UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

"DISEÑO DE PLANEACIÓN DE AUDITORÍA DE SISTEMAS CON BASE A LAS NORMAS ISO 27000 EN LAS EMPRESAS INDUSTRIALES AFILIADAS A LA ASI"

Trabajo de Investigación Presentado Por:

Amaya Miranda; Idalia Isabel

Culina Chinque; Loida Concepción

Gómez Carranza; Yamilet del Carmen

Para optar al grado de:

LICENCIADO EN CONTADURIA PUBLICA

Abril del 2010

San Salvador El Salvador Centro América

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES UNIVERSITARIAS

Rector	:	Máster Rufino Antonio Quezada Sánchez
Secretario	:	Licenciado Douglas Vladimir Alfaro Chávez
Decano de la Facultad de Ciencias Económicas	:	Máster Roger Armando Arias Alvarado
Secretario de la Facultad de Ciencias Económicas	:	Máster José Ciriaco Gutiérrez Contreras
Director de la Escuela de Contaduría Pública	:	Licenciado Juan Vicente Alvarado Rodríguez
Coordinador de seminario	:	Licenciado Roberto Carlos Jovel Jovel
Asesor Director	:	Licenciado Mauricio Ernesto Magaña Menéndez.
Jurado Examinador	:	Licenciado Víctor René Osorio Amaya. Licenciado Mauricio Ernesto Magaña Menéndez.

Abril del 2010.

San Salvador El Salvador Centro América

AGRADECIMIENTOS

A Dios, por darme la vida y haber permitido alcanzar este triunfo en mi vida. A mis Padres, por ser los instrumentos que Dios utilizó para que viniera al mundo, por todo su amor y apoyo incondicional que me dieron a lo largo de la carrera y por acompañarme siempre en los momentos más difíciles e importantes. A mis hermanos/as, por su comprensión y apoyo, en especial a Osmin por ser más que un hermano para mí, como un padre, por confiar plenamente en que lograría coronar mi carrera. A mis sobrinos/as, por haber estado conmigo en los momentos de dificultades. A mi esposo, por darme el apoyo ideal, el amor incondicional durante mi carrera. A mis suegros y cuñadas, por su compresión en los momentos más decisivos. Al Grupo Asunción y San Juan Bosco, por darme la fortaleza y confianza, en el transcurso de mi carrera.

Loida Concepción Culina Chinque

A Dios todopoderoso por darme fortaleza y guiarme día a día en los momentos decisivos en mi vida y en el trascurso de mi carrera. A mi madre, por su apoyo incondicional en el logro de mis metas profesionales y por estar siempre a mi lado en todo momento, a mi tía más querida que fue como mi segunda madre y la cual siempre recordare en todo momento por sus sabios consejos, y a mis primos mis hermanos de corazón por su comprensión y apoyo moral. A nuestros asesores los Licenciados Mauricio Ernesto Magaña Menéndez y Víctor René Osorio Amaya por todo su tiempo y esfuerzo en el transcurso de la investigación. A la Licenciada María Margarita de Jesús Martínez de Hernández por todo su apoyo, dedicación y enseñanzas trasmitidas; porque gracias a sus conocimientos me han ayudado a formarme profesional y académicamente.

Idalia Isabel Amaya Miranda

A Dios, por fortalecer mi corazón y bendecirme con haber puesto a aquellas personas que fueron mi soporte a lo largo de mi carrera. A mi Familia, por su incondicional amor, su tiempo y por ser una de las razones para seguir luchando. A Licda. María Margarita de Jesús Martínez, por brindarme siempre su apoyo, cariño y amistad. A mis amigas de tesis, porque sin su apoyo no hubiera sido posible hacer realidad este sueño. A mis amigos, por compartir conmigo su cariño y amistad que inyectaron ánimo en los momentos que más lo necesite. A todas y cada una de las personas que de una u otra forma aportaron su tiempo, cariño y consejos, desde lo más profundo de mi corazón les digo gracias por ser parte de este sueño.

