger los sistemas que almacenan la información así como todas las pruebas recolectadas en físico, asegurándose que la integridad sea la prioridad de los archivos. Los problemas que se pueden presentar son:

- Acceso físico: la vulnerabilidad de la información puede depender en gran medida a la conciencia del manejo de la misma por parte de los empleados de la firma de auditoría, es por ello que es preciso controlar los usuarios que acceden para prevenir y detectar fallas o accesos no autorizados al sistema. Para detectar estos accesos no deseados se pueden emplear medidas técnicas como cámaras de vigilancia de circuito cerrado o alarmas, así como el paso a salas específicas a los equipos tecnológicos, entre otras medidas.

- Desastres naturales: estos pueden provocar graves consecuencias si no se contemplan políticas y medidas de seguridad que puedan prever estos posibles desastres, así como los terremotos, tormentas eléctricas, inundaciones, incendios, humos y humedad.

- Alteraciones del entorno: son factores del entorno de trabajo que en cierta medida se debe intentar controlar como por ejemplo la alimentación eléctrica de las maquinas, el ruido, cambios bruscos de temperatura, entre otros.

La firma tiene que estar preparada en caso que surja un imprevisto y se pierda información, tomando medidas de precaución como tener copias de seguridad en otros lugares ya que el impacto sería grande, puede ocasionar pérdida de clientes y los costos serian elevados para poder recuperarlos, pero lo más importante que la firma perdería la credibilidad.

Las firmas de auditoría deben implementar planes de recuperación ya que los sistemas de seguridad están inspirados para evitar fallos por un bloqueo inesperado, archivos borrados, infección por virus, entre otras circunstancias que implican la protección de documentos físicos y digitales.

Los profesionales de contaduría pública deben evitar posibles daños y pérdidas que afecten los papeles de trabajo y documentación relacionada y para ello pueden utilizar cualquiera de los siguientes respaldos:

- Completos: los datos escritos que nunca se modifican podrán obtener una réplica exacta del mismo.
- Incrementales: a diferencia de los anteriores, estos en primera secuencia revisan la fecha de modificación o creación del archivo más reciente al último respaldo y si no existe dicha copia significa que el archivo no se ha modificado y se puede obviar el proceso.
- Diferenciales: son similares a los anteriores ya que realizan réplicas de documentos que han sido alterados, la particularidad es que estos son acumulativos.

1.3 Importancia y clasificación de la seguridad de la información en las firmas de auditoría

1.3.1. Importancia de la seguridad de la información

La seguridad de la información según ISO 27001 es la preservación de la confidencialidad, integridad y disponibilidad de la información, lo que implica que se deben poner en práctica un conjunto de medidas preventivas y reactivas que permitan resguardar los datos.

Los sistemas de seguridad de la información son necesarios para todo tipo de empresa, sobre todo para las firmas de auditoría que manejan información ajena, por lo tanto necesitan tener políticas para protegerla, ya que como se menciona en el documento los datos deben permanecer íntegros y disponibles en cualquier momento.

Por tanto un sistema de gestión de seguridad de la información en la firma de auditoría brindaría un control más efectivo sobre la administración de la información. El sistema de

gestión de seguridad debe contener los procedimientos adecuados e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

1.3.2. Clasificación de la seguridad de la información

- Seguridad física

Habitualmente las firmas de auditoría se concentran en proteger la información de los virus, hackers y se olvidan de proteger la documentación física, de eso trata la seguridad física, de implementar medidas de protección para los equipos y otros activos tangibles como los papeles de trabajo que también forman parte del activo de la información.

La seguridad física es aquella que trata de proteger el hardware de los posibles desastres naturales de incendios, inundaciones, sobrecargas eléctricas, de robos y un sinfín de amenazas más. Las firmas de auditoría tienen que implementar medidas de defensa para proteger la información.

- Seguridad lógica

La seguridad lógica complementa a la seguridad física, protegiendo el software de los equipos informáticos, es decir, las aplicaciones y los datos de usuario, de robos, de pérdida de datos, entrada de virus informáticos, modificaciones no autorizadas de los datos, ataques desde la red, entre otros.

La seguridad de la información es casi un reto para todas las empresas porque aunque se tomen medidas de seguridad lógicas como las contraseñas en algún lugar tienen que estar esas contraseñas y se corre el riesgo que alguien ajeno la encuentre o la descifre y tenga acceso a los datos y logre modificarlos. Por eso y mucho más las firmas deben implementar un sistema de gestión de seguridad.

1.4. Ventajas y desventajas de los sistemas de gestión de la seguridad de la información

Los sistemas de gestión de seguridad de la información proporcionan a la entidad la confianza y seguridad que toda la información se encuentra libre de riesgos o con un plan que ayude a minimizar su pérdida; al elegir adoptarlo es iniciar la idea de un ciclo de gestión conocido como Planear-Hacer-Chequear-Actuar (PDCA) que lleva directamente a plantear un sistema de gestión de seguridad de la información que resulta conveniente para cubrir las necesidades que la organización requiere.

La seguridad solo puede considerarse de forma razonable ya que la protección absoluta no existe, de tal forma la metodología que se utiliza para una mejora continua es la que hace que su porcentaje de aceptación en la venta de servicios sea aceptable, es decir que los beneficios son:

a) Mayor competitividad: es uno de los primeros factores que toda entidad desea cumplir y al garantizar una seguridad de calidad en el resguardo y manejo de información de sus terceros, pueden crear un prestigio que incremente su cartera de clientes de forma notable.

b) Reduce riesgos: con los sistemas integrados en todos los procesos de recolección de datos se puede evitar en gran cantidad la pérdida de información ocasionada por siniestros y otros eventos que afectan directa o indirectamente a los archivos recolectados.

c) Simplifica la documentación: se procede a la eliminación de información redundante en los archivos acumulativos de sus clientes, evitando confusión en el manejo de la misma y así facilitar la distribución de encargos a los asistentes de auditoría.

d) Facilita procesos de evaluación y auditoría: la revisión de las actividades que realizan en los encargos de auditoría resulta eficaz por conservar procedimientos que llevan un orden lógico y estandarizado a través de los sistemas de gestión de seguridad.

e) Unificación de control: a través del sistema adecuado se puede observar que los procesos ordenados de forma coherente, con la debida importancia que cada uno posee, unifica todos los procedimientos que la firma realiza lo cual precipita a tener el debido control sobre las actividades de cada colaborador y movimiento de información.

f) Mayor compromiso y motivación al personal: cuando se implementa el ciclo de seguridad estandarizado puede provocar un impacto importante en los trabajadores que colaboran en la firma ya que ellos serán los usuarios principales que harán valer cada detalle que pone en marcha las operaciones de dicha entidad.

g) Reducción de tiempo, de costos y mejora aceptable por parte de los usuarios: cuando se da un error humano o fallo del sistema, este se puede corregir con facilidad ya que todo se encuentra en orden y de forma cronológica, lo cual ayuda a maximizar el tiempo por el evento que sucede sin previo aviso.

h) Visión global con nuevas estrategias empresariales

- Mayor facilidad para el establecimiento, seguimiento y logro de objetivos de gestión en la organización de profesionales.
- Aseguramiento de la identificación y cumplimiento de los requisitos legales
- Incremento de implicación del personal y rotura de la dinámica negativa por exceso de burocracia, entre otros.
- Posibilitar enormemente la prevención y la mejora continua.

- Posibilitar la optimización de recursos y procesos.
- Consolidación de las mejores prácticas.
- Orientación hacia la calidad total.
- Aportación de mayor valor a los negocios, mediante un aumento de la productividad por parte de las personas más directamente relacionadas con la gestión.
- Globalización de la gestión de la empresa a todos los niveles y, en cierta manera, modificación y modernización de la estructura de la misma.

De forma muy frecuente, las actividades de las firmas de auditoría requieren mayor esfuerzo y se encuentran sobrecargados por el ritmo habitual de las mismas, por consiguiente el recargo del trabajo queda en el capital humano y partiendo de estas consideraciones se pueden mencionar algunas de las desventajas de un sistema de gestión de la seguridad:

a) No tiene retorno: cuando se comienza con el sistema y su implementación no se puede retroceder a tomar otra decisión porque implicaría un incremento en costos, esfuerzos y pérdida en inversiones, solo se puede tomar opción de la mejora continua.

b) Largo periodo de esfuerzo para la implementación: para poder llegar a la fase de operatividad con el sistema de gestión en los procesos de la firma de auditoría, se debe esperar un largo proceso para evaluar, determinar, estudiar, e incluir y cubrir todos los elementos necesarios que se requieren para lograr el objetivo deseado para la seguridad de la información.

c) Falta de expertos en el área: al cubrir las necesidades de la organización de profesionales con estos componentes modernos que incluyen la tecnología como un activo principal a la entidad, puede existir una considerable escases de conocimientos en otros

profesionales para poder operar, innovar, sustituir personal o pedir consultoría sobre estos puntos críticos.

d) Dificultad de flexibilidad y adaptabilidad: considerar aspectos que se puedan cambiar o incorporar otros que estén fuera del estándar establecido puede resultar tedioso e incluso sin poder dar una solución.

1.5. Aspectos técnicos relacionados a los sistemas de gestión de seguridad de la información en las firmas de auditoría.

Existe diversidad de normativas técnicas relacionadas con la protección de la información que ayudan a los profesionales, con el objeto de respaldar las actividades de auditoría que realizan, sirviendo como guía para implementar políticas y medidas de protección.(Ver tabla Nº2)

Tabla Nº2 Normativa técnica del Sistema de Gestión de Seguridad de la Información

NORMATIVA	SÍNTESIS
NICC 1 "Control de calidad en las firmas de auditoría que realizan auditorías y revisiones de estados financieros, así como otros encargos que proporcionan un grado de seguridad y servicios relacionados"	Dentro de las firmas de auditoría esta normativa es de suma importancia porque con ella se da la seguridad a los clientes que el servicio brindado es el adecuado, ya que cumple con las responsabilidades y los compromisos de confidencialidad que la firma tiene en relación con su sistema de control de calidad. Esta normativa rige a los profesionales de contaduría pública que ejercen auditoría y revisiones de estado financieros así como otros servicios relacionados, estableciendo una estructura que inicia desde los requerimientos necesarios hasta la creación de un modelo de control de calidad que define que el personal cumple con las bases legales y técnicas para ejercer y que los informes entregados son bajo un criterio adecuado según sea la circunstancia.
NIA 220, Control de calidad de la auditoría de estados	La normativa internacional también obliga al profesional en contaduría pública que al momento de ejercer debe

financieros	aplicar estrictos controles de calidad cumpliendo los siguientes elementos: - Responsabilidades de liderazgo en la calidad dentro de la firma de auditoría; - Requerimientos de ética aplicables; - Aceptación y continuidad de las relaciones con clientes, y de encargos específicos
ISO 17799 Tecnología de la Información – Técnicas De Seguridad - Código para la práctica de la Gestión de la Seguridad de la Información.	Son esenciales para las firmas de auditoría todos los archivos y datos recolectados de sus clientes para los encargos requeridos, lo cual implica que deben existir procedimientos que proporcionen una respuesta a los riesgos que estas se enfrentan. Este estándar internacional proporciona políticas de control adecuados para la protección del hardware y software y toda la infraestructura, capacitación del personal y todo lo que se involucra directa o indirectamente con la seguridad de la información y así poder maximizar recursos, lograr puntos críticos de éxito e impulsar a las organizaciones a elevar su prestigio en el mercado.
ISO 27001 Sistema de Gestión de la Seguridad de la Información	La información, como uno de los principales activos de las organizaciones, debe protegerse a través de la implantación, mantenimiento y mejora de las medidas de seguridad para que cualquier empresa logre sus objetivos de negocio, garantice el cumplimiento legal, de prestigio y de imagen de la compañía. Proporciona los parámetros para la implementación de la seguridad de la información en una organización: establece que esta división se hace en cuatro fases: planificación; implementación; revisión, mantenimiento; y mejora.
ISO 27003 Tecnología de la Información – Técnicas de Seguridad -Sistema de Gestión de la Seguridad de la Información Guía de aplicación	Esta Normativa internacional es básica para el desarrollo de los Sistemas de Gestión de la Seguridad de la Información, ya que en esta Norma se encuentran las directrices necesarias para el diseño y ejecución exitosa de un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001.

COBIT 5	COBIT ofrece un modelo novedoso de negocios para la Seguridad de la Información a través de la presentación de un enfoque integral y orientado al negocio para la gestión de la seguridad de la información, estableciendo un lenguaje común para referirse a la protección de la información. Así mismo, desafía la visión convencional de la inversión en seguridad de la información y explica en forma detallada el modelo de negocio para gestionar la seguridad de la información, invitando a utilizar una perspectiva sistémica
Código de ética de IFAC	El código de ética exhorta a los contadores a poner en práctica el principio de confidencialidad y abstenerse de: Revelar, fuera de la firma u organización que lo emplea, información confidencial obtenida como resultado de las relaciones profesionales o de negocios, sin la autorización apropiada y específica, a menos que haya un derecho o deber legal o profesional de hacer la revelación. Utilizar información confidencial obtenida como resultado de las relaciones profesionales o del negocio, para su ventaja personal o de terceros

1.6. Aspectos legales relacionados a los sistemas de gestión de seguridad de la información en las firmas de auditoría.

En el salvador debido a los riesgos relacionados con la seguridad de la información existen leyes que respaldan las acciones de los profesionales de la contaduría pública en la práctica de la auditoría externa, proporcionando lineamientos legales para la manipulación de datos obtenidos de terceros. (Ver tabla Nº3)

Tabla Nº3 Normativa legal de la Seguridad de la Información

Ley	Desglose de ley	Descripción
Ley Reguladora del Ejercicio de la Contaduría	Art. 3	Esta ley establece todas las características y obligaciones que una persona debe cumplir para poder fungir como contador público y auditor, detallando los entes relacionados a la profesión que regulan las autorizaciones para ejercer. Los sistemas de gestión de seguridad de la información también cubre el cumplimiento de esta legislación para controlar y evitar que personas no autorizadas por el Consejo de vigilancia de la profesión de contaduría pública y auditoría ejerzan como auditores y contadores dentro de la firma de auditoría.
Código penal	Art. 187 Revelación del secreto profesional Art. 217 Aprobación o retenciones indebidas Art. 218	El código penal advierte que quien revelare un secreto del que se ha impuesto en razón de su profesión u oficio, será sancionado con prisión de seis meses a dos años e inhabilitación especial de profesión u oficio de uno a dos años. Las firmas de auditoría, deben proteger los activos, en especial los de tecnología de la información ya que si alguna persona se apropiara de alguno de ellos que le resulte ajeno puede tener una condena de dos a cuatro años de cárcel. El que teniendo a su cargo el manejo , la administración o el cuidado de bienes ajenos, perjudicare a su titular alterando en sus cuentas los precios o condiciones de los contratos, suponiendo operaciones o gastos, aumentando los que hubiere hecho, ocultando o reteniendo valores o empleándolos indebidamente, será sancionado con prisión de tres a cinco años.
Código de comercio	Art. 455 Resguardo de la información en medios electrónicos	El código de comercio hace énfasis en el resguardo de la información por cualquier medio. Siempre y cuando sea certificada por un notario, previa confrontación con los originales.

Código tributario	Art. 28 Reserva de la información	Este articulo exhorta tanto a profesionales pertenecientes a la administración tributaria o no, a que mantengan reserva sobre la información contenida en las declaraciones tributarias ya que solo le compete al sujeto pasivo y a la administración tributaria o a sus dependencias legales hacer uso de los datos para efectos de cumplimiento de sus obligaciones.
	Art. 139 Contabilidad formal	El código tributario establece que no se podrá modificar la información contable, por lo tanto ésta debe permanecer integra para no poner en duda su contenido. Las partidas contables y documentos deberán conservarse en legajos y ordenarse en forma cronológica, en todo caso, las partidas contables deberán poseer la documentación de soporte que permita establecer el origen de las operaciones que sustentan; lo anterior. La contabilidad podrá llevarse en forma manual o mediante sistemas mecanizados, en otras palabras de forma física o digital.
	Art. 147 Obligación de conservar información y pruebas	El código tributario exhorta a que las personas natural o jurídica, contribuyente o no conserven la información en buen estado por un período de 10 años a partir de su emisión o recibo. Después de 4 años de emitidos o recibidos los documentos podrán conservar los archivos contables en microfilm, microfichas, discos ópticos u otros medios electrónicos, siempre que se garantice la integridad de la información.
	Art. 277 Publicidad de deudores	La administración tributaria divulgará a través de los distintos medios de comunicación los nombres de los sujetos pasivos que posean deudas firmes, líquidas y exigibles. Solamente ella está autorizada para hacer pública información confidencial, con el fin que ciertos deudores cumplan con su deber.
Ley contra el lavado de dinero y activos	Art. 7	Los que sin cierto previo con los autores o participes del delito de lavado de dinero y de activos, ocultaren, adquirieren o recibieren dinero, valores u otros bienes y no informaren a la autoridad correspondiente, inmediatamente después de conocer su origen. Este artículo señala que las empresas deben mantener por

	Art. 12	un periodo no menor de 5 años los registros necesarios sobre transacciones realizadas, tanto nacionales como internacionales.
Ley de la firma electrónica	Art. 4 Principios generales Art. 11 Conservación de documentos Art. 14	Esta ley también señala que la información resguardada, será de forma confidencial e integra, por el cual se otorga certeza que nadie ajeno, manipulará la información. Si de acuerdo al acto jurídico o por disposición legal se exige que la información sea conservada en la forma en que originalmente ha sido emitida, se entenderá que un documento electrónico cumple dicha exigencia, si la firma electrónica demuestra que el documento no ha sido alterado. La ley señala que al someterse un documento en almacenamiento debe cumplir con algunos requisitos, ya que tiene que ser resguardado adecuadamente, y deben quedar almacenados en forma íntegra, segura y con absoluta fidelidad. Y que pueda determinarse la fecha en que fue almacenado electrónicamente y que se pueda recuperar. Y sobre todo que cumple con los reglamentos técnicos y normativas establecidas por la autoridad competente.
Ley especial contra delitos informáticos y conexos	Art. 4 Acceso indebido a sistemas informáticos Art. 9 Violación a la seguridad del sistema Art. 12 Espionaje	Esta ley establece que, el que intencionalmente y sin autorización o excediendo la que se le hubiere concedido, acceda, intercepte o utilice parcial o totalmente un sistema informático que utilice las Tecnologías de la Información o la Comunicación, será sancionado con prisión de uno a cuatro años. Las firmas de auditoría deben evitar exponerse a la vulnerabilidad de la seguridad de los archivos y si algún profesional integrado dentro de la misma tiene la intención de perjudicar la imagen de la entidad se puede considerar un delito penado de tres a cinco años, así como la violación al sistema, de tres a seis años de cárcel. Esta ley advierte que el con fines indebidos obtenga datos, información reservada o confidencial contenidas en un sistema que utilice las Tecnologías de la Información y la Comunicación o en cualquiera de sus componentes, será sancionado con prisión de cinco a ocho años. Debido a esto ninguna persona integrante de la firma de auditoría

	informático Art. 15 Manipulación de registros Art. 20 Interferencia de datos	podré extraer información con fines ajenos a la misma. El dominio de datos en manos equivocadas puede resultar agraviante a la integridad de la información que los profesionales de contaduría pública manejan ya que estas pueden ser intervenidas por elementos informáticos que pueden destruir, alterar, duplicar, dañar o procesar archivos confidenciales estos pueden tener una sanción penada y dependerá del agraviante en cuestión. El que interfiera, obstruya o interrumpa el uso legítimo de datos o los produzca nocivos e ineficaces, para alterar o destruir los datos de un tercero, será sancionado con prisión de tres a seis años, de ésta forma queda prohibido que cualquier persona haga uso indebido de información que no le pertenece a la cual no está autorizado para manipular.

1.7. Sistema de gestión de seguridad de la información para los profesionales de la contaduría pública que ejercen la auditoría externa.

1.7.1. Generalidades de la seguridad de la información.

Un sistema de gestión de seguridad de la información es un conjunto de los procesos y sistemas que poseen las empresas para llevar el control de los datos de los cliente y de los activos de información que se posean, cumpliendo así con los elementos de confidencialidad, integridad y disponibilidad de los datos, pueden ser muy esenciales para mantener los niveles de competitividad, rentabilidad y estar conforme al marco legal y cumplir con la misión y visión de la empresa de acuerdo a los objetivos y asegurar los beneficios económicos que favorezcan a la empresa.

Los sistemas de gestión de seguridad de la información pueden abreviarse con las siglas SGSI, entendiendo que la información son todos los conjuntos de datos que una organización

posee ya sea propia o externa, independientemente del tipo de uso que se le dé a la misma.

- **Importancia del sistema de gestión de seguridad de la información.**

Dentro de los activos más importantes de las firmas de auditoría se encuentran: la información, los procesos y los sistemas por medio de los cuales se procesa la misma. Una adecuada protección de la información utilizando como principios bases la confidencialidad, la integridad y la disponibilidad son necesarios para conservar los niveles de competitividad y rentabilidad, indispensables para cumplir los objetivos proyectados de la organización así como los resultados esperados de la misma

En la actualidad todas las firmas y sus sistemas de información están altamente expuestos a un nivel elevado de amenazas que están a la espera de que una de sus vulnerabilidades existentes se convierta en un riesgo que afecte las operaciones.

Los SGSI son de suma importancia dentro de estas entidades ya que su fin es proteger la información y así evitar que estos riesgos sucedan.

- **Alcance del sistema de gestión de seguridad de la información**

La implementación de un SGSI en las firmas de auditoría pretende alcanzar las siguientes metas:

a) Proteger la información resguardada.
b) Mejora continua en la gestión de la seguridad.
c) Garantizar la continuidad y disponibilidad del negocio.
d) Reducción de los costos relacionados a incidentes por pérdida de información.
e) Incrementar niveles de confianza de los clientes y socios.
f) Aumentar el valor comercial y mejorar la imagen de la organización.

1.7.2. Seguridad de la Información

Seguridad de la información según ISO lo define como "preservación de la confidencialidad, integridad y disponibilidad de la información; además también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confidencialidad" (ISO/IEC 27001, 2005). Se toma énfasis en dos aspectos como lo son:

a) Bases de seguridad de la información

- Confidencialidad: procurar que la información sea accesible solo a las personas autorizadas a acceder a su utilización.
- Integridad: asegurar la exactitud y la complejidad de la información y los métodos de su procesamiento.
- Disponibilidad: asegurar que los usuarios autorizados puedan acceder a la información y a los activos asociados cuando lo requieran.

La firma debe implementar políticas de resguardo de la información, buscando los mejores dispositivos de seguridad. Para obtener mayor garantía de la misma evitando fugas de datos, además de lo mencionado anteriormente se debe establecer un compromiso de confidencialidad con los empleados que laboran en la entidad.

El contrato para mantener en secreto lo que resulta de carácter importante, cuyo objetivo principal es evitar la exposición de eventos o documentos que revelen a las empresas y sus clientes como tal ya que los profesionales se deben comprometer a no divulgar ni manipular de manera maliciosa a través de acciones que pueda violentar la confianza que se le ha proporcionado para el acceso a esta.

b) Tecnología de la información y la comunicación (TIC)

El sistema de la información es un mecanismo donde se combinan y se organizan los elementos que componen la tecnología de la información que es presentada a través de imágenes, texto, sonido y otros códigos que permiten la transmisión y lectura de la información.

La tecnología de la información forma parte de las operaciones diarias que depende de estrategias en el manejo de los mismos para respaldar las decisiones y recolección de evidencia en la práctica de auditoría externa por parte de los profesionales de contaduría pública. Como resultado del manejo de la información, los activos deben ser protegidos por los profesionales a fin de garantizar:

- Mantener de forma estratégica los activos de tecnología de la información.
- Maximizar el costo y los recursos en su forma cíclica más conveniente.
- Solucionar y/o prevenir riesgos que desgasten los TI o la vulnerabilidad de la información.
- Dar cumplimiento a la legalidad de los activos de la tecnología de la información

Las firmas de auditoría deben establecer las necesidades que tienen el personal y sus clientes para proteger la información a través de los activos tecnológicos tomando en cuenta los factores externos e internos que permiten alcanzar las metas y objetivos que propician la confidencialidad e integridad de datos, los cuales resultan como requisitos para cumplimiento de leyes, regulaciones y la consideración de riesgos para que puedan ser manejables y sostenibles por los profesionales de contaduría pública.

Los roles y actividades de los profesionales de contaduría pública son el elemento que hace funcionar las operaciones que se realizan dentro de las fases de auditoría, deben integrar las responsabilidades que establece la gerencia de las firmas para la seguridad de la información.

La seguridad lógica es una de las distintas formas de proteger los sistemas de información, utilizando técnicas informáticas o electrónicas. La firma además de proteger la infraestructura y los documentos físicos, también tiene que tomar medidas de precaución del software y los sistemas, la protección de los datos, procesos y programas, así como del acceso ordenado y autorizado de los usuarios.

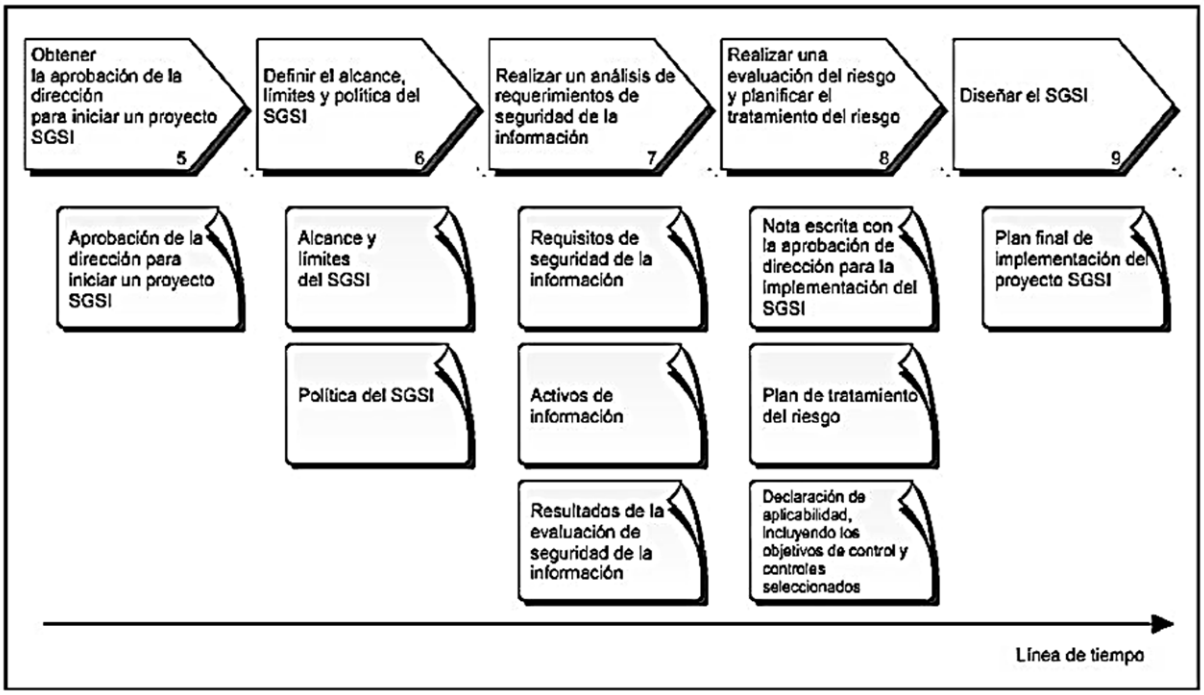
Sin embargo mantener esta seguridad no es nada fácil debido a que los TI están rodeados de peligros que amenazan la integridad de la información, así mismo incluyen ventajas que optimicen los servicios que proporcionan los profesionales a sus clientes. A continuación se presenta de forma estructurada los pasos y requerimientos para la aplicación del modelo de sistema de seguridad para la protección de la información.

1.7.3. Desarrollo e Implementación

Para la implementación de un SGSI en una firma de auditoría se consideran estándares internacionales que brindan los procedimientos específicos, los cuales están contenidos en cinco fases que son: (Ver Figura Nº3)

a) Obtener la aprobación gerencial para iniciar un proyecto SGSI.
b) Definir el Alcance y la Política del SGSI.
c) Realizar un Análisis de la Organización.
d) Realizar una Evaluación del Riesgo y planificar el Tratamiento del Riesgo.
e) Diseñar el SGSI.

Figura Nº3 Fases del proyecto SGSI



Fuente: ***ISO/IEC 27003***

En el inicio de las fases, el objetivo principal es lograr la aprobación de la gerencia, en primer lugar se elaboran los objetivos que la firma tiene en cuanto a la seguridad de la información, debe haber una comprensión de los sistemas y definir las necesidades básicas de protección al igual que las políticas y normas para que la firma pueda aprobar la implementación del sistema de gestión de seguridad. (Ver tabla Nº4)

Tabla N°4 Fase 1: Obtener la aprobación gerencial para iniciar un proyecto SGSI

FASE 1: OBTENER LA APROBACIÓN GERENCIAL		
Nº	**Actividad**	**Unidad / departamento**
1	**Obtener objetivos de la organización:** Se deben elaborar los objetivos a través de las metas deseadas por la gerencia para el crecimiento de la firma de auditoría	Dirección de la firma
	Definición de metas claras y alcanzables	
	Definir qué tipo de objetivos necesita la gerencia	
	Realizar la lista de objetivos	

2	**Lograr la comprensión de los sistemas de gestión existentes**: Es necesario que la gerencia y los profesionales logren comprender los sistemas que se manejan y las necesidades que estos poseen para la preparación futura de los sistemas nuevos que se puedan implementar	Dirección de la firma Encargado Supervisor Asistentes
	Implementar capacitaciones para lograr la comprensión	
	Desarrollo de planes de entrenamiento para la comprensión de los sistemas que poseen	
3	**Definir necesidades de seguridad para la información almacenada de sus clientes**: para poder implementar el SGSI es indispensable listar las necesidades que se desean cubrir para la seguridad de información	Encargado de gestión de seguridad
	Definir las políticas de seguridad para el recibimiento de información de sus clientes	
	Definir las políticas de seguridad para el procesamiento y almacenamiento de información de sus clientes	
	Definir las políticas de seguridad para la entrega del informe final del encargo de auditoría	
4	**Obtener las normas reglamentarias y de cumplimiento a las firmas de auditoría**: se deberán aplicar las normas que apliquen partiendo de su capital, su nivel de manejo de información, su constitución legal, entre otros aspectos.	Dirección de la firma Encargado de gestión de seguridad
	Conocer el entorno de la firma de auditoría	
	Resumir las normas aplicables en base a su entorno y su operacionalización de servicios	
5	**Definir alcance preliminar del SGSI**: se necesita establecer las metas esperadas previamente a la implementación del sistema de seguridad apropiado.	Dirección de la firma Encargado de gestión de seguridad
	A partir de los objetivos y las normas aplicables, describir la visión de proyectos que posee la firma de auditoría antes de implementar el SGSI	
	Describir los roles de cada profesional para el cumplimiento de esas metas proyectadas	
6	**Determinar el plan proyectado para la aprobación de la gerencia**	Encargado de gestión de seguridad
7	**Obtener la aprobación de la gerencia y el compromiso para iniciar el proyecto de implementación de un SGSI**	Dirección de la firma

Fuente: ***ISO/IEC 27003***

En esta fase se debe comprender que es lo que se pretende con la implementación del sistema, definiendo los límites que tendrá el SGSI en cuanto a la tecnología y todo el entorno físico de la entidad, para tener una visión del alcance de las políticas, por medio de un análisis interno y externo de todo lo que la rodea. (Ver tabla Nº5)

Tabla N°5 Fase 2: Definir alcance y política de un SGSI

FASE 2 : DEFINIR ALCANCE Y POLITICA DE SGSI		
Nº	**Actividad**	**Unidad / departamento**
1	**Definir límites de la firma de auditoría**: para poder determinar un nuevo sistema de seguridad de información se deben tener claro los límites que esta posee para lograr cubrirlos y maximizar recursos.	Supervisor y encargado
	Descripción de limites	
	Funciones y estructura de la firma de auditoría	
	Intercambio de información a través de limites	
	Identificación de límites sobre los procesos de información en físico	
	Descripción de las oportunidades dentro y fuera de la firma de auditoría.	
2	**Definir límites de las tecnologías de información y comunicación**: se deben describir los límites que tienen la infraestructura tecnológica que almacena la información para poder mejorar estrategias de mantenimiento.	Encargado de gestión de seguridad
	Descripción de los procesos operativos de las tecnologías de información	
	Descripción de límites de los activos tecnológicos	
	Descripción de los alcances dentro y fuera de la firma de auditoría	
3	**Definir límites físicos:** las instalaciones pueden poseer limitantes que se deban cubrir para poner como propuesta en los alcances del SGSI.	Encargado de gestión de seguridad
	Descripción de límites físicos	
	Descripción de las características geográficas	
	Descripción de los límites de las características geográficas	
	Descripción de los alcances internos y externos en la ubicación de la firma	

4	**Finalizar límites para el alcance del SGSI**	Encargado de gestión de seguridad
5	**Desarrollar la política del SGSI:** cuando se tengan elaboradas las políticas se deberá preparar para la aprobación de la dirección de la firma y gestionar la fase 3.	Dirección de la firma

Fuente: ***ISO/IEC 27003***

Antes de la implementación se debe realizar un análisis exhaustivo de la firma, en cuanto a las vulnerabilidades físicas y lógicas, además de identificar las actividades que realiza cada empleado para verificar si cumplen con la confidencialidad, integridad y disponibilidad de la información. (Ver tabla Nº6)

Tabla N°6 Fase 3: Definir requerimientos de seguridad de la información.

FASE 3: DEFINIR ALCANCE Y POLÍTICA DE UN SGSI		
Nº	**Actividad**	**Unidad / Departamento**
1	La firma tendrá un listado de las principales funciones de cada auditor, regidos por el código de ética profesional, el cual lo faculta para: Verificar datos confidenciales de los clientes. Recopilar información adecuada y suficiente para cumplir con el encargo. Denunciar en caso de descubrir un fraude. **Sistemas de información** La firma debe: Diseñar sistemas y software con un enfoque modular. Estructurar y documentar sistemas y software usando métodos sistemáticos. Probar sistemas y software de manera que se puedan mantener y auditar fácilmente. **Redes de comunicación:** El sistema debe estar protegido mediante contraseñas, que se cambiaran cada 15 días y solo tendrá acceso el personal autorizado por la dirección.	Encargado de gestión de seguridad

2	**Requerimientos de la organización referentes a confidencialidad, disponibilidad e integridad**: Los auditores firmaran un contrato de confidencialidad, como compromiso legal el cuál prohíbe revelar información de los clientes. En cuanto a la disponibilidad, es obligación como medida de seguridad de la información, crear respaldos y guardar copias de todos los datos. Los auditores tendrán acceso a áreas específicas, y solo mediante autorización del cual se llevará un control mediante fichas o formularios.	Encargado de gestión de seguridad
3	**Requerimientos de la organización relacionados a requisitos legales y reglamentarios, contractuales y de seguridad de información del negocio**: Cada empleado firmará contrato de trabajo y de confidencialidad. Se firmará contrato con la empresa a la cual se le hará el encargo. Se deberán tener políticas de seguridad de la información, relacionadas con el resguardo desde el inicio hasta que finalice el encargo.	Encargado de gestión de seguridad
4	Lista de vulnerabilidades conocidas de la organización. Para lo cual se deben establecer medidas de seguridad: **Ambientales**: se deben establecer medidas de protección en todo el entorno físico donde se resguarda la información para protegerse de los desastres naturales. **Económicas**: Crear un plan de contingencia económica para contar con los recursos necesarios para proteger la información. **Falta de formación y conciencia:** Se tiene que capacitar al personal para que tengan la formación necesaria de acuerdo a sus obligaciones. **Fuga de información:** Evitar que personas ajenas a la firma tengan acceso a los sistemas y a la documentación física mediante cámaras y un estricto control en la entrada donde se procesa la información.	Encargado de gestión de seguridad

5	Descripción de los principales procesos de la firma: Al aceptar el encargo la firma se hace responsable de revisar toda la información de la empresa, mediante un proceso de recopilación de información necesaria y adecuada para lo cual se hará un análisis del que posteriormente darán su opinión, consiste en tres fases: planeación, ejecución e informe.	Gerencia General
6	Identificación de activos de información de los principales procesos de la organización. La firma cuenta con: 2 Computadoras de Escritorios 3 Computadoras Laptops 10 memorias USB 50 CD en blanco	Encargado de gestión de seguridad
7	Documento del estado actual de seguridad de la información de la organización y su evaluación incluyendo controles de seguridad existentes.	Dirección de la Firma
8	Documento de las deficiencias de la organización evaluadas y valoradas	Encargado de gestión de seguridad

Fuente: ***ISO/IEC 27003***

Después de analizar el entorno de la entidad se deben evaluar los riesgos a los que se enfrenta la firma, clasificar dichos peligros que resultan tanto interna como externa y encontrar las posibles soluciones en base a criterios e innovación de controles que puedan minimizar las consecuencias, posteriormente en base a los resultados obtenidos donde se demuestra que la entidad está expuesta a muchos riesgos a los cuales se les puede enfrentar y solucionar se procederá a redactar el documento para la aceptación del SGSI por parte de la dirección de la firma. (Ver tabla Nº7)

Tabla N°7 Fase 4: Evaluación del riesgo y selección de opciones para su tratamiento

FASE 4 : EVALUACION DEL RIESGO Y SELECCIÓN DE OPCIONES PARA SU TRATAMIENTO		
Nº	**Actividad**	**Unidad / Departamento**
1	**Realizar una evaluación del riesgo:** Se deberá realizar un estudio para conocer e identificar cuáles son los riesgos que posee.	Encargado de gestión de seguridad
2	**Alcance para la evaluación del riesgo:** Se deberá definir los riesgos internos y externos cercanos a la firma de auditoría.	Encargado de gestión de seguridad
3	**Metodología de evaluación del riesgo aprobada:** En base a la metodología aprobada por la administración se debe realizar una evaluación de cada uno de los riesgos identificados.	Encargado de gestión de seguridad
4	**Criterio de aceptación del riesgo:** Se deberán establecer criterios de valoración para tomar decisiones sobre la aceptación ó negación del riesgo, tales como: riesgos de nivel alto, bajo o medio.	Encargado de gestión de seguridad
5	**Objetivos de control y controles:** Al definir los riesgos, su valuación y aceptación, se deben definir objetivos para contrarrestar la afectación de los mismos y controles que ayuden al cumplimiento de los objetivos definidos.	Encargado de gestión de seguridad
6	**Resultados totales de la evaluación de riesgos:** En base a la aplicación de los controles se determinará cuál ha sido la evaluación del riesgo para obtener un resultado global del mismo.	Encargado de gestión de seguridad
7	**Aprobación de la dirección para implementar SGSI:** En base a los resultados obtenidos se podrá sustentar la necesidad de un SGSI que previo a su implementación deberá ser aprobado por la dirección de la firma. Se deberá realizar un informe detallando los riesgos identificados y las opciones para el tratamiento del mismo en base a los objetivos de control establecidos y los controles de cumplimiento; se debe considerar que el riesgo siempre está latente por lo que existirá un porcentaje ó una valoración residual la cual debe ser aprobada por la dirección para ser autorizado el SGSI.	Dirección de la Firma
8	**Preparar declaración de aplicabilidad:** Al tener la aprobación y autorización para la implementación y manejo del SGSI se deberá elaborar una declaración de la aplicabilidad del mismo.	Encargado de gestión de seguridad

Fuente: ***ISO/IEC 27003***

En la parte final se diseñará el SGSI tomando en cuenta toda la estructura de la firma, en base a objetivos, documentos que sustentan los procedimientos, políticas de seguridad físicas y lógicas. (Ver tabla Nº8)

Tabla Nº8 Fase 5: Diseño del SGSI

FASE 5: Diseño del SGSI		
Nº	**Actividad**	**Unidad / departamento**
1	**Diseñar la seguridad de la organización**	Encargado de gestión de seguridad
	Estructura de la organización, roles y responsabilidades relacionados con la seguridad de la información	
	Identificación de documentación relacionada al SGSI	
	Plantillas para los registros del SGSI e instrucciones para su uso y almacenamiento	
	Documento de política de seguridad de información	
	Línea base de políticas de seguridad de la información y procedimientos (y si es aplicable planes para desarrollar políticas, procedimientos, entre otros de términos específicos)	
2	**Diseñar la seguridad de la información física y de las TIC**	Encargado de gestión de seguridad
	Implementación del plan de proyecto para el proceso de los controles diseñados para la seguridad física y de las TIC seleccionados	
3	**Diseñar la seguridad de la información específica del SGSI**	Encargado de gestión de seguridad
	Procedimientos describiendo el reporte y los procesos de revisión por la dirección.	
	Descripciones para auditorías, seguimientos y mediciones	
	Programa de entrenamiento y concientización	
4	**Producir el plan final del proyecto SGSI**	Encargado de gestión de seguridad
	Plan de proyecto de implementación aprobado por la dirección para los procesos de implementación	
5	**El plan final del proyecto SGSI**	Encargado de gestión de seguridad
	Plan de proyecto de implementación del SGSI especifico de la organización cubriendo el plan de ejecución de las actividades para seguridad de la información organizacional, física y de las TIC, así como también los Requerimientos específicos para implementar un SGSI de acuerdo al resultado de las actividades incluidas en ISO/IEC 27003	

Fuente: ***ISO/IEC 27003***

CAPÍTULO II METODOLOGÍA DE INVESTIGACIÓN

2.1. Tipo de estudio

Para el desarrollo de esta investigación se requieren aspectos que puedan describir los procedimientos y factores que influyen en el Sistema de Gestión de Seguridad de la Información basado en ISO 27001 y 27003 y poder comparar con las normativas y leyes que estén relacionadas en la misma función, es por ello que la investigación se considera "analítica – descriptiva"

2.2. Unidad de análisis

La población a considerar fueron las personas naturales y jurídicas autorizadas que pueden ejercer la contaduría pública y auditoría bajo los términos de la Ley Reguladora del Ejercicio de la Contaduría Pública.

2.3. Universo y muestra

2.3.1. Universo

Así como se definió la unidad de análisis, según la publicación del 31 de diciembre de 2014 proporcionada por el Consejo de Vigilancia de la profesión de contaduría pública y auditoría, son en total 4,250 profesionales autorizados de El Salvador.

2.3.2. Muestra

La muestra se consideró que a partir del universo de estudio determinado se seleccionó con las mismas probabilidades y fue calculada a través de la siguiente fórmula:

Dónde:

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

Símbolo	Significado	Numero considerado
n	tamaño de la muestra	x
N	población	4.250
Z	coeficiente de confianza	1.96
e	margen de error	0.04
P	probabilidad de éxitos de que la problemática exista	0.95
Q	Probabilidad de fracaso	0.05

Sustituyendo los valores en la formula, el resultado es:

$$n=\frac{(4250)(0.95)(0.05)(1.96)^2}{(4250-1)(0.04)^2+(0.95)(0.05)(1.96)^2}$$

$$n=\frac{(4037.50)(0.19208)}{(6.7984)+(0.182476)}$$

$$n=\frac{775.523}{6.980876}$$

$$n=111.0923$$

De acuerdo a lo obtenido de la formula la muestra es de 111 profesionales autorizados que ejercen la contaduría pública y auditoría, en el método de elección tienen la misma probabilidad la población en estudio ya que es en forma aleatoria.

2.4. Instrumentos y técnicas a utilizar en la investigación

2.4.1. Instrumento

La investigación requirió información y experiencia de los que participan en esta profesión de auditoría externa para determinar la problemática o procedimientos que ellos mismos aplican y determinar lo que las organizaciones actualmente tiende a repetir u omitir sin percibir estas acciones.

Es por ello que se aplicó como herramienta la encuesta, para realizar las debidas preguntas a la población adecuada y poder realizar un diagnóstico y una conclusión según la participación de la población profesional y poder determinar los factores en estudio para que sean aplicables en los servicios de auditorías externas.

2.4.2. Técnica

La encuesta se realizó con preguntas de selección múltiple y cerradas a los profesionales de contaduría pública que ejercen la auditoría externa para proceder a la tabulación y realizar el diagnostico de acuerdo a los resultados.

2.5. Recolección de la información

La información fue recolectada a través de diferentes medios relacionados a la temática de estudio, y a su vez es utilizada como marco de referencia para realizar el diagnóstico adecuado.

2.5.1. Bibliografía

Para el desarrollo de este modelo de sistema de gestión, fue utilizada la información disponible en los gremios relacionados a la profesión de contaduría pública, además se utilizaron archivos que se encuentran accesibles para complementarla como: internet, libros, tesis, entre otros.

2.6. Procesamiento de la información

La información obtenida a través de la encuesta será procesada conforme a cálculos en Excel para que a mayor vistosidad, se puedan interpretar los resultados, a través de una gráfica y luego su análisis posteriormente revelar el diagnostico pertinente.

2.7. Diagnóstico de la investigación.

Con base a la información obtenida se pueden identificar causas, consecuencias, limitantes u omisiones que el problema abarca en términos de aplicación lo cual ayudará a determinar factores de mejora para que los profesionales de contaduría pública que ejercen auditorías externas puedan aplicar los Sistemas de Gestión de Seguridad de la Información y poder tener mayor competencia en el mercado como organización que ofrece servicios profesionales. En relación a lo expuesto se destacan las siguientes temáticas:

- Conocer como impactaría la implementación de un modelo de sistema de gestión de seguridad de la información en referencia al marco de ISO 27001 Y 27003.
- La necesidad de implementar dicho modelo, es con el propósito de mejorar la seguridad de la información de sus clientes y de su misma organización a través de controles que estén relacionados de forma directa e indirecta.
- Los profesionales de contaduría pública y su participación en conocimiento y aplicación para el resguardo de información.

A continuación se realiza un diagnóstico relacionando las preguntas más similares que se elaboraron en la encuesta para presentar un análisis más certero acerca de la problemática.

Diagnóstico para los profesionales de contaduría pública que ejercen auditoría externa

A partir de los resultados de las encuestas se determinó que la mayoría de los profesionales de contaduría pública poseen poco conocimiento sobre los sistemas de gestión de la seguridad de la información, por lo que las medidas preventivas para el resguardo de datos de las entidades auditadas no son aplicadas correctamente, ya que los encargados carecen de la parte formativa e

informativa por la falta de continuidad en seminarios, y a su vez son afectados por la limitación de capacitaciones especializadas en el tema por parte de los gremios. (Ver tabla Nº9)

Tabla Nº9 Conocimiento que se tiene acerca del SGSI

Pregunta	Criterio	Alternativa	Frecuencia absoluta	Frecuencia relativa
17	Conocimiento de SGSI	Sí conozco	28	25.23%
		Conozco poco	69	62.16%
		No conozco	14	12.61%
18	A través de qué medios obtuvo conocimiento del SGSI	Congresos	17	17.53%
		Seminarios	60	61.86%
		Internet	62	63.92%
		Libros	7	7.22%
		Folletos	20	20.62%
		Revistas	5	5.15%

Fuente: Elaboración propia

Respecto a los datos tabulados se pudo constatar que poseen deficiencias en los controles para mantener la integridad de los datos, ya que los dispositivos de respaldo que dicen utilizar los profesionales encuestados, en su mayoría se encuentran expuestos a robo, virus, error humano entre otros, en consecuencia de esto, el enfrentamiento ante un siniestro implicaría un impacto significativo por no poseer los planes de contingencia más adecuados y esto podría poner en discrepancia la eficiencia y eficacia de la firma afectando la cartera de clientes como tal.

Sin embargo, los profesionales manifiestan que en las firmas de auditoría se establecen compromisos de confidencialidad con el personal de trabajo, lo cual no les garantiza que se encuentren libres de riesgo, ya que puede suceder que se tenga acceso no autorizado a la información que se encuentra en custodia y está pudiendo ser manipulada, lo que implicaría un costo económico, la pérdida del cliente o de la credibilidad de la organización.

De acuerdo a los sistemas de gestión, la disponibilidad de los datos y archivos se mantienen a través de planes de contingencia ante fallas de red, mantenimientos del servidor y otro tipo de controles que según los datos tabulados son los que se utilizan con menor frecuencia por parte de los profesionales y esto provocaría que la accesibilidad de la información no se encuentre disponible en el momento preciso. (Ver tabla Nº10)

Tabla Nº10 ¿Qué debe incluir el SGSI?

Pregunta	Criterio	Alternativa	Frecuencia absoluta	Frecuencia relativa
7	Compromisos de confidencialidad	Si	100	90.09%
		No	11	9.91%
8	Controles de confidencialidad de la información	Encriptación de la información	44	39.64%
		Firmas electrónicas	57	51.35%
		Restricción de puertos USB	31	27.93%
		Restricción de impresiones	23	20.72%
		Codificación de accesos y permisos	52	46.85%
		Restricción de acceso a internet	39	35.14%
		Acceso solo a correos empresariales	48	43.24%
9	Dispositivos de respaldo	Disco duro	96	86.49%
		Nube	39	35.14%
		USB	67	60.36%
		Correo electrónico	49	44.14%
		Servidores en red	32	28.83%
		Celulares	4	3.60%
		Tablet	7	6.31%
		Otros	2	1.80%
10	Controles para conservar la integridad de la información	Modificación solo mediante personal autorizado	61	54.95%
		Criptografía de datos	27	24.32%
		Registro de actividades y eventos	38	34.23%
		Controlar el acceso físico a los equipos y componentes de la red	37	33.33%
		Firma digital	47	42.34%

		Control para resguardo de los dispositivos de almacenamiento	30	27.03%
		Actualizaciones del sistema operativo	35	31.53%
		Firewall o cortafuegos	41	36.94%
		Restricción de acceso a programas y archivos	50	45.05%
		Restricción de ubicación y horario	12	10.81%
13	Controles para la disponibilidad	Respaldo virtual de información	63	56.76%
		Acceso a personal autorizado	56	50.45%
		Plan de contingencia ante fallas de la red	21	18.92%
		Mantenimiento de equipos	83	74.77%
		Mantenimiento de infraestructura e instalaciones	17	15.32%
		Mantenimiento del servidor de red	36	32.43%
		Mantenimiento de la red inalámbrica	12	10.81%
		Mantenimiento de correos electrónicos	38	34.23%
		Mantenimiento del equipo electrónico	36	32.43%

Fuente: elaboración propia

Según la recolección de datos es preciso notar que las firmas de auditoría contienen una variedad de encargados para recibir la información lo que implicaría, verificar la situación individual de cada entidad para analizar cómo están conformadas y poder delegar a la persona más adecuada como responsable de la auditoría para que tenga la potestad de distribuir y manipular los datos de la entidad auditada, y aunque la tabulación revela que menos del 50% sufrieron una pérdida de archivos sobre sus clientes, es innegable que los profesionales deben tomar medidas de control ya que lo contrario de la población reveló que su mayor causa de

pérdida de información fue por error humano o por virus por lo que la recuperación de sus papeles físicos y digitales fueron en su mayoría reconstruidos o recuperados por medio de correo electrónico lo que indica que un SGSI sería apropiado para cubrir el área del personal de trabajo así como el mantenimiento de los activos tecnológicos que almacenan la información confidencial e indispensable para cumplir con el encargo requerido. (Ver tabla Nº11)

Tabla Nº11 Importancia del SGSI

Pregunta	Criterio	Alternativa	Frecuencia absoluta	Frecuencia relativa
4	Auditor responsable de recibir la información	Encargado o gerente de auditoría	72	64.86%
		Supervisor	49	44.14%
		Asistente Senior	42	37.84%
		Asistente Junior	18	16.22%
		Otro	6	5.41%
11	Controles para mantener la integridad ante un siniestro	Perfectas condiciones de las instalaciones eléctricas	48	43.24%
		Instalar, utilizar y mantener actualizados antivirus y anti - spyware	74	66.67%
		Servidores de respaldo	65	58.56%
		Servidores en la nube	38	34.23%
		Uso de polarizado en las instalaciones	23	20.72%
		UPS	45	40.54%
		Póliza de seguro	13	11.71%
		Otro	1	0.90%
12	Métodos de protección para papeles físicos	Clasificación de acuerdo a confidencialidad y sensibilidad de la información contenida	50	45.05%
		Almacenamiento en lugares de acceso restringido	77	69.37%
		Emisión de autorización previa para el uso y manejo de la información	40	36.04%
		Control por escrito de entradas y salidas de los papeles físicos	52	46.85%
		Mantenimiento de	51	45.95%

		instalaciones		
14	Perdida de información en las firmas de auditoría	Si	52	46.85%
		No	59	53.15%
15	Causas de perdida de información	Por robo o hurto	14	26.92%
		Por virus	21	40.38%
		Por error humano	28	53.85%
		Fallas eléctricas	9	17.31%
		Accidentes incendios	0	0.00%
		Problemas del software	7	13.46%
		Problemas del hardware	7	13.46%
16	Actividades para recuperar la información	Lo recupera con el respaldo almacenado en la nube	40	36.04%
		Recuperación por medio de cuenta de correos electrónicos	43	38.74%
		Resguardo en dispositivos móviles (celulares, Tablet)	12	10.81%
		Reconstrucción de papeles físicos	49	44.14%
		Se le solicita al cliente nuevamente	36	32.43%
		Recuperaría la información a través de un servidor externo	27	24.32%
		Otro	6	5.41%

Fuente: elaboración propia

La población encuestada revela que la constitución de una firma de auditoría independientemente sea conformada por una sola persona natural o varias formando una entidad jurídica es muy similar en estructura y obligaciones de los mismos, aunque la cantidad de información varía significativamente entre estas por el nivel de clientes a los que se les presta el servicio, para ello siempre es recomendable la implementación de un sistema de seguridad ya que eso permitirá dar un valor agregado a su entidad independientemente del tipo que sea.

El modelo de SGSI es aceptable por la población de los profesionales y aunque las limitaciones de cada profesional no sean tan fáciles de suprimir, el motivo principal para su implementación es la seguridad de la información. Es por ello la iniciativa de crear el sistema más apropiado para las firmas de auditoría y mejorar los procedimientos de control para el resguardo de información y el mantenimiento de los activos tecnológicos que la almacenan.

Tabla Nº12 Limitaciones para la adopción o aplicación del SGSI

Pregunta	**Criterio**	**Alternativa**	**Frecuencia absoluta**	**Frecuencia relativa**
1	Constitución legal	Persona natural	56	50.45%
		Persona jurídica	55	49.55%
2	Servicios de las firmas de auditoría	Auditoría externa	110	99.10%
		Auditoría fiscal	75	67.57%
		Auditoría Forense	18	16.22%
		Auditoría interna	38	34.23%
		Auditoría en sistemas	24	21.62%
		Contabilidad	91	81.98%
		Consultoría	58	52.25%
		Asesoría	59	53.15%
3	Cargos de auditoría	Encargado o gerente de auditoría	92	82.88%
		Supervisor	70	63.06%
		Asistente Senior	66	59.46%
		Asistente Junior	55	49.55%
		Otro	10	9.01%
19	Aceptación del Modelo SGSI	Si	92	82.88%
		No	12	10.81%
		Abstinencia	7	6.31%

Basado en toda la información recolectada, antes detallada podemos determinar que los profesionales de contaduría pública que ejercen la auditoría externa en el país, si bien se comprobó que utilizan métodos básicos como antivirus, equipos de respaldo, mantenimientos

entre otros para proteger los activos donde resguardan la información de sus clientes, existen muchas necesidad para que esta protección sea más confiable y segura.

Es por ello que se plantea la opción de un modelo de sistema de gestión de la seguridad de la información adaptado para una firma de auditoría como herramienta para la protección de la información, el cual aportará grandes beneficios entre ellos un valor agregado y prestigio, los resultados indican que los profesionales necesitan este modelo para mejorar sus procesos y están dispuestos a aceptarlo.

CAPÍTULO III. Sistema Gestión de Seguridad de la Información en una firma de auditoría

El presente modelo de sistema de gestión de seguridad de la información aplicado a los profesionales de contaduría pública que ejercen la auditoría externa con el propósito de facilitar y mejorar los procesos de resguardo y protección de la información que se maneja en los encargos puede ser utilizado por las firmas jurídicas y las naturales.

Para el desarrollo se deberá designar un encargado quien lo llevará a cabo por medio de las siguientes fases:

a) Obtener la aprobación gerencial para iniciar un proyecto SGSI
b) Definir alcance y política de un SGSI
c) Definir requerimientos de seguridad de la información
d) Realizar una evaluación del riesgo
e) Diseño del SGSI

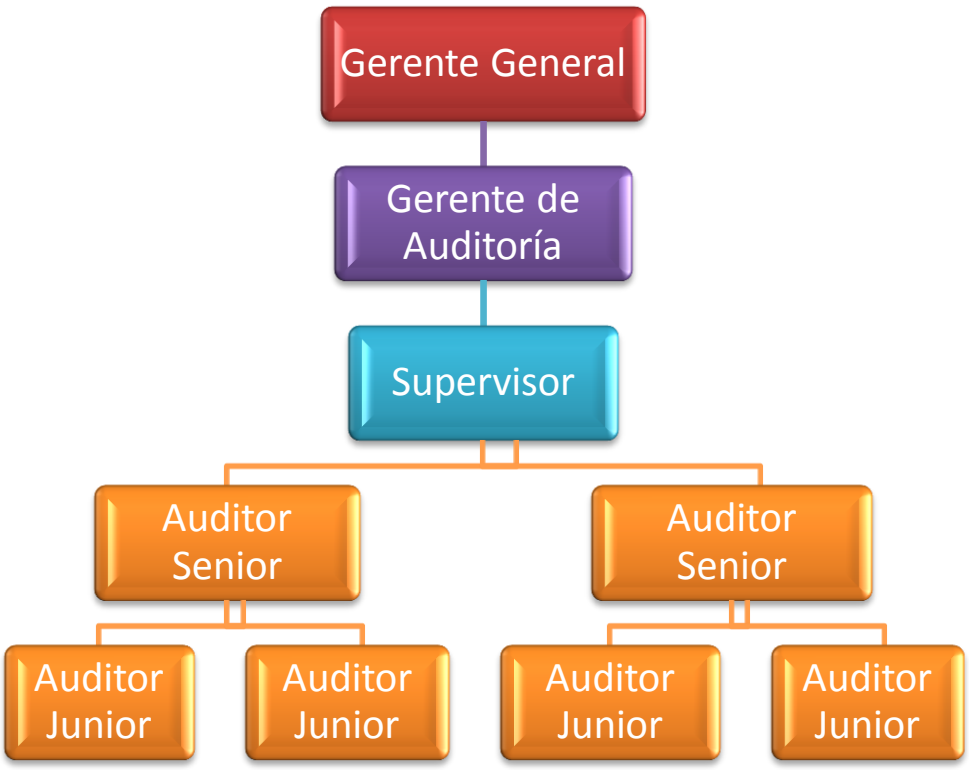
Para acompañar este modelo ha sido desarrollado un estudio de caso con el propósito de instruir cómo se pueden aplicar en el ejercicio profesional, a continuación se desplegara información sobre una firma de auditoría ficticia, H.L.H y CIA, S.A.; sin omitir que este caso es únicamente ilustrativo y según sea la estructura y requerimientos de la firma podrá ser adaptado a las necesidades.

H.L.H y CIA, S.A.

Es una firma de auditoría conformada por tres socios Wanda Huezo, Fiorela Larios y Lya Hurtado quienes se unieron y decidieron formar la sociedad anónima H.L.H., S.A., fue años después que se le incluyo al nombre la palabra compañía en sus siglas CIA debido a la inclusión nuevos socios a la firma, con la aportación de infraestructura donde se encuentran ubicadas

actualmente las oficinas de la firma, a este edificio no se le da mantenimiento preventivo solo correctivo cuando sucede un siniestro.

Servicios y empleados



La firma brinda servicios tales como consultorías, asesorías, auditorías forenses, fiscales, especial pero su especialidad son las Auditorías Externas, actualmente cuenta con nueve empleados desempeñando puestos desde Gerente General hasta Auditor Junior, la estructura de la empresa es la siguiente:

Donde el Gerente General ó Administrador Lic. Antonio Jovel, es el encargado de controlar los intereses de la firma, la Gerente de Auditoría Licda. Raquel Girón controla las operaciones y servicios con ayuda del supervisor Lic. Marvin Díaz quien es el encargado de monitorear el desarrollo que realizan los auditores senior Lic. Samuel Alvarado y Lic. Carlos Novoa y juniors

Cecilia Navas, Alice Martínez, Federico Argueta y Andrea Rivas. Ocasionalmente permiten la realización de pasantías u horas sociales a estudiantes de bachillerato y universidad.

De la información en la firma.

Al momento que un cliente solicita llevar a cabo un encargo el supervisor asigna a uno de los auditores senior y junior para preparar la oferta técnica y económica y ser enviada al cliente por medio de servicio de correspondencia subcontratada (AEROFLASH), al momento que el cliente firma de aceptado y retorna la oferta, se procede a realizar la planificación de la auditoría externa que se llevará acabo, una vez establecida se inicia el desarrollo durante el proceso se hace un intercambio de información entre el cliente y la firma, esta documentación es solicitada por teléfono, en las visitas, por correo electrónico y a través de correspondencia, cuando lo solicitado llega es recibido por el que este más inmediato (gerente de auditoría, supervisor, senior ó junior), posteriormente es entregada a la persona encargada en este lapso de tiempo no hay supervisión de la información queda expuesta y al alcance de todos.

El senior con ayuda del junior preparan los tres archivos necesarios (Administrativo, Permanente y Corriente) una parte en físico y otra en digital esta última está guardada en el disco duro de la computadora portátil de uno de ellos, cuando el otro necesita de cierta información se la trasladan a través de un correo electrónico no empresarial y en cualquier momento (día y hora). La documentación física se encuentra en archivadores disponibles para todos los empleados de la empresa, hasta de los pasantes.

Las TIC en la firma

La sociedad cuenta con 3 computadoras de escritorio todas conectadas a un regulador de voltaje, 4 portátiles que pertenecen a los auditores (seniors y juniors), todas poseen antivirus libre

el cual renuevan en línea de forma gratuita cada cierto tiempo, dentro de la firma poseen acceso a Internet sin ninguna restricción ni control la compañía contratada chequea eventualmente el funcionamiento de la red, fuera de ella tienen la accesibilidad de conectarse a cualquier red inalámbrica pública o privada.

Han adquirido un sistema de auditoría donde se vacía la información recopilada a lo largo del encargo para la generación de informes y otros documentos como cedulas de resumen, detalle, analíticas y de hallazgos que ayudan a la realización del informe. Todos tienen acceso a este pero no cuentan con una configuración en red, por lo que el trabajo y las modificaciones solo se encuentran en el equipo asignado de quien lo realiza, cada uno es responsable de crear su propio respaldo y a menudo este es en una USB que no ha sido proporcionada por la firma y no se mantiene resguardada dentro de la misma, no poseen claves de ingresos ni contraseñas.

A las computadoras se les da mantenimiento cada tres meses por una empresa subcontratada quien llega a la firma y retira una maquina se la lleva a las instalaciones para el mantenimiento y luego las devuelve este trámite tarda entre 3-4 horas.

Finalización del servicio

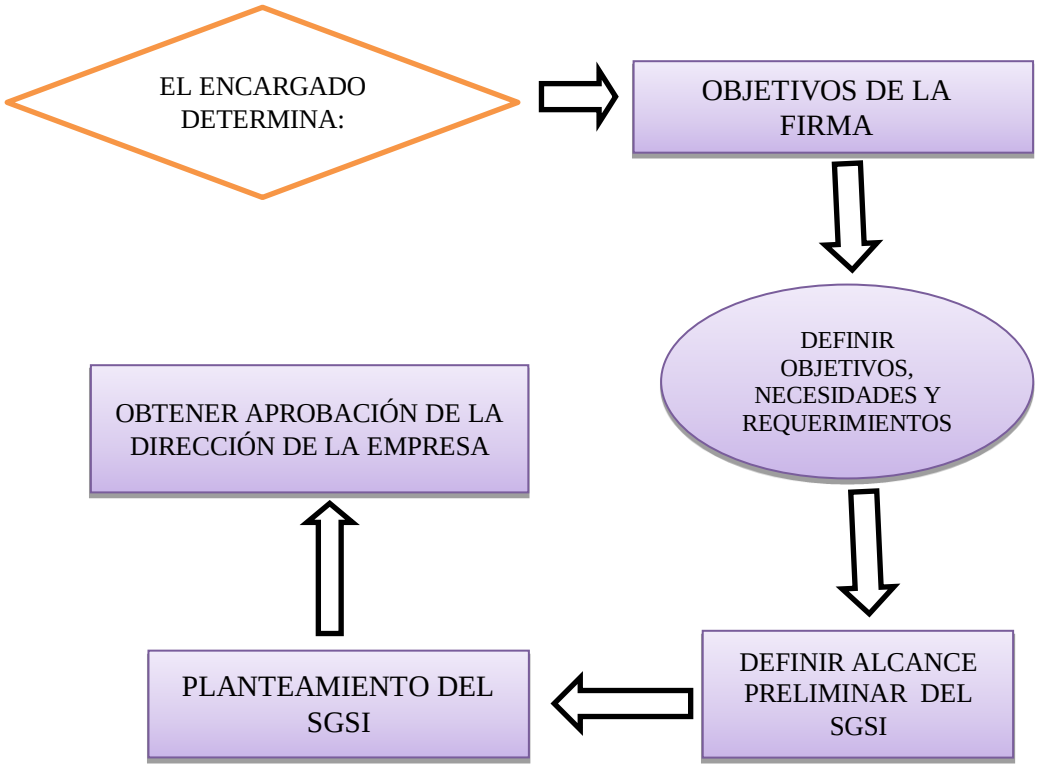
Previo a la emisión el dictamen se realiza un preliminar o borrador que es enviado al cliente para su verificación por medio de correo electrónico, el cliente lo revisa hace sus comentarios o recomendaciones y lo devuelve por el mismo medio, una vez subsanadas las observaciones se imprime, se firma y se envía por correspondencia subcontratada.

Modelo de sistema de gestión de la seguridad de la información en la firma

Luego de conocer los procesos y características de la firma se propone la implementación del modelo en H.L.H y CIA, S.A., para lo cual se nombra como encargado de la gestión de la seguridad al Lic. Marvin Díaz (supervisor) cumpliendo las fases citadas inicialmente.

3.1. Obtener la aprobación gerencial para iniciar un proyecto SGSI

Figura Nº4 Flujograma de fase 1



El Lic. Díaz realiza la gestión de aprobación de la gerencia general, con el formulario de "aprobación gerencial" en el cual se definen los objetivos, normas reglamentarias y de cumplimiento, alcance y plan del SGSI.

APROBACIÓN GERENCIAL

PROCEDIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

ÁREA:		FECHA:
SOLICITADO POR:	Lic. Marvin Díaz	AUTORIZADO POR: Lic. Antonio Jovel
REVISADO POR:	Licda. Raquel Girón	
APROBADO POR:	Licda. Raquel Girón	FECHA: 15/07/2016

OBSERVACIONES O COMENTARIOS:

OBJETIVOS DE LA FIRMA

- Fortalecer en los auditores de la firma los valores éticos y morales respecto a la seguridad de la información
- Fomentar en los empleados de la firma la responsabilidad del manejo de la seguridad de la información, desde la perspectiva de la confiabilidad, integridad y disponibilidad
- Aumentar el valor agregado en la firma de auditoría, para brindar un mejor servicio a los clientes.

ALCANCE DEL SGSI

La implementación del modelo tiene como alcance mejorar la seguridad de información que se encuentra bajo la responsabilidad de la firma ya sea propia o de clientes, así como pretende alcanzar un alto nivel de protección.

PLANTEAMIENTO DEL SGSI

El sistema de gestión de seguridad de la información, mejorará los proceso actuales de H.L.H. y CIA, S.A., y los complementará con métodos innovadores y tecnológicos que incrementaran la seguridad y la protección de los datos y archivos que en la firma se resguardan, además reducirá el riesgo de pérdida y reforzando así la confidencialidad, integridad y disponibilidad.

OBJETIVOS Y NECESIDADES DE LA FIRMA

OBJETIVOS:

Implementar un modelo de SGSI que mejore los procesos de seguridad de la firma y de la información que en ella se maneja.

Reforzar la protección de la documentación, datos y archivos tanto físicos como digitales.

NECESIDADES:

La firma necesita incrementar la seguridad y los respaldos de la información.

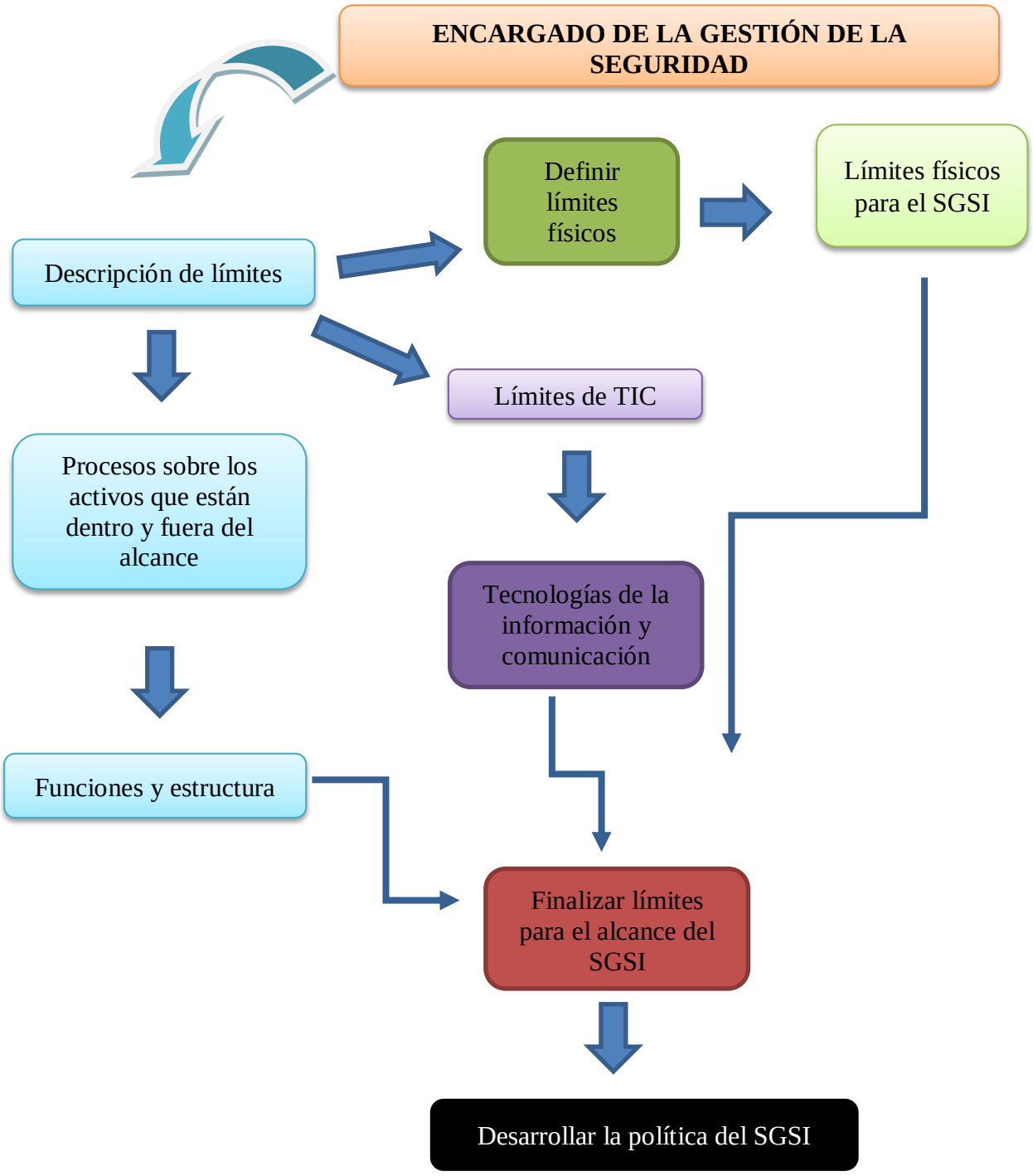
Trabajar con un servidor o realizar una configuración en red para evitar pérdidas de información.

Definir roles para cada uno de los empleados, identificando a los responsables del manejo de la información.

3.2. Definir alcance y política de un SGSI

Una vez obtenida la aprobación general para llevar a cabo el SGSI se deberá realizar la definición de alcances y política del SGSI

Figura Nº5 Flujograma de fase 2



El encargado deberá determinar los límites de la firma apoyándose con el formulario denominado “límites de la firma de auditoría”:

PROCEDIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN				
TÍTULO: LIMITES DE LA FIRMA DE AUDITORÍA				
Niveles / **Parámetros de medición**	**Nulo**	**Bajo**	**Medio**	**Alto**
Protección de antivirus		X		
Seguridad de vigilantes	X			
Encriptación de información	X			
Codificación de accesos y permisos hardware	X			
Codificación de accesos y permisos software	X			
Restricción de acceso a internet	X			
Modificación de información solo mediante personal autorizado	X			
Actualizaciones del sistema operativo		X		
Restricción de accesos a programas y archivos	X			
Mantenimiento de equipos		X		
Mantenimiento de infraestructura e instalaciones		X		
Mantenimiento de servidor de red	X			
Mantenimiento de red inalámbrica		X		

Estructura de la firma de auditoría

Para definir cuál es la estructura que la firma posee se deberá completar el formulario siguiente:

ESTRUCTURA DE LA FIRMA			
PROCEDIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN			
ÁREA:		FECHA:	14-07-16
SOLICITADO POR:	Lic. Marvin Díaz	AUTORIZADO POR:	Lic. Antonio Jovel
REVISADO POR:	Licda. Raquel Girón		
APROBADO POR:	Licda. Raquel Girón	FECHA:	15-07-16
OBSERVACIONES O COMENTARIOS:			

	Nombre del empleado	Rol	Descripción	% Responsabilidad de la información de la firma
1	Antonio Jovel	Vela por los intereses	Gte. Gral	0%
2	Raquel Girón	Controla la Operación	Gte. de Auditoría	20%
3	Marvin Díaz	Supervisa el cumplimiento	Supervisor	20%
4	Samuel Alvarado	Prepara las auditorías	Aud. Senior	60%
5	Carlos Novoa	Prepara las auditorías	Aud. Senior	60%
6	Cecilia Navas	Apoya con las auditorías	Aud. Junior	20%
7	Alice Martínez	Apoya con las auditorías	Aud. Junior	20%
8	Federico Argueta	Apoya con las auditorías	Aud. Junior	20%
9	Andrea Rivas	Apoya con las auditorías	Aud. Junior	20%

Al tener definida la parte organizacional se deberá analizar las Tecnologías de la Información y Comunicación (TIC), iniciando con un registro de los procesos tecnológicos que se llevan a cabo en la firma ya sea a raíz de problemas o por mantenimiento, con el formato siguiente:

PROCEDIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
Bitácora de descripción de procesos tecnológicos		
FECHA	**DESCRIPCIÓN**	**SOLUCIÓN**

Donde la fecha será la del día del proceso, la descripción porque se dio el proceso tecnológico como reparaciones, instalaciones, entre otros, que solución se le aplicó y quien lo realizó lo anterior para conocer cuáles son los procesos que se llevan a cabo en la firma y las principales razones, para definir las características y límites de las TIC.

Sin embargo en H.L.H. y CIA, S.A. no se posee un control de estos procesos debido a que son eventuales y poco regulares. A continuación del estudio de las TIC, se puede determinar el alcance del SGSI en la firma de auditoría, con base al siguiente procedimiento:

PROCEDIMIENTO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

TÍTULO
PROCEDIMIENTO PARA DETERMINAR ALCANCE DEL SGSI EN LA FIRMA DE AUDITORÍA

Objetivo:
Establecer una metodología planificada y sistemática para el seguimiento de la aplicación de la Política de la seguridad

Alcance: Esta instrucción será aplicable a la definición y seguimiento de los objetivos de seguridad de la firma.

DESCRIPCIÓN:
El siguiente procedimiento describirá la forma de elaborar un alcance y objetivo del Sistema de Gestión de seguridad de la Información (SGSI).
Las fuentes del Objetivo y alance del SGSI pueden ser emanadas de cualquiera de los encargados de la información con respaldo de la Gerencia General en los casos de las firmas con calidad jurídica y por el propietario de las firmas naturales (en el caso que tenga empleados) sino bastará solo con su revisión, en las jurídicas deberán ser revisados y aprobados por el encargado de Gestión de Seguridad, estos deberán ser coherentes con la Política de seguridad.

Los objetivos y alcance de la seguridad deberán cumplir las siguientes premisas: Medibles, específicos y realistas.
El formulario de "objetivo y alcance de seguridad" se estructurarán de la siguiente manera:

1. **Punto relacionado de la Política de Seguridad:** en este campo se especifica la relación que tiene el objetivo con la política de seguridad, es decir hacia qué punto de ésta última va orientado.
2. **Orientación del Objetivo:** especificación del origen del objetivo a desarrollar:
   - "Mejora Continua", algo ya implantado, del cual surge un cambio sustantivo en lo especificado, pueden ser determinadas por todos los sectores de la Organización.
   - "Diseño y Desarrollo", es un proyecto nuevo que surge por las necesidades empresariales.
3. **Objetivo:** Definición temática del proceso o sistema a mejorar incluyendo las característica a alcanzar.
4. **Acciones:** es la descripción de las acciones a tomar para el desarrollo del Objetivo y alcance de seguridad, estableciendo Metas de Ejecución con la especificación de las áreas que la generaran y la fecha tope de realización; se deberá determinar la fecha Final / límite de finalización de cada meta.

Como estrategia de seguimiento y control se deberá dar seguimiento dentro del plazo en que se defina el cumplimiento de las acciones establecidas, el responsable será el encargado de gestión de la seguridad.

OBJETIVO Y ALCANCE DE SEGURIDAD			
PROCEDIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN			
ÁREA:		FECHA:	14/07/16
SOLICITADO POR:	Lic. Marvin Díaz	AUTORIZADO POR:	
REVISADO POR:	Licda. Raquel Girón	Lic. Antonio Jovel	
APROBADO POR:	Licda. Raquel Girón	FECHA	15/07/16
OBSERVACIONES O COMENTARIOS:			

PUNTO RELACIONADO CON LA POLITICA DE SEGURIDAD

El punto principal objetivo que se deberá relacionar con la política de seguridad es el refuerzo y mejoramiento de la protección de la información

ORIENTACION DEL OBJETIVO

Implementar el diseño de la fase 5, dándole mantenimiento continuo y seguimiento permanente.

OBJETIVO

Implementar un modelo de SGSI que mejore los procesos de seguridad de la firma y de la información que en ella se maneja.
Reforzar la protección de la documentación, datos y archivos tanto físicos como digitales.

ACCIONES

Creación de usuarios y contraseñas para el uso del sistema.
Configuración y conexión de computadoras en red, con respaldo en un servidor en una nube
Compra de licencias de antivirus privadas
Restricción de acceso a internet
Creación de correo institucional
Refuerzo y mantenimiento de las instalaciones
Compra de caja de seguridad para resguardo de documentación física.

Teniendo definidos los objetivos y alcances pasamos a crear la política de seguridad:

Procedimiento del Sistema de gestión de seguridad de la información
Título Política de seguridad y custodia de documentos
Objetivo: Establecer un procedimiento para la seguridad y custodia de la documentación física y digital. Alcance: toda la documentación generada del proceso de auditoría. **Descripción:** Las políticas generales que se describen a continuación, se refiere al proceso de seguridad y custodia de documentación física y digital, generada por los diferentes procesos. la descripción del procedimiento es el siguiente: Se establecerán contraseñas de seguridad para ingreso a las computadoras asignadas y en ellas también para el sistema de auditoría, los archivos con información digital deberán ser guardados en el disco duro con copia de respaldo en una carpeta asignada en red y en la nube. Con la información física se llevara un control de entrada y salida de información, cualquiera que quiera solicitar expedientes u otro documento físico resguardado deberá completar el formulario de "solicitud de información clasificada" para tener acceso, el resguardo de la misma deberá ser en un lugar seguro que cumpla las medidas de seguridad necesarias en cuanto infraestructura como seguridad. Todos los empleados deberán informar de cualquier anomalía o pérdida con la información física ó digital, para generar la recuperación a través de la nube. Los dispositivos extraíbles como USB los deberá proporcionar la firma y será la encargada de resguardarlos en un espacio con acceso restringido, preferiblemente una caja fuerte donde solo la alta gerencia tenga acceso (General y Auditoría), y será registrado con el siguiente formato:

PROCEDIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN												
POLITICA DE SEGURIDAD DE INFORMÁTICA												
FORMULARIO DE CONTROL DE TRASLADO DE DISPOSITIVOS DE BACK-UP HACIA CAJA DE SEGURIDAD												
SEMANAS		DIAS DE LA SEMANA							NOMBRE DE QUIEN ENTREGA	FIRMA	NOMBRE DE QUIEN RECIBE	FIRMA
DESDE	HASTA	L	M	M	J	V	S	D				
Revisado por:												
Autorizado por:												

Se deberá realizar la compra de antivirus para ser instalado en todas las computadoras, solicitando a la entidad subcontratada del mantenimiento y soporte que los instale, al mismo tiempo deberá restringir el acceso a Internet limitándolo a los sitios web relacionados con la firma.

Se deberá solicitar la creación e instalación de un correo empresarial con un formato similar para todos los empleados, con autorización de entradas y salidas de correos electrónicos, requiriendo al proveedor de este servicio proporcione mantenimiento periódico constante para dar fe del buen funcionamiento de este.

Los requerimientos de información física se podrán realizar por correo electrónico siempre y cuando sean encriptados, para este mismo fin se deberá contratar a una persona que sea la

designada para trasladar la información personalmente y de forma oficial; en la firma solamente quien requirió la información podrá recibirla e inmediatamente se convertirá en el responsable de la misma y será el obligado de realizar un respaldo y resguardo adecuado de la misma.

Se deberá realizar un inventario físico de los activos de tecnología y comunicaciones que se tienen en la firma por lo menos una vez al año esto como parte de la seguridad para llevar un registro de los accesos que posee y los datos principales, por lo que se sugiere el siguiente formulario para ello:

FORMULARIO DE MOVIMIENTOS DE PC Y ACCESOS ESPECIALES					
Nombre	**Locación**	**Motivo de cambio de área**	**Dirección IP**	**Correo Internet**	**Navegar en Internet**
Revisado por:					
Autorizado por:					

Finalmente para controlar el recurso humano se deberán establecer compromisos de confidencialidad con todo el personal con el formato siguiente:

PROCEDIMIENTO DEL
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

TÍTULO
CONTRATO DE CONFIDENCIALIDAD

El objetivo de garantizar la confidencialidad del presente proyecto _____ en colaboración entre las partes implicadas, se hace necesario la firma de un acuerdo que garantice unos niveles de confianza entre las partes.

I PARTE

_____ _____

Nombre de la firma de auditoría Nombre del apoderado de la firma

II PARTE

_____

Nombre del empleado

REUNIDOS EN _____ EL DIA_____DE_____ DEL_____

EXPONEN:

Que las partes involucradas, están interesadas en desarrollar el presente contrato para llegar al acuerdo de confidencialidad con el fin de custodiar y no transmitir a terceros la información recolectada de los clientes, así mismo la que es propia de la firma. Las partes se consideran responsabilidad y obligaciones inherentes, siempre y cuando dé lugar a las normativas aplicables vigentes para efectos de este contrato.

Este acuerdo no autoriza a ninguna de las partes a solicitar o exigir de la otra parte el suministro de información, y cualquier otro tipo de acción, ya que los datos se consideran secretos, confidenciales o restringidos.

Se anexan otros acuerdos y definiciones a este contrato de confidencialidad.

_____ _____

_ Firma

Firma representante _____ representante_____

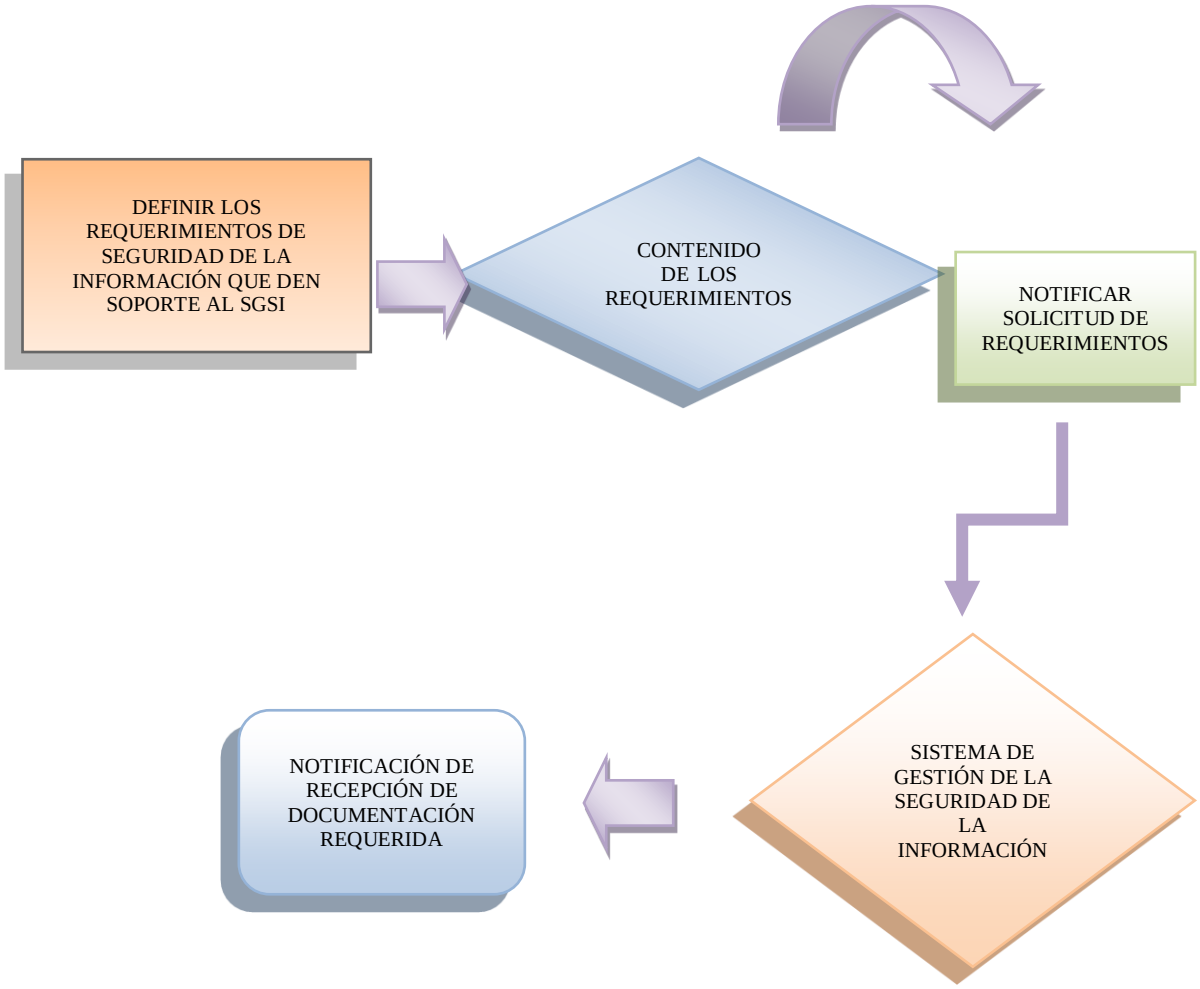
DUI representante_____ DUI representante_____

SELLO

3.3 Definir requerimientos de seguridad de la información

Al tener definidos los objetivos, alcance y la política de seguridad de la información, pasamos a establecer los requerimientos que le darán soporte al SGSI.

Figura Nº6 Flujograma de fase 3



Se inicia definiendo las funciones y el acceso que tiene a la información cada auditor (es) que integra(n) la firma, al momento de realizar un encargo:

<table>
<tr><th colspan="2">PROCEDIMIENTO DEL
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</th></tr>
<tr><th colspan="2">TÍTULO: LISTADO DE FUNCIONES DE CADA AUDITOR</th></tr>
<tr><td colspan="2">GERENCIA DE AUDITORÍA: se encarga de distribuir encargos al personal adecuado para el desarrollo de encargos, ya que autoriza cada movimiento del equipo de trabajo.</td></tr>
<tr><td>FUNCION</td><td>ACCESO DISPONIBLE</td></tr>
<tr><td>Verificar datos confidenciales del cliente</td><td rowspan="3">Sistema de auditoría, toda la documentación y acceso a las computadoras de los seniors y juniors</td></tr>
<tr><td>Recopilar información adecuada y suficiente para cumplir con el encargo.</td></tr>
<tr><td>Denunciar en caso de descubrir un fraude.</td></tr>
<tr><td colspan="2">SUPERVISOR: su misión es velar por el buen cumplimiento de los procesos, políticas y direcciones de los encargos de auditoría.</td></tr>
<tr><td>FUNCION</td><td>ACCESO DISPONIBLE</td></tr>
<tr><td>Verificar datos confidenciales del cliente</td><td rowspan="3">Sistema de auditoría, toda la documentación y acceso a las computadoras de los seniors y juniors</td></tr>
<tr><td>Recopilar información adecuada y suficiente para cumplir con el encargo.</td></tr>
<tr><td>Denunciar en caso de descubrir un fraude.</td></tr>
<tr><td colspan="2">ASISTENTE SENIOR: su función es como referirse a un técnico ya que es indispensable; con su ayuda se pueden colaborar en retos que resulten más desafiantes, como la recopilación de evidencia, para considerarse en este puesto, debe tener como mínimo 6 años de experiencia.</td></tr>
<tr><td>FUNCIÓN</td><td>ACCESO DISPONIBLE</td></tr>
<tr><td>Verificar datos confidenciales del cliente</td><td rowspan="3">Sistema de auditoría, toda la documentación del encargo asignado</td></tr>
<tr><td>Recopilar información adecuada y suficiente para cumplir con el encargo</td></tr>
<tr><td>Denunciar en caso de descubrir un fraude</td></tr>
<tr><td colspan="2">ASISTENTE JUNIOR: es un colaborador que tiene alrededor de 2 años de experiencia en el área de auditoría, aunque no conoce todos los estándares, su colaboración con el auditor senior determina la eficacia con que se logre terminar el encargo.</td></tr>
<tr><td>FUNCIÓN</td><td>ACCESO DISPONIBLE</td></tr>
<tr><td>Verificar datos confidenciales del cliente</td><td rowspan="3">Sistema de auditoría, toda la documentación del encargo asignado</td></tr>
<tr><td>Recopilar información adecuada y suficiente para cumplir con el encargo</td></tr>
<tr><td>Denunciar en caso de descubrir un fraude</td></tr>
</table>

Se deben establecer contratos para cada uno de los empleados de la firma, sino se poseen se brinda el siguiente formato:

PROCEDIMIENTO DEL
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

TÍTULO
CONTRATOS PARA EMPLEADOS DE LA FIRMA DE AUDITORÍA

Nombre completo_____
Edad_____ fecha de nacimiento_____ Estado civil_____
Nacionalidad _____Encargado de trabajo contratado(a):_____
Domicilio_____
DUI_____ NIT_____

_____
(RAZÓN SOCIAL O NOMBRE DEL PATRONO)

_____
(NOMBRE DEL CONTRATANTE PATRONAL)

De las generales arriba indicadas que aparece expresado, convenimos en celebrar el presente contrato individual de trabajo sujeto a las estipulaciones siguientes:

A) clase de trabajo

El trabajador se obliga a prestar sus servicios al patrono como_____

Además de las obligaciones que le impongan las leyes y reglamentos vigentes, tendrá como obligaciones propias de su cargo las siguientes:_____

_____

B) duración del contrato y tiempo de servicio:_____

_____ _____
(firma del contratado) (firma del contratante)

Sello

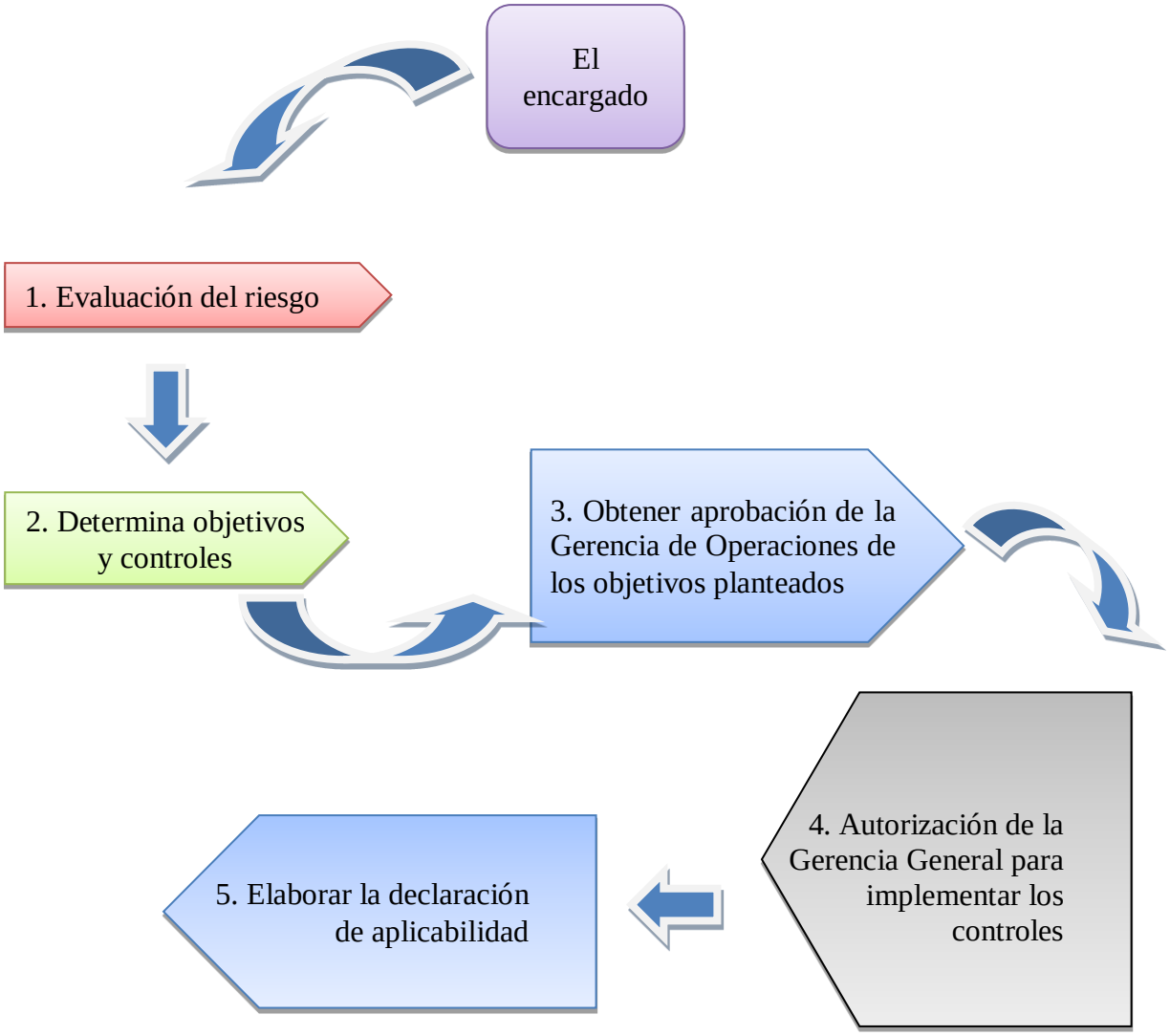
La firma deberá definir un procedimiento de su o sus procesos como el que se muestra a continuación:

PROCEDIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
TÍTULO PROCESOS DE LA FIRMA DE AUDITORÍA
Al momento de adquirir la información de una entidad para realizar el encargo de auditoría, los profesionales deben realizar: Evaluación continua del sistema de control de calidad que sus empleados realizan, así como proporcionar seminarios sobre las normas y requisitos que avalan los procedimientos. - Se deben controlar los informes que realicen los socios de la organización para verificar que estos hayan sido planeados de acuerdo a los estándares establecidos por la gerencia. - Se realizara una inspección al azar para establecer acciones correcticas apropiadas, si estas se consideran necesarias. - Se comunicará a los socios del trabajo sobre los resultados de dicha evaluación para realizar mejoras y/o cambio de estrategia para dichos procedimientos. El cliente podrá hacer cualquier pregunta relativa a su actividad comercial: - Dependiendo de la consulta del auditado se podrá atender por escrito, presencial u otra forma que quedara a criterio profesional del auditor Se nombrara un responsable para cada encargo a desarrollar, así como su personal de trabajo.

PLANEACIÓN	EJECUCIÓN	INFORME DE RESULTADOS	SEGUIMIENTO
Investigación preliminar	Inicio de auditoría	Oficio de envío	Dependerá del nivel de revisión que el auditor realiza
Cronograma de actividades	Acta de inicio	Caratula del informe	Pueden suceder dos circunstancias: - Inquirir en la situación actual
Carta de planeación	Examen y evaluación del sistema de control interno	Índice	- Revisión técnica del sistema
	Planeación detallada	Cuerpo de informe	
	Ejecución del trabajo	Cedulas de observaciones	
REVISADO POR:			
AUTORIZADO POR:			

3.4 Realizar una evaluación del riesgo y seleccionar opciones de tratamiento del riesgo

Figura Nº7 Flujograma de fase 4



Cuando el encargado de la gestión de la seguridad en la firma ha cumplido con la revisión organizacional determinando objetivos, alcances y requerimientos es el momento de realizar la evaluación del riesgo en la firma para lo cual se deberá completar el siguiente formulario:

EVALUACIÓN DE RIESGOS
PROCEDIMIENTO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN **RESPONSABLE: Lic. Marvin Díaz** **FECHA:** 14/07/16 **ÁREA** _____ **SOLICITADO POR:** Lic. Marvin Díaz **AUTORIZADO POR:** Lic. Antonio Jovel **OBSERVACIONES: Ninguna**
APROBADO POR: Licda. Raquel Girón
FORTALEZAS DE LA FIRMA • Activos de Tecnología Avanzado • Buena estructura organizacional • Utilización de Software Privado • Sólido Prestigio
OPORTUNIDADES DE LA FIRMA
• Invertir en renovación continua de tecnología • Capacitaciones para el personal en temas de seguridad informática • Compra o contratación de un servidor de datos o nube privada • Contratación de vigilancia de los bienes de la firma y la documentación
DEBILIDADES DE LA FIRMA
• Carencia de conocimientos informativos de seguridad • Utilización de cuentas de correo comercial • La firma no cuenta con vigilancia dentro o fuera • El personal no recibe capacitación continua de temas relacionados a tecnología • Falta de control en trabajos de campo
AMENAZAS DE LA FIRMA
• Pérdida o fuga de información • Amenazas de virus electrónicos • Fraude o plagio por falta de seguridad • Robo • Peligro de incendio por fallas eléctricas
ALCANCE DE LA EVALUACIÓN
Esta evaluación pretende alcanzar todas las áreas de la compañía, incluyendo la gerencia general.
METODOLOGIA DE LA EVALUACIÓN:
El método a utilizar será el analítico y con base a los resultados se iniciará el proceso de determinación de controles y procesos que minimicen la ocurrencia del riesgo. La parte que resta lo llamaremos riesgo residual el cual no deberá ser significativo aunque sucediera.

Cuando el encargado ha determinado la metodología es momento de completar el "Formulario de criterios y evaluación del riesgo", para determinar las opciones de tratamiento, estimar cual es el riesgo residual y seleccionar los objetivos de control.

OBJETIVO Y ALCANCE DE SEGURIDAD			
PROCEDIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN			
ÁREA:		FECHA:	14-07-16
SOLICITADO POR:	Marvin Díaz	AUTORIZADO POR: Lic. Antonio Jovel	
REVISADO POR:	Licda. Raquel Girón		
APROBADO POR:	Licda. Raquel Girón	FECHA	15-07-16
OBSERVACIONES Ó COMENTARIOS: Ninguno			
PUNTO RELACIONADO CON LA POLITICA DE SEGURIDAD			
El punto principal del objetivos que se deberá relacionar con la política de seguridad es el refuerzo y mejoramiento de la protección de la información			
ORIENTACION DEL OBJETIVO			
Implementar el diseño de la fase 5, dándole mantenimiento continuo y seguimiento permanente.			
OBJETIVO			
Implementar un modelo de SGSI que mejore los procesos de seguridad de la firma y de la información que en ella se maneja. Reforzar la protección de la documentación, datos y archivos tanto físicos como digitales.			
ACCIONES			
Creación de usuarios y contraseñas para el uso del sistema. Configuración y conexión de computadoras en red, con respaldo en un servidor en una nube Compra de licencias de antivirus privadas Restricción de acceso a internet Creación de correo institucional Refuerzo y mantenimiento de las instalaciones Compra de caja de seguridad para resguardo de documentación física.			

Habiendo establecido los resultados del riesgo es oportuno crear los objetivos y controles contra el riesgo evaluado.

CRITERIO Y RESULTADO DE LA EVALUACIÓN DEL RIESGO			
PROCEDIMIENTO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN			
ÁREA:		FECHA:	14/07/2016
SOLICITADO POR:	Lic. Marvin Díaz	AUTORIZADO POR:	
REVISADO POR:	Licda. Raquel Girón	Lic. Antonio Jovel	
APROBADO POR:	Licda. Raquel Girón	FECHA	15/07/2016

OBSERVACIONES Ó COMENTARIOS: Ninguno

	RIESGO ENCONTRADO	PROBABILIDAD		
		BAJO	**MEDIO**	**ALTO**
1	Carencia de conocimientos de seguridad informática		X	
2	Perdida ó fuga de información			X
3	Fraude ó plagio	X		
4	Virus			X
5	Incendio por corto circuito		X	
6	Inundaciones		X	
7	Divulgación de la información			X
8	Robo			X
9	Fallo de las computadores por choques eléctricos			X
	TOTALES	1	3	5

RESULTADO DEL RIESGO

Hay una alta probabilidad que el riesgo suceda, por lo que es necesario realizar implementación de controles y aplicación de objetivos que minimicen esta posibilidad, asegurando de manera adecuada la información de la firma así como las instalaciones físicas.

ACEPTACIÓN/ RECHAZO DEL RIESGO

A pesar que la probabilidad es alta, el riesgo es aceptable ya que existen controles que lo mejorarán hasta casi extinguirlo.

Para finalizar esta etapa se deberá preparar una declaración de aplicabilidad del SGSI y esta deberá ser aprobada y autorizada por la Gerencia General y Operativa.

DECLARACIÓN DE APLICABILIDAD			
Descripción	**Aplica**		**Registro de implementación**
POLITICAS DE SEGURIDAD			
Documento de la política de seguridad de la información.	Si	Tiene una aplicabilidad en todo el SGSI y la firma	Documento de política firmado por la Gerencia General y la Gerencia de Auditoría
Revisión de la política de seguridad de la información.	Si	De manera periódica se debe realizar la revisión y documentar las acciones de mejora	Actas de revisión periódica
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			
Compromiso de la dirección con la seguridad de la información	Si	Es fundamental, dado que tienen la responsabilidad de aprobar el SGSI.	Acta firmada por la Gerencia General y la de Auditoría.
Coordinación de la seguridad de la información.	Si	Debe designar un encargado que lidere la implementación del SGSI	La gerencia de auditoría lo definirá
Acuerdos sobre confidencialidad	Si	La información es fundamental en la firma por lo que hay que velar por su protección	Contratos de confidencialidad entre la firma y los empleados
Consideraciones de la seguridad cuando se trata con los clientes	Si	Por ser una firma de auditoría, es fundamental obtener valor agregado en la misma y generar una mayor confianza al cliente, por ello se debe fortalecer la seguridad que la información se está manejando correctamente	Las ofertas técnicas y económicas llevaran una clausula con la información necesaria para darle seguridad al cliente
GESTIÓN DE ACTIVOS			
Inventario de activos	Si	Para una adecuada gestión de riesgos y tratamiento de estos, es necesario conocer los activos de información que se tienen.	Listado con activos de información

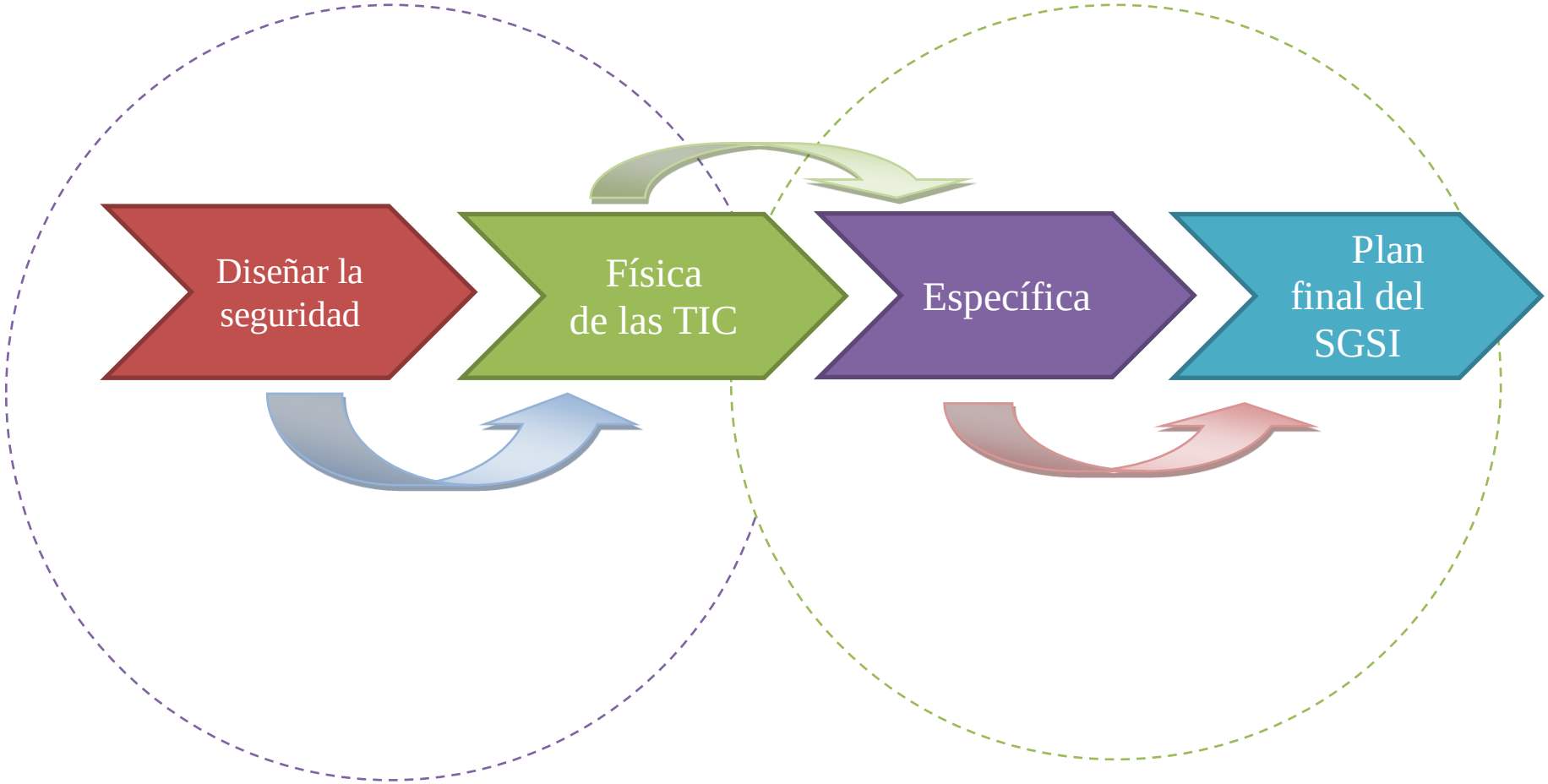
Propiedad de los activos	Si	Cada activo de información debe tener un responsable	Listado con activos de información con responsable
Etiquetado y manejo de información	Si	La información debe protegerse acorde a su criticidad, por ello es necesario clasificarla	Documento con los niveles de clasificación y procedimiento para etiquetado
SEGURIDAD DE LOS RECURSOS HUMANOS			
Roles y responsabilidades	Si	A las áreas deben asociarse las responsabilidades frente al SGSI.	Nuevo formulario de estructura organizativa asignado los nuevos roles y niveles de responsabilidad
Términos y condiciones laborales	Si	Todas las acciones permitidas dentro y fuera de la firma, así como las obligaciones y restricciones	Contrato de ingreso
Educación, formación y concientización sobre la seguridad de la información	Si	Ser competitivos es de gran importancia para la implementación y mantenimiento del SGSI, esto implica tener planes de capacitación frente a los temas de seguridad	Plan de capacitación o registros de participación.
SEGURIDAD FÍSICA Y AMBIENTAL			
Perímetro de seguridad física	Si	Las instalaciones y todos los equipos dentro de la firma y los equipos portátiles	Contratación de seguridad y vigilancia
Controles de acceso físico	Si	Las instalaciones y los lugares que resguardan información	Control de ingresos y salidas
Mantenimiento de los equipos	Si	Todos los equipos de la firma	Contratación de técnicos y plan de programación de mantenimientos
Seguridad de los equipos fuera de las instalaciones	Si	Todos los equipos de la firma	Contratación de pólizas de seguros para la protección de los activos.
GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES			
Documentación de los procedimientos de operación	Si	Todos los procedimientos deben estar documentados.	Documentos y manuales de auditoría

Gestión del cambio	Si	Se debe controlar de manera adecuada los cambios en plataformas y sistemas de información, de modo que se reduzcan los errores operativos	Formularios de solicitud de creaciones y modificaciones de usuarios
Controles contra códigos maliciosos	Si	Se debe controlar de manera adecuada los códigos maliciosos.	Instalación firewall y anti spyware
Respaldo de la información	Si	Ante eventos de seguridad, es necesario contar con *backup* que permitan la recuperación de la información.	Procedimientos para el respaldo de la información en la nube y otros dispositivos; formulario de traslado de back up a caja de seguridad
Controles de las redes	Si	El control de acceso a las redes debe permitir la reducción de los riesgos	Procedimientos para el control de acceso (creación, bloqueo, modificación, aprovisionamiento).
Procedimientos para el manejo de la información	Si	Toda la información debidamente clasificada	Documento con niveles de clasificación y ejecución de planes de sensibilización.
Políticas y procedimientos para el intercambio de la información	Si	Toda la información.	Formularios de entrada y salida de documentación
Mensajería electrónica	Si	Toda la información digital	Contratación de correo empresarial
Registro de auditorías	Si	Periódicamente se realizarán auditorías para verificar el buen uso y manejo de la información	Programación de auditorías e informe.
CONTROL DE ACCESO			
Registro de usuarios	Si	Todos los empleados de la firma que tengan acceso al sistema informático	Formulario de creación y modificación de usuarios
Gestión de contraseñas para usuario	Si	Todos los empleados de la firma que tengan acceso al sistema informático	Formulario de creación y modificación de usuarios
Uso de contraseñas	Si	Todos los empleados de la firma que tengan acceso al sistema informático	Formulario de creación y modificación de usuarios, controlada por el encargado del SGSI
Restricción de acceso a la información	Si	Todos los empleados de la firma que tengan acceso al sistema informático	Los usuarios que posean accesos especiales deberán respaldarlos con el formulario de comunicaciones.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN			
Análisis y especificación de los requisitos de seguridad	Si	Los desarrollos y mantenimiento de sistemas de información son un foco de vulnerabilidades, por ello se les debe dar máxima prioridad en la protección	Complementación con fase 3
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			
Reporte sobre los eventos de seguridad de la información	Si	Fallas en equipos de la firma	Bitácora de descripción de procesos tecnológicos
Responsabilidades y procedimientos	Si	Parte fundamental de la gestión de riesgos es la fuente de incidentes de seguridad y la gestión sobre éstos, por ello se deben reportar adecuadamente	Documento de políticas de seguridad, documento con las responsabilidades de las áreas frente a los incidentes de seguridad.
Recolección de evidencia	Si	Todos los equipos de la firma	Formularios de movimientos de Equipo y accesos especiales
CUMPLIMIENTO			
Identificación de legislación aplicable	Si	Es necesario conocer las reglamentaciones a nivel Nacional e Internacional aplicable para las firmas de auditoría	Detalle de leyes y normas aplicables

3.5.Diseñar el SGSI

Figura Nº8 Flujograma de fase 5



Esta es la etapa final y para el diseño de cómo será el SGSI se deberá realizar una nueva estructuración de los empleados de la firma, asignando nuevos roles y funciones enfocados en la seguridad de la información.

ESTRUCTURA DE LA FIRMA			
PROCEDIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN			
ÁREA:		FECHA:	14-07-16
SOLICITADO POR:	Lic. Marvin Díaz	AUTORIZADO POR:	Lic. Antonio Jovel
REVISADO POR:	Licda. Raquel Girón		
APROBADO POR:	Licda. Raquel Girón	FECHA:	15-07-16
OBSERVACIONES Ó COMENTARIOS:			

Nombre del empleado		**Rol**	**Descripción**	**% Responsabilidad de la información de la firma**
1	Antonio Jovel	Vela por los intereses	Gte. Gral	0%
2	Raquel Girón	Controla la Operación	Gte. de Auditoría	100%
3	Marvin Díaz	Supervisa el cumplimiento	Supervisor	0%
4	Samuel Alvarado	Prepara las auditorías	Aud. Senior	75%
5	Carlos Novoa	Prepara las auditorías	Aud. Senior	75%
6	Cecilia Navas	apoya con las auditorías	Aud. Junior	25%
7	Alice Martínez	apoya con las auditorías	Aud. Junior	25%
8	Federico Argueta	apoya con las auditorías	Aud. Junior	25%
9	Andrea Rivas	apoya con las auditorías	Aud. Junior	25%

Es necesario que quien controle la operación pueda manejar el 100% de la información para poder verificar que se estén cumpliendo los procedimientos y procesos adecuados, los auditores juniors tienen menor presencia y solo controlarán la documentación que el auditor senior les proporcione no podrán solicitar información a los clientes.

Diseño de la seguridad física y de las TIC

La contratación de técnicos que darán mantenimiento a las instalaciones internas como externas, verificación de extintores, goteras, exposiciones al sol, instalaciones eléctricas, cableado entre otras para reducir el riesgo a causa de hechos naturales y cortocircuito.

De igual manera se gestionarán revisiones periódicas de las computadoras y otros equipos de tecnología y comunicación, para mantenimiento preventivo.

Ambas entidades que brinden el servicio a la firma deberán presentar referencias y tener un sólido prestigio, para asegurar que el trabajo a realizar sea de calidad y cumpla con las políticas establecidas en el SGSI.

Adicionalmente se deben comprar licencias de antivirus, firewall y anti spyware para instalar en todas las computadoras y equipos que lo requieran.

Diseñar la seguridad de la información específica del SGSI

Se preparan procedimientos para evitar las fugas y pérdidas de información tales como:

- **Revisión por la Administración:** Este establece que toda la documentación deberá ser revisada y aprobada por la administración.

TÍTULO: REVISIÓN POR LA ADMINISTRACIÓN

Objetivo: Obtener mejoras en la adecuación y eficacia del Sistema de Gestión de Seguridad de la Información a través de revisiones periódicas por parte de la administración de la empresa.

Alcance: Las revisiones alcanzan al Sistema de Gestión de Seguridad de la Información y sus partes constitutivas.

DESCRIPCIÓN:

Como política, la Dirección ha establecido dos metodologías básicas para revisar el funcionamiento del Sistema de Gestión de Seguridad de la información, siendo éstas una reunión anual completa y una revisión mensual parcial como mínimo.

En la revisión mensual, se efectúa una revisión de las desviaciones de los procesos que se efectúan a diario para prestar los servicios. Se evalúa en su totalidad la eficiencia del sistema bajo el cual se brinda el servicio y se da cumplimiento al contrato establecido con los clientes, mediante diversas herramientas y estudio de casos orientados a la mejora continua.

Las diferentes herramientas de medición que utiliza la Administración para conocer si el sistema de gestión de seguridad de la información se encuentra dentro de los niveles establecidos y si está brindando aportes para la mejora:

a) Seguimiento y medición de los procesos.
b) Informe de la prestación del servicio a los clientes
c) Procesos relacionados con el cliente mediante el análisis conjunto de requerimientos escritos, efectuando reuniones adicionales con las Gerencias

Adicionalmente se establece un procedimiento de control de la documentación para evitar fugas de información y/o extravío de la misma.

TÍTULO: CONTROL DE DOCUMENTOS
Objetivo: Gestionar que los documentos que contienen información relativa a los clientes y a los servicios sean convenientemente administrados y distribuidos en la firma. **Alcance**: Esta metodología es aplicable a los documentos técnico operativos, llamados "Documentos Internos" **DESCRIPCIÓN:** Debido a la utilización en la mayoría de los puestos de trabajo de información de los clientes y de la entidad que usa y alimenta la base de datos para la elaboración de informes, análisis de estados financieros, preparación de consultorías y/o asesorías se ha decidido que los documentos de Información se mantengan en resguardados en un lugar seguro el cual tendrá acceso restringido, adicional deberá tener un soporte magnético con disponibilidad de solo lectura en un sistema de red u otros dispositivos. Para la administración de estos documentos se utilizará el concepto de archivos protegidos contra escritura siendo el encargado de Gestión de Seguridad ó la Gerencia General los únicos autorizados a incorporar cambios en ellos. Cuando se haga requerimiento de la documentación física se deberá completar una bitácora de entrada y salida de la documentación, y esto aplica para el ingreso de nueva documentación.

Este procedimiento va de la mano con el "formulario de solicitud de información clasificada" Se entenderá que es toda aquella información que no le corresponda al solicitante tener para su desarrollo laboral.

Esta plantilla o formulario deberá completarse detallando la información a solicitar y el porqué de la solicitud, deberá ser firma por los superiores al solicitante. De igual forma este formulario se utilizará para solicitar la información a los clientes.

SOLICITUD DE INFORMACIÓN CLASIFICADA					
PROCEDIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN					
SOLICITADO POR			FECHA		
REVISADO POR			FECHA		
APROBADO POR			FECHA		
AUTORIZADO			FECHA		
NOTAS:					
FORMATO DE SALIDA	REPORTE FISICO	☐	ARCHIIVO EN EXCEL ☐		ARCHIVO ENCRIPTADO ☐
FORMA DE ENTREGA:	CORREO	☐	USB	☐	CD ☐
CUENTAS DE CORREO ELECTRÓNICO (SI ES POR CORREO):					
DETALLE DE INFORMACIÓN QUE SOLICITA:					

Todos los movimientos de la documentación sin importar en el formato que salga (digital o física) deberán ser registrados en el siguiente formulario, se tendrá un formulario por cada encargo para registrar toda la documentación relacionada a este cliente.

Formulario de bitácora de ingresos y salidas de documentación

MANEJO DE DOCUMENTACIÓN						
PROCEDIMIENTOS DE GESTIÓN DE SEGURIDAD						
ÁREA:		RESPONSABLE:				
SOLICITADO POR:		AUTORIZADO POR:		FECHA:		
OBSERVACIONES:						
APROBADO POR:						
DESCRIPCIÓN DEL DOCUMENTO		ENTRADA	SALIDA	FIRMA ENTREGA	FIRMA RECIBE	FECHA
1						
2						
3						
4						
5						
6						
7						
n..						

Para el control del sistema en la firma de auditoría se deberán establecer los códigos de identificación para cada uno de los usuarios y una clave de acceso, para individualizar las acciones de cada uno por lo que para estos casos se deberá presentar un formulario para realizar cualquier tipo de creaciones o modificaciones de usuarios en el sistema.

CREACIÓN Y ADMINISTRACIÓN DE USUARIOS CON ACCESO A LA BASE DE DATOS						
PROCEDIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN						
SOLICITADO POR:	Lic. Marvin Díaz		**FECHA SOLICITUD**			
REVISADO POR:	Licda. Raquel Girón		**AUTORIZADO:**	Lic. Antonio Jovel		
APROBADO POR:	Licda. Raquel Girón		**FECHA DE AUTORIZACIO N**			
CREACIÓN ☐	**ELIMINACIÓN** ☐		**CAMBIO** ☐	**ACCESO** ☐		
NOMBRES:			**APELLIDOS:**			
USUARIO:			**COD. EMPLEADO**		-	
CAMBIO	**DATO NUEVO**		**DATO ANTERIOR**			
UNIDAD LABORAL	AE ☐ AI☐ CYA☐ CON☐ OTROS☐		AE ☐ AI ☐ CYA ☐ CON ☐ OTROS ☐			
MENÚ DE TRABAJO	Sistema de Auditoría					
PUESTO	Auditor Senior					
PERFIL DE OPERACIÓN	Accesos a lectura y escritura de la información, creación y modificación de reporte, ingreso y egreso de valores.		Esta parte se deberá completar únicamente si la solicitud es por cambio ó acceso			
PIN DE AUTORIZACIÓN	SI ☐	NO ☐				
FIRMA DIGITALIZADA	SI ☐	NO ☐	**HUELLA DIGITAL**	SI ☐	NO ☐	

Dónde:

AE= Auditoría Externa.

AI= Auditoría Interna

CyA= Consultoría y Asesoría

Cuando se requieran accesos especiales se deberá completar el siguiente formulario con previa autorización del superior del solicitante y autorización de la Gerencia General.

Formulario para solicitud de accesos:

SOLICITUD DE COMUNICACIONES			
PROCEDIMIENTO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN			
			FECHA: 17/07/2016
ÁREA	Auditoría Externa	**APROBADO POR:**	Lida. Raquel Girón
SOLICITADO POR:	Cecilia Navas	**AUTORIZADO POR:**	Lic. Carlos Novoa y Lic. Antonio Jovel
REVISADO POR:	Lic. Marvin Díaz		
OBSERVACIONES: Se autorizará acceso restringido a Internet para realización de trámites legales.			

INSTITUCIÓN O EMPRESA QUE SOLICITA		
TIPO DE SOLICITUD	ACCESO A INTERNET	☐
	ACCESO A BASE DE DATOS	☐
	CREACIÓN DE APLICACIONES WEB	☐
	CAMBIOS EN LA RED	☐
	CORREO ELECTRONICO	☐
	OTRO_____	

DESCRIPCIÓN DETALLADA DE SOLICITUD
Se solicita acceso a internet especialmente a las paginas siguientes: www.mh.gob.sv, www.isss.gob.sv, www.gob.sv
JUSTIFICACIÓN
Lo anteriores para presentar declaraciones mensuales y otros trámites de ley

El encargado de la seguridad deberá llevar un control y registro de las revisiones mensuales y anuales realizadas así como se deben la elaboración de auditorías internas ejercidas por un tercero, respaldadas con el procedimiento siguiente:

PROCEDIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
TÍTULO: AUDITORÍAS INTERNAS
DESCRIPCIÓN: Realizar auditorías internas para verificar el sistema de Gestión de Seguridad establecido. Medidas a aplicar en las Auditorías Internas: 1. Las auditorías serán realizadas por auditores capacitados para la actividad de verificar e informar dichos resultados. 2. Las personas que realicen auditorías no tendrán responsabilidades directas sobre los sistemas analizados por ellos. 3. Las auditorías internas se establecerán en un programa anual que contemplará los procesos y los puntos de la norma a ser auditados al menos una vez al año.

FORMULARIO DE CALENDARIZACIÓN DE AUDITORÍAS AÑO: XXXX

ÁREA	**PROCESO**	**MESES**										
		E	F	M	A	M	J	J	A	S	O	N
	AUDITORÍA											
	INFORME											
	VACIADO DE DATOS											
	CIERRE											

4. En caso de ser necesario se elaborará previamente a las auditorías, un *check list* de los puntos a verificar, tomando como base toda la documentación disponible referente a la actividad a auditar.
5. Con los resultados de cada Auditoría se redactará un informe que contenga al menos la siguiente información:

• Área a auditar	• Auditor responsable del área.
• Equipo auditor	• Fecha de la auditoría
• Procedimientos relacionados.	• Puntos a Auditar

Los registros de las auditorías internas se realizarán bajo el siguiente formulario:

INFORME DE AUDITORÍA INTERNA, DEL SISTEMA DE GESTIÓN DE SEGURIDAD N°0 /0000						
PROCESO		EQUIPO AUDITOR				
ÁREA						
PROCEDIMIENTOS A VERIFICAR		POSICIÓN		FECHA DE AUDITORÍA		
				DIA	MES	AÑO
Estado del Sistema de Seguridad en general:						
Aspectos Auditados del Sistema de la Calidad en general						
Recursos Humano ☐		Compromiso ☐		Materiales y Equipo ☐		
Política ☐		Usuarios ☐		Proveedores ☐		
Cliente ☐		Procedimientos ☐		Planificación eficiente ☐		

6. La numeración de los informes de auditoría será la misma para todos los años, lo que significa que cada año iniciaran con el informe AI 001, la única diferencia será el año de emisión de éstos
7. Una vez efectuado el Informe de auditoría, este deberá ser firmado por el auditor Representante del Sistema de Gestión de Seguridad y luego ser comunicado al área o áreas correspondientes conteniendo firma de notificado.
8. El auditor interno dará un plazo para realizar las mejoras de los procesos encontrados con fallas lo cual está determinado en el documento o informe final, una vez corregidas las observaciones se dará por finalizada la auditoría.

Para finalizar el diseño se deberá completar el formulario siguiente para respaldar la aceptación de la implementación del sistema de gestión de seguridad de la información, donde se detalle el plan final, la justificación, la versión y las áreas de aplicabilidad, como se desarrollará y las capacitaciones que se brindarán.

Será la alta gerencia ó la administración quien autorizará y aprobará este procedimiento de control.

ACEPTACIÓN DE PROYECTO DE IMPLEMENTACIÓN DEL SGSI				
PROCEDIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD				
REVISADO POR:	Licda. Raquel Girón	FECHA: 19/07/2016	AUTORIZA	
APROBADO POR:	Licda. Raquel Girón	FECHA: 19/07/2016	Lic. Antonio Jovel	FECHA 20/07/2016
Planteamiento				
Implementación del modelo de gestión de seguridad de la información para firmas de auditoría externa, que incluya procedimientos debidos para el resguardo y manejo de información, así como el registro de modificaciones, creaciones y solicitudes de información, usuarios y accesos.				
Justificación				
Con base al estudio realizado sobre los alcances y límites que posee la firma de auditoría se elabora un proyecto de modelo de sistema de gestión de seguridad de la información que ayuda a mejorar los procesos actuales y cree controles para dar mayor seguridad a la información tanto de la firma como de los clientes.				
NOMBRE	Modelo de sistema de gestión de seguridad de la información para las firmas de auditoría			
VERSIÓN	1			
ÁREAS RELACIONADAS				
DESARROLLO				
El desarrollo será llevado a cabo por el personal que la firma asigne como departamento de gestión de seguridad, que será el mismo que velará por el cumplimiento de los procesos y controles, así como el seguimiento a través de auditorías internas periódicamente.				
CAPACITACIÓN				
FECHA: (una vez aprobado el proyecto)		**CAPACITADOR: (Encargado de gestión de seguridad)**		**CAPACITADO: toda la firma**
OBSERVACIONES:				

Se deberán establecer capacitaciones para todo el personal de la firma que se programaran periódicamente para reforzar los conocimientos el registro de estas se realizará con el siguiente formulario:

FORMULARIO DE SOLICITUD Y REGISTRO DE LA CAPACITACIÓN					
A. Información general de la solicitud de capacitación:					
Nombre de la capacitación solicitada:	Sistema de Gestión de Seguridad de la Información				
Persona que solicita capacitación:					
Capacitación solicitada para el área:					
Lugar y fecha a impartir la capacitación:					
Fecha Inicial	Fecha Final	Teoría	Practica	Ubicación	Responsable
Tipo de la capacitación:	Ingreso ☐	Orientada al Desarrollo Humano ☐		Refuerzo☐	
☐	Nuevo ingreso	☐	Solicitud de Instituciones		
☐	Rotación	☐	Sugerencias de usuarios/personal		
☐	Evaluación	☐	Plan de Capacitación		
☐	Documentos de Mejora	☐	Sistema de Gestión de Calidad		
☐	Modificaciones de procesos	☐	Sistema de Salud y Seguridad Ocupacional		
☐	Nuevos procesos/equipos	☐	Otros:		
La capacitación se impartirá: Completa ☐ Parcial ☐					
GUIAS EXISTENTES					
Código de la Guía: ISO/IEC 27001:2011			Temas a seleccionar: TODOS		
Objetivo de la capacitación: Que el personal de la firma comprenda los Sistemas de Gestión de Seguridad de la Información y su aplicación.					
B. Medición posterior de la capacitación (basándose en los resultados esperados)					
Fecha de Seguimiento:		Responsables del seguimiento			
Medio a utilizar para el seguimiento:					
Mediante formularios de pregunta-respuesta personal	☐				
Mediante producción y seguimiento de la medición mensual de los estándares de calidad	☐				
Otros, especifique	☐				
Firma de autorizado:					

Estas capacitaciones deberán ser recibidas por todos los miembros de la firma y otorgadas por una entidad competente para ellos, además el encargado de la gestión de seguridad deberá dar seguimiento al cumplimiento de lo brindado en cada capacitación.

CAPÍTULO IV CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

La información es el activo más importante de una organización y en las firmas de auditoría con mucha más razón ya que se encuentra documentación propia y de terceros que es de suma confidencialidad e importancia y se debe velar que ésta se encuentre completa y disponible para cuando sea necesario, el presente trabajo sirvió para conocer como los profesionales de la contaduría pública que ejercen la auditoría externa protegen y resguardan la información, de donde se pudieron determinar varios factores que están afectando las acciones para realizar un buen manejo de la misma, lo cuál puede ser reforzado con la implementación de un modelo de sistema de gestión de la seguridad de la información, creado con base a la ISO 27001 y 27003. Concluyendo lo siguiente.

- La investigación demuestra que los profesionales de contaduría pública que ejercen la auditoría externa, no poseen sólidos conocimientos sobre los sistemas de gestión de seguridad de la información y que lo poco que conocen en su mayoría ha sido adquirido a través de internet.
- Las firmas de auditoría demuestran que no poseen estrictos sistemas de control para dar la seguridad necesaria a la información y que a pesar de los contratos de confidencialidad con los empleados, la documentación tanto física como digital se encuentra expuesta a pérdida por robo, virus o desastre natural.
- Los profesionales de contaduría pública que ejercen la auditoría externa ya sea en carácter de asociados o personal, poseen auxiliares que se convierten en los encargados de recibir información de los clientes para llevar a cabo la auditoría, por lo tanto debe

haber una definición de roles y responsabilidades para un mayor control de la información.

- Las firmas de auditoría no implementan los procesos de resguardo y protección de la información necesaria al momento de llevar a cabo un encargo, usualmente por falta de recursos o conocimientos de seguridad de la información.

4.2 RECOMENDACIONES

Con base a las conclusiones, se recomienda a los profesionales de contaduría pública que ejercen la auditoría externa lo siguiente:

- Que en las carreras de educación superior relacionadas con la contaduría pública, se incluya enseñanza sobre los SGSI y seguridad de la información; de igual forma se exhorta a las instituciones especializadas en la enseñanza contable que se incluya este tema como parte fundamental de la formación profesional.
- Que adoptando el modelo de SGSI como herramienta de una firma de auditoría optimiza los sistemas de control existente y crea nuevos para dar la seguridad necesaria a la información y al resguardo de la misma, además promueve capacitaciones constantes para los empleados que mejorará la protección por parte del personal, ya que el fin es concientizar la importancia que la información tiene dentro de la empresa y lo que representa la perdida de misma.
- Con la ejecución de un SGSI en las firmas de auditoría ayuda a establecer una estructura jerárquica, definiendo roles y funciones en relación con la información y el manejo de las mismas con el propósito de asegurar la disponibilidad, integridad y confidencialidad de la información.
- Con la propuesta del modelo de SGSI, se pueden mejorar los procesos de resguardo y protección de la información al momento de llevar a cabo un encargo, ya que facilitará los procedimientos a través de formularios donde se registrará cada paso en la manipulación tanto de la información física como digital evitando la elevación de costos y se mantiene la capacitación continua del personal y la gerencia.

BIBLIOGRAFÍA

Acosta F.C. (2009). Modelo de responsabilidad social empresarial (RSE) como una estrategia comunitaria de las firmas de auditoría del área metropolitana de San Salvador. Sam Salvador.

IASB (International Accounting Standars Board). (2009). NIA 120 Marcos de Referencia de las Normas Internacionales de Auditoría.

Interna, I. d. (2009). *Marco para la práctica de la auditoría interna.* San Salvador: Insituto de Auditoría Interna.

ISACA. (2005). *ISO 27001*.

Monge, P. (2006). Aspectos generales de la firma de auditoría y del area metropolitana de San Salvador. San Salvador.

ANEXOS

ÍNDICE DE ANEXOS

ANEXO N° I

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

CUESTIONARIO

DIRIGIDO A: Los encargados del resguardo de la información en las firmas de auditoría conformadas por los Contadores Públicos autorizados por el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría.

OBJETIVO: Obtener información relevante acerca de cómo los profesionales de la contaduría pública que ejercen la auditoría externa, protegen la información física y digital de sus clientes.

INDICACIONES: Marque con una "x" la opción que usted considere conveniente según sea el caso.

1. ¿Cómo está constituida legalmente su firma de auditoría?
    a. Persona natural ☐
    b. Persona jurídica ☐
2. En sus firmas de auditoría, de acuerdo al siguiente listado ¿Qué tipo de servicios realizan? (Puede seleccionar más de una opción)
    a. Auditoría externa ☐
    b. Auditoría fiscal ☐
    c. Auditoría forense ☐
    d. Auditoría interna ☐

e. Auditoría en sistemas ☐

f. Contabilidad ☐

g. Consultoría ☐

h. Asesoría ☐

3. De los siguientes cargos, en el área de auditoría externa ¿Cuáles existen en su firma? (Puede seleccionar más de una opción)

   a. Encargado o gerente de auditoría ☐

   b. Supervisor ☐

   c. Asistente Senior ☐

   d. Asistente Junior ☐

   e. Otra categoría ☐

Especifique _____

4. Dentro de su firma ¿Quién es el responsable para recibir la información de sus clientes, en el momento de realizar el encargo de auditoría? (Puede seleccionar más de una opción)

   a. Encargado o gerente de Auditoría ☐

   b. Supervisor ☐

   c. Asistente Senior ☐

   d. Asistente Junior ☐

   e. Otra categoría ☐

Especifique _____

5. ¿A través de qué medio le solicita o transfieren la información de sus clientes? (Puede seleccionar más de una opción)

    a. Por correo electrónico ☐

    b. Dispositivo extraíble a través de correspondencia ☐

    c. Dispositivo extraíble entregado personalmente ☐

    d. Documentos físicos por correspondencia ☐

    e. Documentos físicos entregados personalmente ☐

6. En su firma de auditoría ¿Qué tipo de actividades realiza para la formación de su personal en cuanto a la seguridad de la información? (Puede seleccionar más de una opción)

    a. Capacitaciones ☐

    b. Seminarios de especialización ☐

    c. Entrenamiento ☐

    d. Ninguna ☐

7. ¿Establecen compromisos de confidencialidad de información, con el personal que trabaja en los encargos de auditoría en la firma?

    Si ☐ No☐

8. ¿Qué tipo de controles realiza para mantener la confidencialidad de la información de los encargos de auditoría en la firma? (Puede seleccionar más de una opción)

    a. Encriptación de la información ☐

    b. Firmas electrónicas ☐

c. Restricción de puertos USB ☐

d. Restricción de Impresiones ☐

e. Codificación de accesos y permisos ☐

f. Restricciones de acceso a internet ☐

g. Acceso solo a correos empresariales ☐

9. Al realizar un trabajo de auditoría ¿Qué dispositivos y/o medios utiliza para el respaldo de la información? (Puede señalar más de una opción)

a. Disco duro ☐

b. Nube ☐

c. USB ☐

d. Correo electrónico ☐

e. Servidores en Red ☐

f. Celulares ☐

g. Tablet ☐

h. otros ☐

10. En su firma de auditoría ¿Qué tipo de controles realiza para conservar la integridad de la información? (Puede seleccionar más de una opción)

a. Modificación solo mediante personal autorizados ☐

b. Criptografía de datos ☐

c. Registro de actividades y eventos ☐

d. Controlar el acceso físico a los equipos y componentes de la red ☐

e. Firma digital ☐

f. Control para resguardo de los dispositivos de almacenamiento ☐

g. Actualizaciones del sistema operativo ☐

h. Firewall o cortafuegos ☐

i. Restricción de accesos a programas y archivos ☐

j. Restricción de ubicación y horario ☐

11. ¿De qué manera se asegura que la información se encuentra completa, ante el riesgo de un siniestro? (Puede señalar más de una opción)

a. Perfectas condiciones de las instalaciones eléctricas ☐

b. Instalar, utilizar y mantener actualizados anti-virus y anti-spyware ☐

c. Servidores de respaldo ☐

d. Servidores en la nube ☐

e. Uso de polarizado en las instalaciones ☐

f. UPS ☐

g. Póliza de Seguro ☐

h. Otros ☐

Especifique: _____

12. De los siguientes métodos seleccione los que utiliza para la protección de los papeles

físicos (Puede señalar más de una opción):

a. Clasificación de acuerdo a confidencialidad y sensibilidad de la información contenida ☐
b. Almacenamiento en lugares de acceso restringido ☐
c. Emisión de autorización previa para el uso y manejo de la información ☐
d. Control por escrito de entradas y salidas de los papeles físicos ☐
e. Mantenimiento de instalaciones ☐

13. ¿Qué tipo de controles realiza para que la información mantenga la disponibilidad adecuada? (Puede seleccionar más de una opción)

a. Respaldo virtual de información ☐
b. Acceso a personal autorizado ☐
c. Plan de contingencia ante fallas de la red ☐
d. Mantenimiento de equipos ☐
e. Mantenimiento de infraestructura e instalaciones ☐
f. Mantenimiento del servidor de red ☐
g. Mantenimiento de la red inalámbrica ☐
h. Mantenimiento de correos electrónicos ☐
i. Mantenimiento del equipo electrónico ☐

14. En su firma de auditoría ¿Ha sufrido alguna pérdida de información física y/o digital? (Si su respuesta es no, continúe en la pregunta 16)

Si ☐ No ☐

15. Del siguiente listado ¿Cuáles han sido las causas de la pérdida de información?

    a. Por robo o hurto ☐
    b. Por virus ☐
    c. Por error humano ☐
    d. Fallas eléctricas ☐
    e. Accidentes, incendios. ☐
    f. Problemas del software ☐
    g. Problemas del hardware ☐

16. ¿Qué haría para recuperar la información de sus clientes si esta se perdiera por causa de un siniestro? (puede seleccionar más de una opción)

    a. Lo recupera con el respaldo almacenado en la Nube ☐
    b. Recuperación por medio de cuenta de correos electrónicos ☐
    c. Resguardo en dispositivos móviles (celulares, Tablet) ☐
    d. Reconstrucción con papeles físicos ☐
    e. Se la solicita al cliente nuevamente ☐
    f. Recuperaría la información a través de un servidor externo ☐
    g. Otra ☐

    Especifique: _____

17. ¿Tiene conocimiento sobre los Sistemas de Gestión de la Seguridad de la Información?

Si conozco ☐ Conozco poco☐ No conozco ☐

18. ¿A través de que medio obtuvo conocimientos de los Sistemas de Gestión de la Seguridad de la Información? (Puede seleccionar más de una opción)

    a. Congresos ☐
    b. Seminarios ☐
    c. Internet ☐
    d. Libros ☐
    e. Folletos ☐
    f. Revistas ☐

19. Sí existiera un Modelo de Sistema de Gestión de la Seguridad de la Información estaría interesado en aplicarlo para mejorar la seguridad de la información de su firma de auditoría y de sus clientes:

    Sí ☐ No☐

¿Por qué?_____

ANALISIS E INTERPRETACION DE RESULTADOS

ANEXO N° II

PREGUNTA Nº1

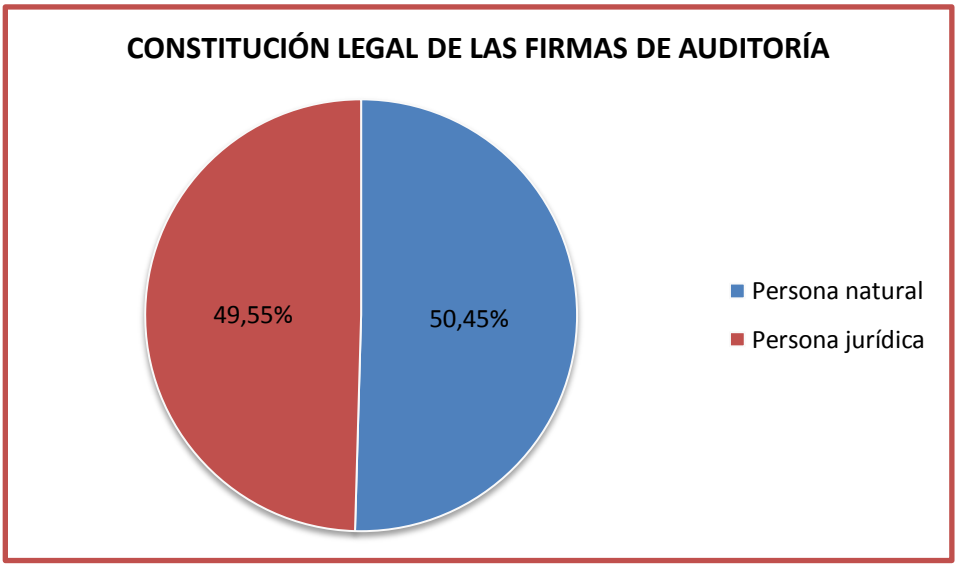
¿Cómo está constituida legalmente su firma de auditoría?

OBJETIVO:

Indagar cual es la constitución legal de las firmas de auditoría encuestadas para así poder estimar la magnitud de la información que se maneja en las misma.

TABULACIÓN

Nº	**Respuesta/variable**	**frecuencia**	
		absoluta	**relativa**
1	Persona natural	56	50,45%
2	Persona jurídica	55	49,55%



ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

De acuerdo al resultado de la encuesta, en la muestra tomada se refleja que existen de forma general un equilibrio en la inscripción de la legalidad entre personas jurídicas con un 49% y naturales con un porcentaje de 50.45%, por consiguiente aunque la magnitud de información varia, se puede determinar que el sistema de gestión de seguridad de la información será realizado para ambos considerando sus oportunidades y a la vez sus limitantes.

PREGUNTA Nº2

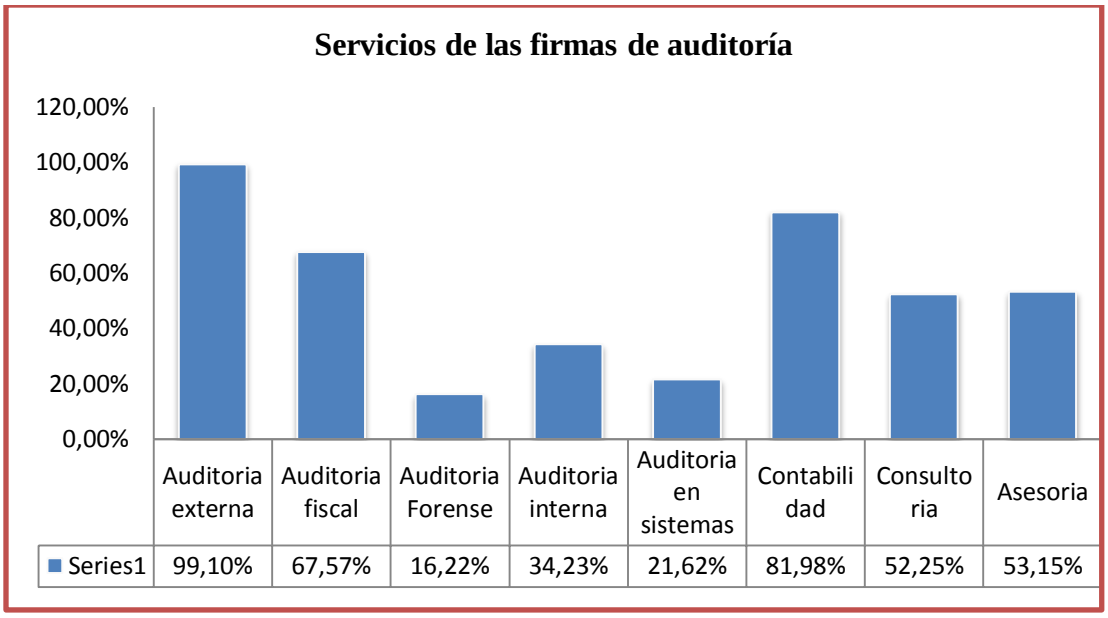
En sus firmas de auditoría, de acuerdo al siguiente listado ¿Qué tipo de servicios realizan? (Puede seleccionar más de una opción)

OBJETIVO

Conocer los servicios que son brindados por las firmas a sus clientes.

TABULACIÓN

Nº	Respuesta/variable	frecuencia	
		absoluta	relativa
a	Auditoría externa	110	99,10%
b	Auditoría fiscal	75	67,57%
c	Auditoría Forense	18	16,22%
d	Auditoría interna	38	34,23%
e	Auditoría en sistemas	24	21,62%
f	Contabilidad	91	81,98%
g	Consultoria	58	52,25%
h	Asesoria	59	53,15%



ANÁLISIS E INTERPRETACION DE LOS RESULTADOS

Las firmas de auditoría prestan sus servicios y con el 99.10% se puede diferenciar que la auditoría externa resulta ser la actividad profesional más común que realizan, seguido por la contabilidad con un 81.98%, auditoría fiscal con un 67.57%, asesoría 53.15%, consultoría 52.25%, auditoría interna 34.23%, auditoría en sistemas 21.62% y finalmente auditoría forense con un 16.22% por lo que la presente investigación resulta apropiada para apoyar a los profesionales y al resguardo de información de terceros y de su propia organización como tal.

PREGUNTA Nº3

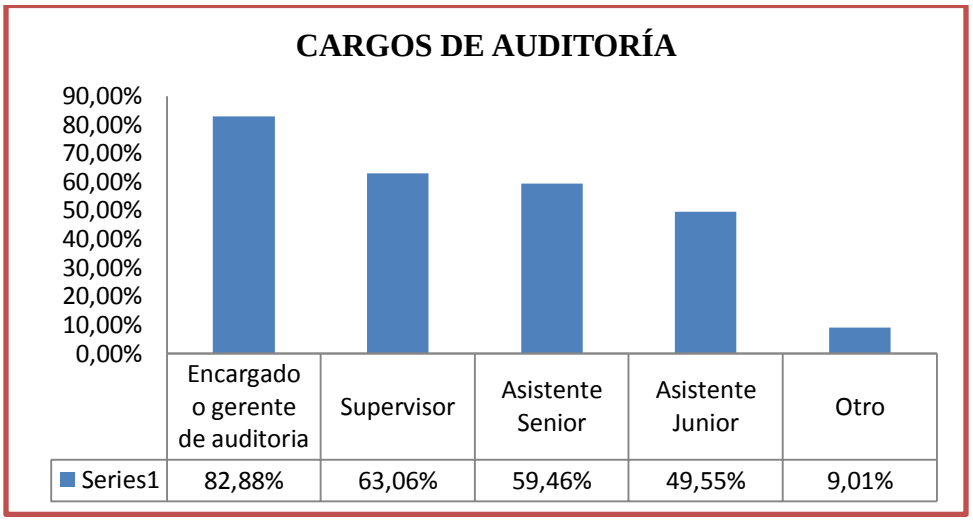
De los siguientes cargos, en el área de auditoría externa ¿Cuáles existen en su firma?

OBJETIVO

Identificar la estructura jerárquica con la que trabajan en las firmas de auditoría para la elaboración de los encargos.

TABULACION

Nº	Respuesta/variable	frecuencia	
		absoluta	relativa
a	Encargado o gerente de auditoría	92	82,88%
b	Supervisor	70	63,06%
c	Asistente Senior	66	59,46%
d	Asistente Junior	55	49,55%
e	Otro	10	9,01%



ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Resulta indispensable conocer la variedad de personal que poseen las firmas de auditoría para considerar sus funciones y su requerimiento para el desarrollo de implementación del modelo en cuestión y según lo observado en el resultado de la tabulación, con un 82.88% predomina que dentro de la organización existe un encargado o gerente de auditoría, seguido con un 63.06% existe un supervisor, con un 59.% asistente senior, con un 49.55% asistente junior y un 9.01% optaron por otro tipo de opciones; de igual forma se puede notar que existe en proporción similar la cantidad de personal en las firmas de auditoría.

PREGUNTA Nº 4

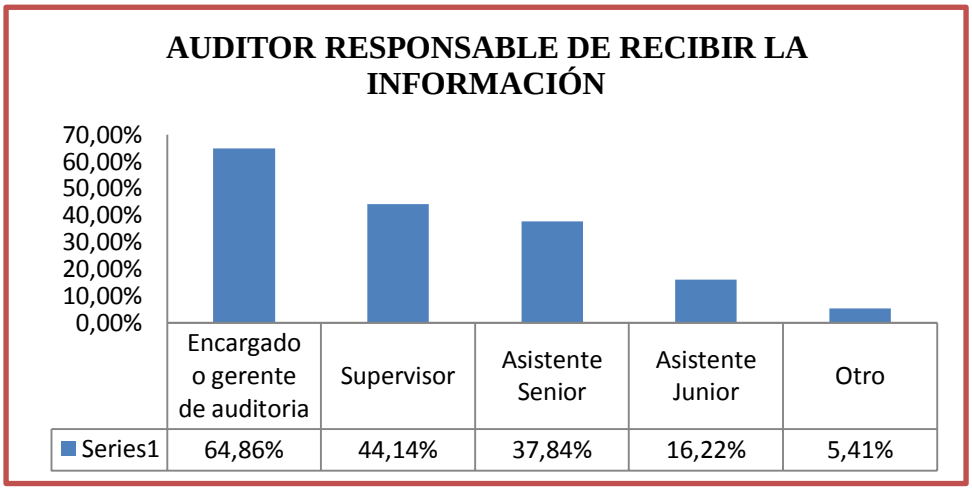
Dentro de su firma ¿Quién es el responsable para recibir la información de sus clientes, en el momento de realizar el encargo de auditoría? (Puede seleccionar más de una opción)

OBJETIVO

Determinar quién es el responsable de recibir la información de los clientes en la firma de auditoría.

TABULACION

Nº	Respuesta/variable	frecuencia	
		absoluta	relativa
a	Encargado o gerente de auditoría	72	64,86%
b	Supervisor	49	44,14%
c	Asistente Senior	42	37,84%
d	Asistente Junior	18	16,22%
e	Otro	6	5,41%



ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Con un 64.86% los encuestados dijeron que el responsable de recibir la información es el encargado o gerente de auditoría, seguido con un 44.14% el supervisor de la misma; asistente

senior con un 37.84%, asistente junior con un 16.22%; lo cual es preciso mencionar que el encargado de cumplir con la auditoría y el mismo que organiza el equipo de trabajo, según sea el caso, para realizar el encargo, es el que tendrá la responsabilidad de recibirla y manipularla de forma adecuada, sin omitir que un 5.41% optaron por otras opciones.

PREGUNTA Nº5

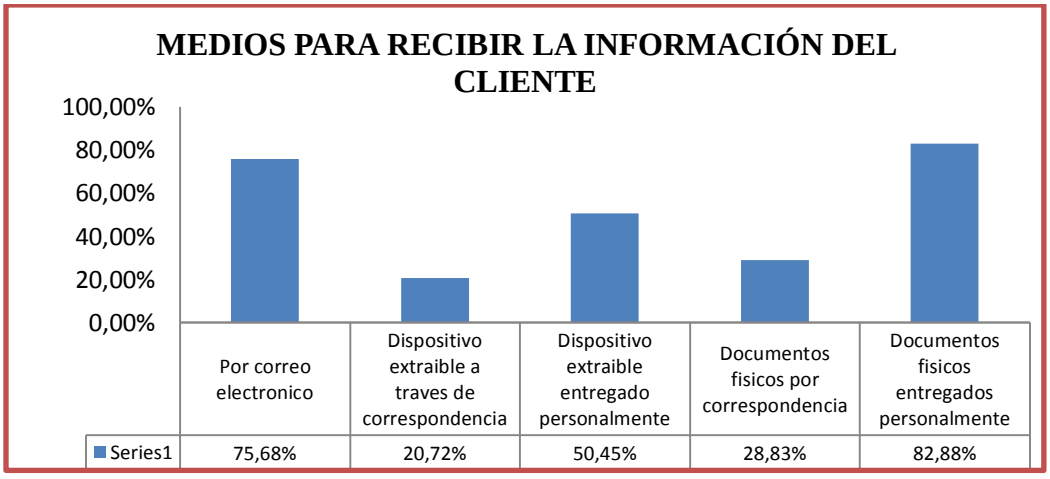
¿A través de qué medio le solicita o transfieren la información de sus clientes?

OBJETIVO

Conocer cuáles son los medios más utilizados por el personal de la firma y los clientes para la transferencia de información entre ellos.

TABULACION

Nº	Respuesta/variable	frecuencia	
		absoluta	relativa
a	Por correo electrónico	84	75.68%
b	Dispositivo extraíble a través de correspondencia	23	20.72%
c	Dispositivo extraíble entregado personalmente	56	50.45%
d	Documentos físicos por correspondencia	32	28.83%
e	Documentos físicos entregados personalmente	92	82.88%



ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Los profesionales de contaduría pública que ejercen auditoría externa, revelan en los datos estadísticos con un 82.88% que reciben la información a través de documentos físicos personalmente complementando así con la transferencia por correo electrónico con un 75.68%., seguido por el uso de dispositivos extraíbles entregados personalmente con un 50.45, la recepción documentos físicos por correspondencia con un 28.83% y finalmente el uso de dispositivos extraíbles por correspondencia con un 20.72%; exponiendo así la información de sus clientes por el uso de terceros o de dispositivos que pueden sufrir graves consecuencias por diferentes siniestros antes de llegar directamente con el auditor que realizara el encargo.

PREGUNTA N°6

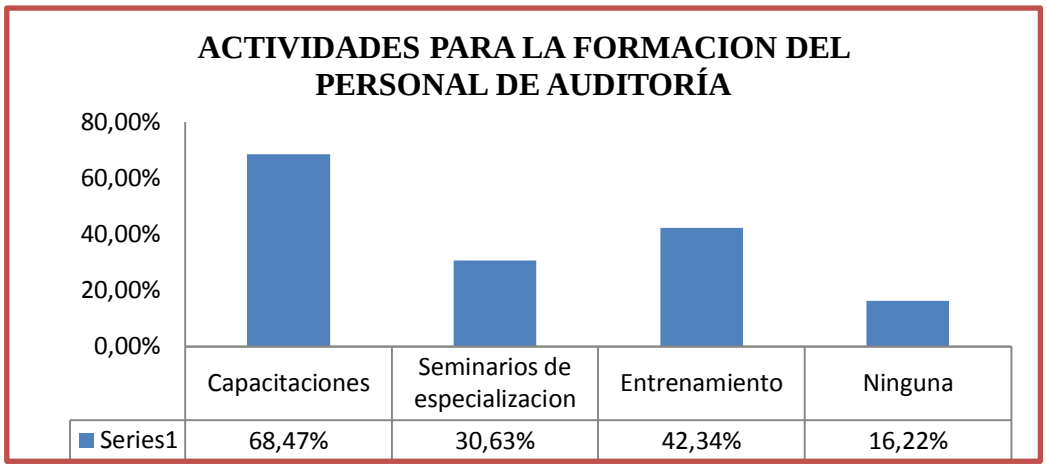
En su firma de auditoría ¿Qué tipo de actividades realiza para la formación de su personal en cuanto a la seguridad de la información? (Puede seleccionar más de una opción)

OBJETIVO

Investigar las actividades que las firmas de auditoría realizan para la formación del personal que trabaja dentro de las mismas y que manejan información de los encargos.

TABULACION

Nº	Respuesta/variable	frecuencia	
		absoluta	relativa
a	Capacitaciones	76	68.47%
b	Seminarios de especialización	34	30.63%
c	Entrenamiento	47	42.34%
d	Ninguna	18	16.22%



ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Según los encuestados el 68.47% incorporan capacitaciones al personal dentro de su firma de auditoría y aunque dicen practicar entrenamiento con un 42.34% para los profesionales, existe una considerable baja de formación con seminarios de especialización ocupando un 30.63% y esto puede impactar para que los colaboradores en la organización carezcan de conocimiento específicos para implementar la nueva tendencia tecnológica y otros procedimientos que garantizan la seguridad de la información de sus clientes y la que manejan como propia para el funcionamiento de la misma, sin omitir que una pequeña parte de los profesionales encuestados con 16.22% no realizan ninguna de las opciones antes mencionadas.

PREGUNTA N°7

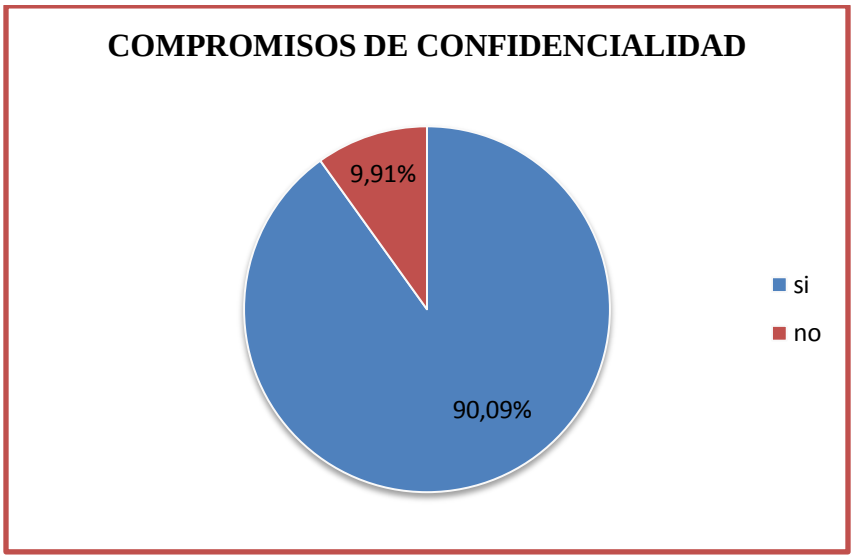
¿Establecen compromisos de confidencialidad de información, con el personal que trabaja en los encargos de auditoría en la firma?

OBJETIVO

Investigar las actividades que las firmas de auditoría realizan para la formación del personal que trabaja dentro de las mismas y que manejan información de los encargos.

TABULACION

Nº	Respuesta/variable	frecuencia	
		absoluta	relativa
a	si	100	90.09%
b	no	11	9.91%



ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

En el resultado de la tabulación, los datos revelan que los encuestados con un 90.09% si establecen compromisos de confidencialidad y un pequeño porcentaje con 9.91% no los establecen, lo cual según el dato anterior, en la pregunta 6, no hay seminarios de especialización y esto puede indicar que puede que no exista un seguimiento de control con respecto al compromiso de confidencialidad con el personal de la firma, en consecuencia la probabilidad de perdida de información por robo o acceso no autorizado incrementa de forma significativa.

PREGUNTA Nº8

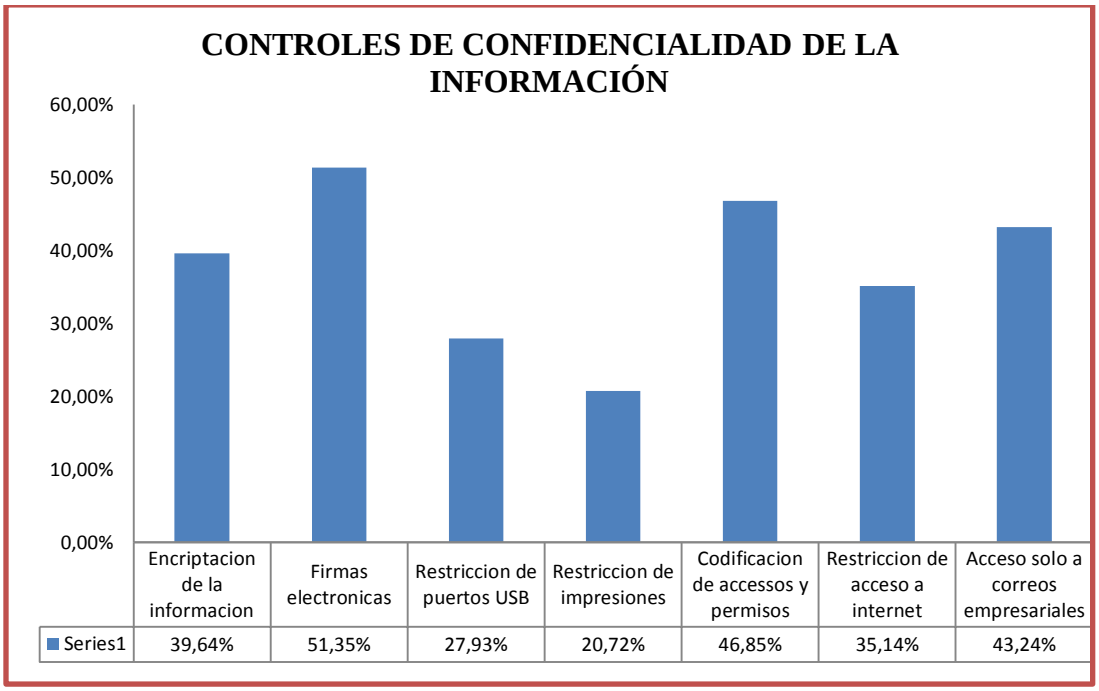
¿Qué tipo de controles realiza para mantener la confidencialidad de la información de los encargos de auditoría en la firma?

OBJETIVO

Indagar sobre los tipos de controles que utilizan las firmas de auditoría como estrategia para evitar la fuga de información de sus clientes.

TABULACION

Nº	Respuesta/variable	frecuencia	
		absoluta	relativa
a	Encriptación de la información	44	39,64%
b	Firmas electrónicas	57	51,35%
c	Restricción de puertos USB	31	27,93%
d	Restricción de impresiones	23	20,72%
e	Codificación de accesos y permisos	52	46,85%
f	Restricción de acceso a internet	39	35,14%
g	Acceso solo a correos empresariales	48	43,24%



ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Según los resultados obtenidos con el método de investigación observamos que los controles que utilizan con mayor frecuencia las firmas de auditoría para mantener la confidencialidad de los datos y archivos de los encargos es el de firmas electrónicas con un 51.35% seguido por la codificación de accesos y permisos con un 46.85%, acceso solo a correos empresariales con el 43.24%, encriptación de la información con el 39.64%, restricción de acceso a internet 35.14%, restricción de puertos USB con el 27.93% finalmente restricción de impresiones con el 20.72%; lo anterior indica que en poca frecuencia, las firmas de auditoría conocen sobre los sistemas tecnológicos y sus procedimientos de seguridad a través de encriptación y otros controles sobre los activos de tecnología de la información.

PREGUNTA Nº9

Al realizar un trabajo de auditoría ¿Qué dispositivos y/o medios utiliza para el respaldo de la información?

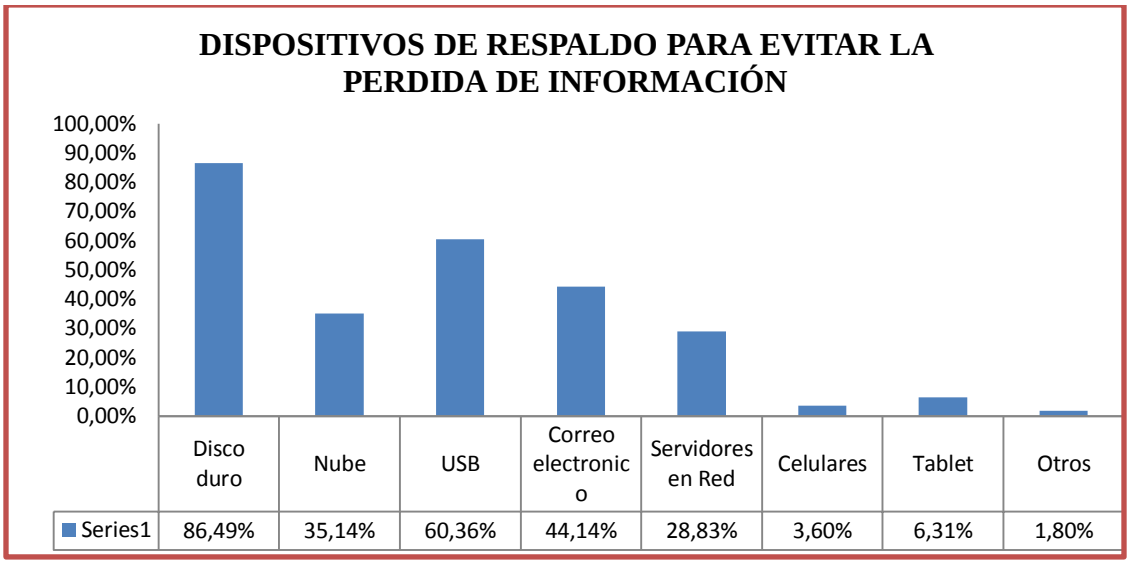
OBJETIVO

Conocer que dispositivos y/o medios prefieren las firmas de auditoría para mantener copias de la información como medida de protección ante cualquier fallo de los sistemas y posible pérdida de datos.

TABULACION

Nº	Respuesta/variable	frecuencia	
		absoluta	relativa
a	Disco duro	96	86,49%
b	Nube	39	35,14%
c	USB	67	60,36%
d	Correo electrónico	49	44,14%
e	Servidores en Red	32	28,83%

f	Celulares	4	3,60%
g	Tablet	7	6,31%
h	Otros	2	1,80%



ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

En las firmas de auditoría el dispositivo más utilizado para realizar respaldo de la información es el disco duro con un 86.49%, el segundo más utilizado con 60.36 % son los dispositivos USB, seguido por los correos electrónicos con el 44.14%, en cuarto lugar se encuentra la nube con el 35.14%, un porcentaje menor utiliza los dispositivos como Tablet 6.31%, celulares 3.60%, y otros como CD con el 1.80%; con lo cual se revela que la tendencia de la mayoría no conocen los aspectos tecnológicos y los beneficios que estos agregarían a las firmas, por consiguiente esta popularidad de dispositivos se encuentran vulnerables a robos, virus, errores humanos y otros que perjudican directamente a la perdida de datos y archivos confidenciales.

PREGUNTA Nº10

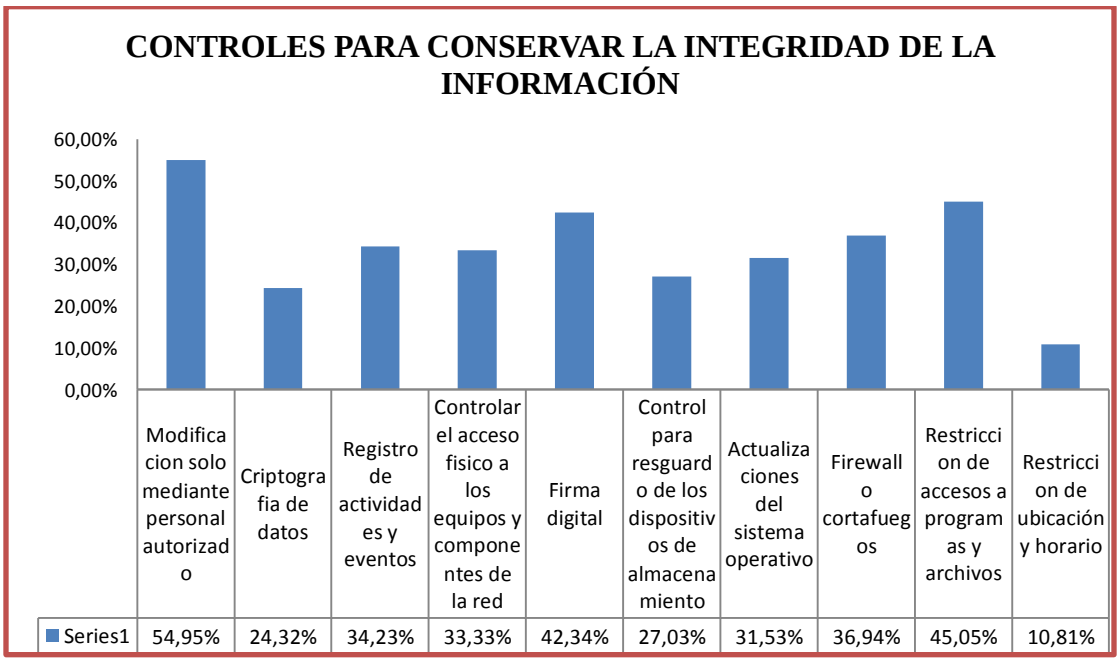
En su firma de auditoría ¿Qué tipo de controles realiza para conservar la integridad de la información?

OBJETIVO

Investigar sobre los controles que utilizan las firmas para mantener la información integra y que no sea alterada por personal no autorizado.

TABULACION

Nº	Respuesta/variable	frecuencia	
		absoluta	relativa
a	Modificación solo mediante personal autorizado	61	54,95%
b	Criptografía de datos	27	24,32%
c	Registro de actividades y eventos	38	34,23%
d	Controlar el acceso físico a los equipos y componentes de la red	37	33,33%
e	Firma digital	47	42,34%
f	Control para resguardo de los dispositivos de almacenamiento	30	27,03%
g	Actualizaciones del sistema operativo	35	31,53%
h	Firewall o cortafuegos	41	36,94%
i	Restricción de accesos a programas y archivos	50	45,05%
j	Restricción de ubicación y horario	12	10,81%



ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Según la investigación se observa que las firmas de auditoría utilizan para conservar integra la información los siguientes controles: modificación solo mediante personal autorizados con un 54.95% así como la restricción de accesos a programas y archivos con el 45.05%, firmas digitales con el 42.34%, firewall ó cortafuegos con el 36.94%, registro de actividades y eventos con el 34.23%, actualizaciones del sistema operativo 31.53%, control para resguardo de los dispositivos de almacenamiento con el 27.03%, criptografía de la información con el 24.32% en último lugar la restricción de ubicación y horario; haciendo de forma notoria la falta de implementación de controles y recursos tecnológicos que garantizaran la integridad de los datos.

PREGUNTA Nº11

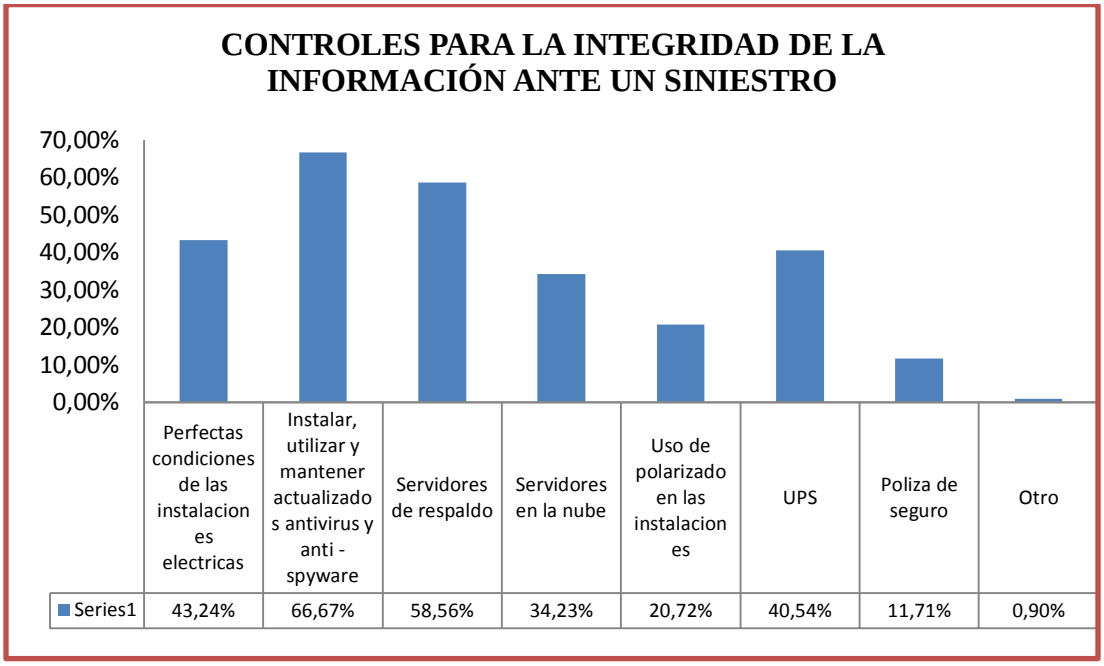
¿De qué manera se asegura que la información se encuentra completa, ante el riesgo de un siniestro?

OBJETIVO

Conocer qué medidas utilizan para asegurar que la información esté protegida ante la ocurrencia de un hecho inesperado que cause la pérdida de ésta.

TABULACION

Nº	Respuesta/variable	frecuencia	
		absoluta	relativa
a	Perfectas condiciones de las instalaciones eléctricas	48	43,24%
b	Instalar, utilizar y mantener actualizados antivirus y anti - spyware	74	66,67%
c	Servidores de respaldo	65	58,56%
d	Servidores en la nube	38	34,23%
e	Uso de polarizado en las instalaciones	23	20,72%
f	UPS	45	40,54%
g	Póliza de seguro	13	11,71%
h	Otro	1	0,90%



ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

La completitud de la información es de suma importancia en las firmas de auditorías es por ello que según los datos encuestados, la manera con que aseguran que esto se cumpla, es instalando, utilizando y manteniendo actualizados anti-virus y anti-spyware con el 66.67%, servidores de respaldo con el 58.56%, perfectas condiciones de las instalaciones eléctricas con 43.24%, UPS con 40.54%, servidores en la nube 34.23%, uso de polarizado en las instalaciones el 20.72%, pólizas de seguros 11.71% y finalmente otros con el 0.90%, con lo anterior se puede determinar que los profesionales omiten muchas veces la necesidad de respaldar la información en servidores tecnológicos y de igual manera la omisión del mantenimiento de instalaciones por lo que no se encuentran preparados de forma adecuada para un siniestro.

PREGUNTA Nº12

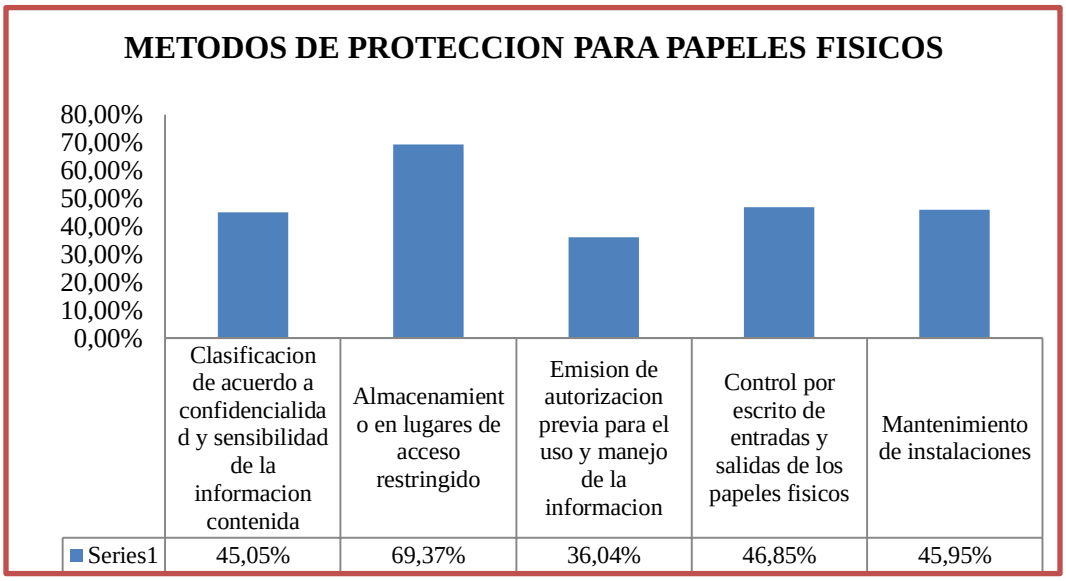
De los siguientes métodos seleccione los que utiliza para la protección de los papeles físicos

OBJETIVO

Evaluar los métodos utilizados para proteger la información física de los clientes y de qué forma mantienen un control sobre el acceso a ella.

TABULACION

Nº	Respuesta/variable	frecuencia	
		absoluta	relativa
a	Clasificación de acuerdo a confidencialidad y sensibilidad de la información contenida	50	45,05%
b	Almacenamiento en lugares de acceso restringido	77	69,37%
c	Emisión de autorización previa para el uso y manejo de la información	40	36,04%
d	Control por escrito de entradas y salidas de los papeles físicos	52	46,85%
e	Mantenimiento de instalaciones	51	45,95%



ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Sin dejar de lado la importancia de los papeles físicos los profesionales de contaduría pública que ejercen la auditoría externa en su mayoría contestaron que el método más utilizado para la protección de estos es el almacenamiento en lugares de acceso restringido con el 69.37%, control por escrito de entradas y salidas de los papeles físicos con 46.84%mantenimiento de las

instalaciones con el 45.95%, clasificación de acuerdo a confidencialidad y sensibilidad de la información contenida con el 45.05%, emisión de autorización previa para el uso y manejo de la información con el 36.04%, esto nos deja comprobado que se están omitiendo controles que responsabilicen al personal en específico y la administración de estos por lo que la supleción de estas medidas pueden causar la perdida que puede resultar significativa.

PREGUNTA Nº13

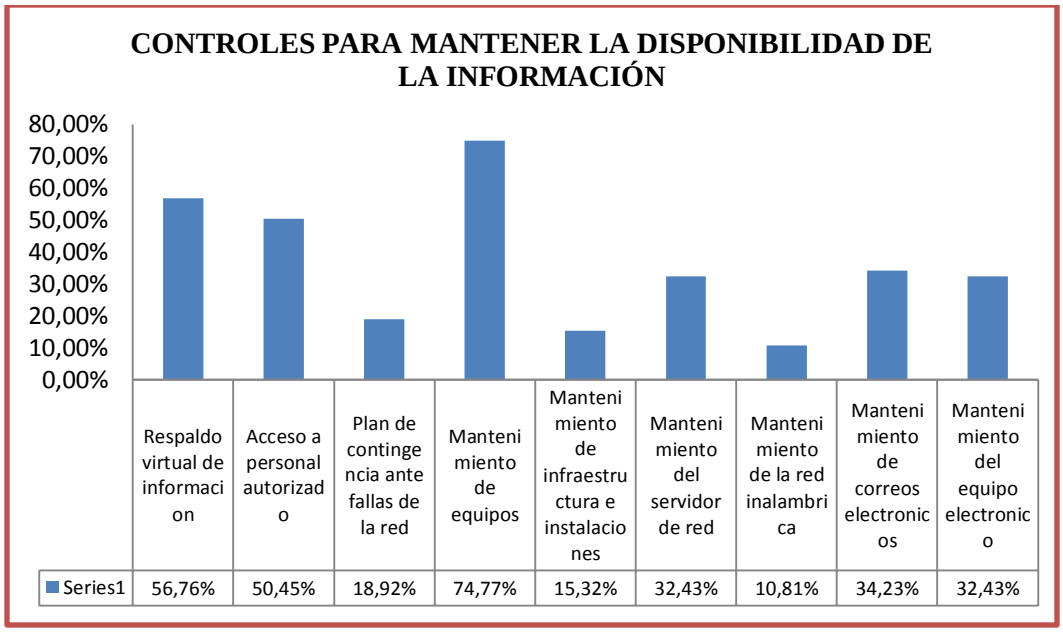
¿Qué tipo de controles realiza para que la información mantenga la disponibilidad adecuada?

OBJETIVO

Interpretar cuales son los tipos de controles más frecuentes que practican en las firmas de auditoría para garantizar la disponibilidad de la información.

TABULACION

Nº	Respuesta/variable	frecuencia	
		absoluta	relativa
a	Respaldo virtual de información	63	56,76%
b	Acceso a personal autorizado	56	50,45%
c	Plan de contingencia ante fallas de la red	21	18,92%
d	Mantenimiento de equipos	83	74,77%
e	Mantenimiento de infraestructura e instalaciones	17	15,32%
f	Mantenimiento del servidor de red	36	32,43%
g	Mantenimiento de la red inalámbrica	12	10,81%
h	Mantenimiento de correos electrónicos	38	34,23%
i	Mantenimiento del equipo electrónico	36	32,43%



ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Con base a los resultado las firmas de auditorías el control que realizan con mayor frecuencia para que la información mantenga la disponibilidad adecuada es el mantenimiento de equipos con el 74.77% seguido por el respaldo virtual de información con el 56.76%, acceso a la información con el 56.76%, acceso a personal autorizados 50.45%, mantenimiento del equipo electrónico y de servidor de red con 32.43% cada uno, mantenimiento de correos electrónicos con el 34.23%, plan de contingencia ante fallas de la red 18.92%, mantenimiento de infraestructura e instalaciones 15.32% y finalmente mantenimiento de la red inalámbrica 10.81%, verificando así, que las firmas de auditoría no poseen estrategias sofisticadas que ayuden a mantener en perfectas condiciones la infraestructura y los dispositivos que almacenan la información.

PREGUNTA Nº14

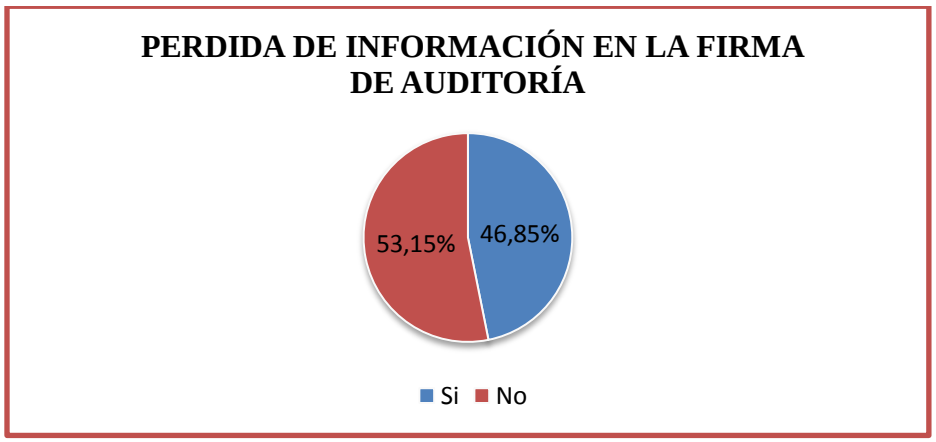
En su firma de auditoría ¿Ha sufrido alguna pérdida de información física y/o digital?

OBJETIVO

Conocer con qué frecuencia las firmas de auditoría se han enfrentado a una pérdida de información.

TABULACION

Nº	Respuesta/variable	frecuencia	
		absoluta	relativa
a	Si	52	46,85%
b	No	59	53,15%



ANÁLISIS E INTERPRETACION DE LOS RESULTADOS

Del total de los encuestados, un 53.15% contestó que no han sufrido pérdida de la información, y un 46.85 % contestó que sí, sin embargo es muy poca la diferencia por lo que se puede observar que muchos corren el riesgo de perder información.

PREGUNTA Nº15

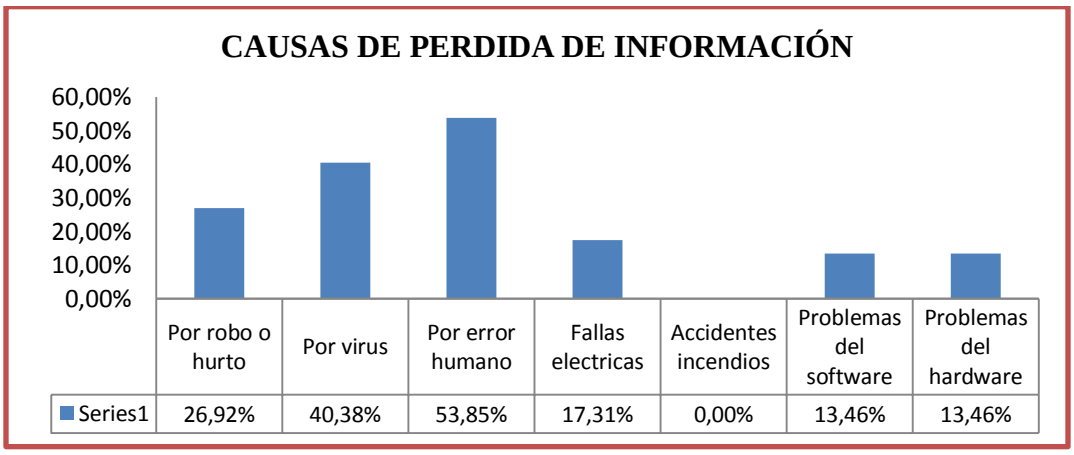
Del siguiente listado ¿Cuáles han sido las causas de la pérdida de información?

OBJETIVO

Analizar cuáles son las causas más comunes que provocan la perdida de información en las firmas de auditoría.

TABULACION

Nº	Respuesta/variable	frecuencia	
		absoluta	relativa
a	Por robo o hurto	14	26,92%
b	Por virus	21	40,38%
c	Por error humano	28	53,85%
d	Fallas eléctricas	9	17,31%
e	Accidentes incendios	0	0,00%
f	Problemas del software	7	13,46%
g	Problemas del hardware	7	13,46%



ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

De acuerdo a los resultados la mayor pérdida de información se da a causa de error humano con 53.85% como resultado, seguido del 40.38% por virus, en tercer lugar el 26.92% por robo o hurto, en cuarto lugar el 17.31% por fallas eléctricas y por último el 13.46% por problemas de software, resultando que el mayor problema se debe al error humano, por lo que se determina que no existen las medidas necesarias para protegerla incluso del propio personal de trabajo responsable de suministrarla.

PREGUNTA Nº16

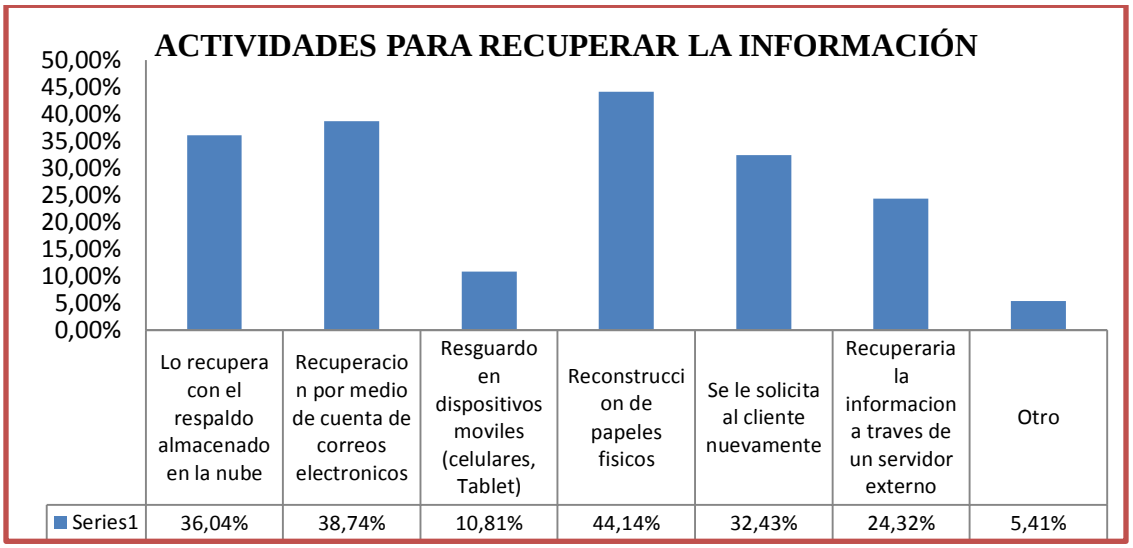
¿Qué haría para recuperar la información de sus clientes si esta se perdiera por causa de un siniestro?

OBJETIVO

Interpretar cuales son las acciones que comúnmente los profesionales de contaduría pública realizan ante una pérdida de información a causa de un siniestro.

TABULACION

Nº	Respuesta/variable	frecuencia	
		absoluta	relativa
a	Lo recupera con el respaldo almacenado en la nube	40	36,04%
b	Recuperación por medio de cuenta de correos electrónicos	43	38,74%
c	Resguardo en dispositivos móviles (celulares, Tablet)	12	10,81%
d	Reconstrucción de papeles físicos	49	44,14%
e	Se le solicita al cliente nuevamente	36	32,43%
f	Recuperaría la información a través de un servidor externo	27	24,32%
g	Otro	6	5,41%



ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Del 100% de los encuestados el 44.14% respondió que en caso de pérdida de la información la recupera por reconstrucción de papeles físicos, en segundo lugar un 38.74% respondió que por

medio de correo electrónico, el 36.04% por almacenamiento en la nube, el 32.43% lo solicita nuevamente al cliente, el 24.32% a través de un servidor externo y por ultimo un 5.41% por otros medios, por lo que se concluye que son muy pocos los que utilizan todos los medios para el resguardo de la información y que no están adecuadamente preparados.

PREGUNTA Nº17

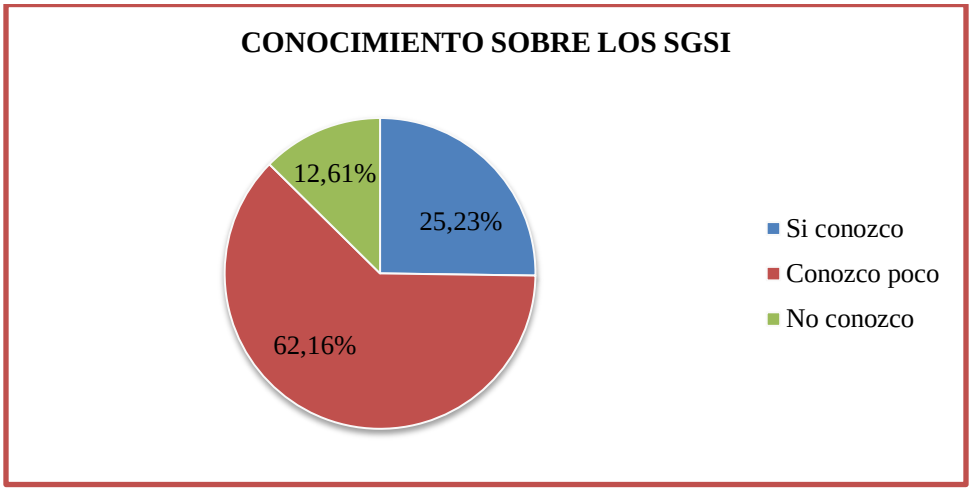
¿Tiene conocimiento sobre los Sistemas de Gestión de la Seguridad de la Información?

OBJETIVO

Indagar sobre el nivel de conocimiento de los profesionales que laboran en las firmas de auditoría sobre los Sistemas de Gestión de la Seguridad de la información.

TABULACION

Nº	Respuesta/variable	frecuencia	
		absoluta	relativa
a	Si conozco	28	25,23%
b	Conozco poco	69	62,16%
c	No conozco	14	12,61%



ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Del total de los encuestados al preguntarles si conocían del SGSI un 62.16% respondió que conoce poco, seguido de un 25.23% que contestó que si conoce y por ultimo un 12.61% que dice no conocer, por lo que es necesario capacitar al personal en cuanto a la tecnología y los avances tecnológicos que proporcionan las normas en relación para tener un mayor control sobre la información.

PREGUNTA Nº18

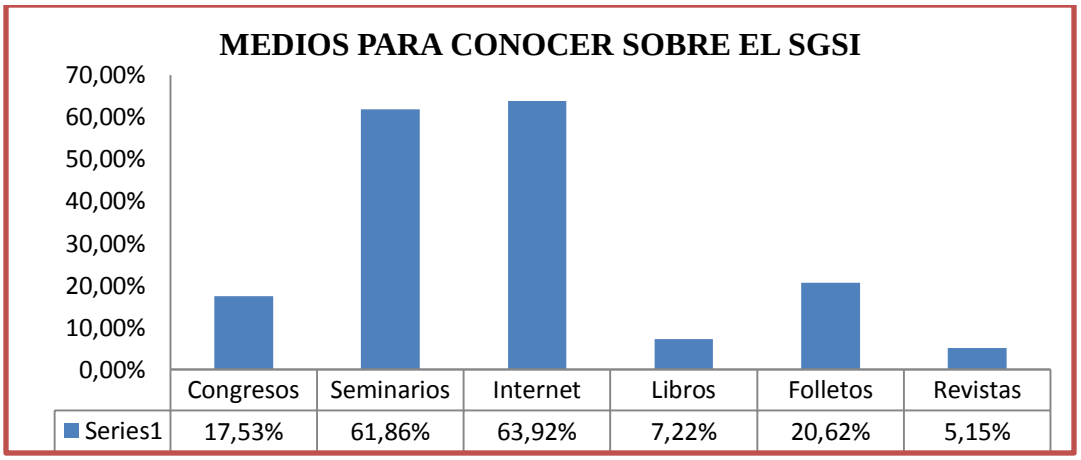
¿A través de que medio obtuvo conocimientos de los Sistemas de Gestión de la Seguridad de la Información?

OBJETIVO

Conocer a través de qué medios, los profesionales de la firma de auditoría, obtuvieron conocimientos sobre los sistemas de gestión de la seguridad de la información.

TABULACION

Nº	Respuesta/variable	frecuencia	
		absoluta	relativa
a	Congresos	17	17,53%
b	Seminarios	60	61,86%
c	Internet	62	63,92%
d	Libros	7	7,22%
e	Folletos	20	20,62%
f	Revistas	5	5,15%



ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

De los 60 encuestados que representan el total un 63.92%, dicen haber obtenido información de los sistemas de gestión de seguridad de la información a través de internet, seguido de un 61.86% que lo obtuvo a través de seminarios, en tercer lugar un 20.62% por medio de folletos, un 17.53% a través de congresos, el 7.22% por medio de libros y el 5.15% por revistas, por lo que se puede concluir que aún no es muy conocido éste tipo de sistemas y muy poca la información compartida.

PREGUNTA Nº19

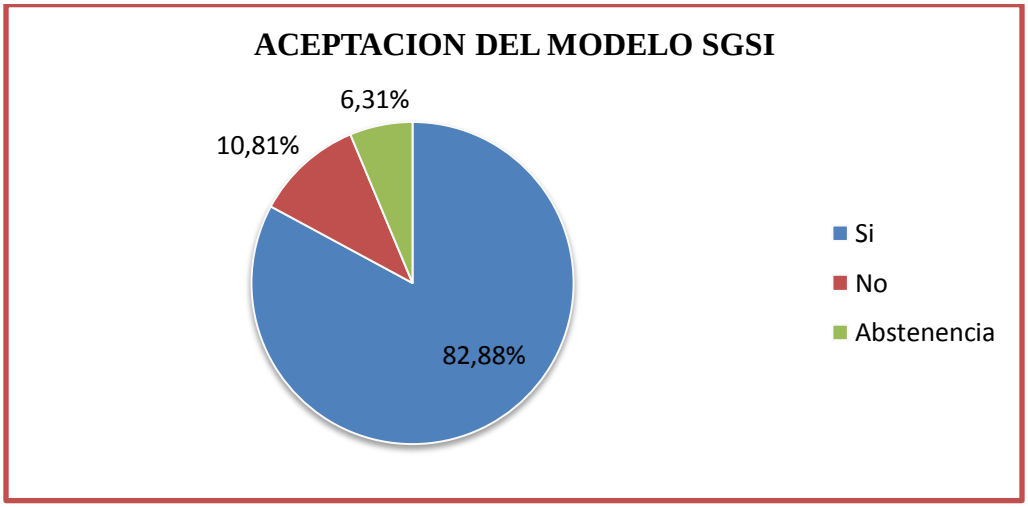
Sí existiera un Modelo de Sistema de Gestión de la Seguridad de la Información estaría interesado en aplicarlo para mejorar la seguridad de la información de su firma de auditoría y de sus clientes:

OBJETIVO

Determinar la aceptación de un SGSI en los profesionales de contaduría pública que ejercen la Auditoría externa para mejorar sus métodos de resguardo.

TABULACION

Nº	Respuesta/variable	frecuencia	
		absoluta	relativa
a	Si	92	82,88%
b	No	12	10,81%
c	Abstinencia	7	6,31%



ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

De 111 encuestados el 82.88% dijeron que si estarían dispuestos a implementar un modelo de seguridad de la información, el 10.81% dijo que no y el 6.31 se abstuvieron de contestar, por lo que se puede deducir que la mayoría está interesado en proteger el activo más importante de las empresas que es la información, ya que esto les servirá para darle un valor agregado a las firmas, incrementado la credibilidad con los clientes y las personas que contestaron que no es porque no conocen del tema o les parece muy costoso.