Yamilet Del Carmen Gómez Carranza

INDICE

RESUMEN EJECUTIVO i

INTRODUCCION iii

CAPITULO I – MARCO TEÓRICO

1.1. Antecedentes 1

1.1.1. Los Sistemas Informáticos e Industria 1

1.1.2. Auditoria de Sistemas 2

1.1.3. Normativa ISO 27000 3

1.2. Diferencias entre Auditoría Financiera y Auditoría de Sistemas 5

1.3. Recursos comparables entre Auditoría Financiera y Auditoría de Sistemas 6

1.4. Consideraciones clave del estándar ISO 27000 6

1.5. Importancia de Auditoría de Sistemas con Enfoque ISO 27000 15

1.6. Características de Auditoría de Sistemas con Enfoque ISO 27000 16

1.7. Ventajas y Desventajas de Auditoría de Sistemas con Enfoque ISO 27000 17

1.8. Planeación de Auditoría de Sistemas 19

1.8.1 Memorándum de Planeación 20

1.8.1.1. Objetivos y Términos de Contratación 20

1.8.1.2. Conocimiento del Cliente 20

1.8.1.3. Cuestionario de Evaluación del Sistema 21

1.8.1.4. Matriz de Evaluación de Control de Riesgo del Sistema 21

1.8.1.5. Programas de Auditoria 22

1.8.1.5.1. Software 22

1.8.1.5.2. Hardware 23

1.8.1.5.3. Procesamiento Electrónico de Datos 24

1.8.1.5.4. Recursos Humanos 24

1.9. Base Técnica con Relación a la Auditoría de Sistemas 25

1.9.1 Normas Internacionales de Contabilidad 25

1.9.2. Normas Internacionales de Auditoría (NIAS) 25

1.10. Base Legal 26

1.10.1 Código Tributario 26

1.10.2. Ley de Fomento y Protección de la Propiedad Intelectual 27

1.10.3. Código Penal 27
1.11. Generalidades de los sistemas 28

CAPITULO I I – METODOLOGIA Y DIAGNOSTICO DE LA INVESTIGACION

2.1. Tipo de Investigación 30
2.2. Tipo de Estudio 30
2.3. Unidades de Análisis 30
2.4. Universo o Población 30
2.5. Muestra 31
2.6. Instrumentos y Técnicas Utilizadas en la Investigación 32
2.7. Procesamiento y Tabulación de Datos 32
2.8. Diagnostico de la Investigación 32
2.8.1. Conocimiento que el Contador Público Tiene Sobre la Normativa ISO 27000 33
2.8.2. Importancia del Desarrollo de Auditoria de Sistemas Con Enfoque ISO 27000 36
2.8.3. Importancia de Contar con un Modelo de Planeación de Auditoria de Sistemas 38

CAPITULO III DISEÑO DE PLANEACION DE AUDITORIA DE SISTEMAS CON BASE A LAS NORMAS ISO 27000 EN LAS EMPRESAS INDUSTRIASLES AFILIADAS A LA ASI

3.1. Análisis de Check Listt 45
3.2. MP1 Objetivos, responsabilidad, compromiso y términos de contratación. 47
3.3. MP2 Conocimiento del Cliente 51
3.4. MP3 Cuestionarios de evaluación del sistema 54
3.5. MP4 Grafica de riesgo de impacto 62
3.6. MP5 Programas 64

CAPITULO IV - CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES 92
RECOMENDACIONES 93
BIBLIOGRAFÍA 94
A N E X O S

RESUMEN EJECUTIVO

En un ambiente tecnológicamente cambiante como el que vivimos día a día, las empresa industriales procuran estar a la vanguardia y utilizar mecanismos que les permita competir en un mercado demandado cada ves más por la calidad y confianza tanto en sus productos como la información que manejan y que les permite mejorar y crecer como entidad. En tal sentido las auditorias de sistemas son cada vez más importante para dichas compañías, las cuales necesitan confiar en la información que los sistemas informáticos que poseen generan.

La calidad de la información, armonía y efectividad de los sistemas en las empresas es un punto crucial para estas, los profesionales en contaduría publica tienen ante si un campo de trabajo muy poco aprovechado; pero, que representa una oportunidad para ampliar sus servicios, más aun si este cuenta con una herramienta que le permita no solo incursionar en auditorias de sistemas sino además valla sumado con la base de las normas ISO 27000.

Si bien es cierto que partimos de los avances tecnológicos y de la implementación de estos en las empresas, el estándar de calidad ISO 27000 esta orientado ha aspectos organizativos; es decir a la organización de la seguridad de la información; por tanto la auditoria de sistemas bajo el enfoque de dicha norma trata no solo de poner de manifiesto la existencia de un correcto sistema de calidad documentado sino también de que los sistemas sean conocidos por toda la organización.

Sin embargo, este campo representa para los profesionales en contaduría publica un reto y demanda que estén al tanto de las nuevas innovaciones de normalización y su desarrollo, por tanto y como medida de apoyo, es necesario contar con los pasos o lineamientos para el desarrollo de una auditoria de sistemas con base a las normas ISO 27000; las cuales vendrían a dar un valor agregado a los servicios que prestan, es por eso que surge la presente investigación con el objetivo de brindar una herramienta que les permita conocer e implementar las normas ya mencionadas en este tipo de trabajos.

La investigación se desarrolló bajo el enfoque hipotético deductivo, empleando un estudio de tipo descriptivo analítico y mediante técnicas e instrumentos como la encuesta, el muestreo y la investigación bibliográfica que permitió conocer la situación actual en cuanto a los conocimientos de los profesionales

en contradiría publica sobre las normas de calidad ISO 27000 y su implementación en las auditorias de sistemas. Con relación a lo anteriormente expuesto, actualmente no se cuenta con este tipo de herramientas, las cuales brindarían un aporte a los trabajos realizados.

En conclusión un modelo de planeación de auditoria de sistemas con base a las normas ISO 27000 representa una herramienta útil para aquellos profesionales que ya se encuentran desarrollando trabajos de auditoria de sistemas y como un aliciente para aquellos que todavía no se deciden a incursionar en dicho campo.

Por tanto se sugiere tomar como base para el desarrollo de este tipo de trabajos el presente modelo de planeación de auditoría de sistemas con base a las normas ISO 27000 para las empresas industriales.

INTRODUCCION

La auditoría de sistemas es de gran importancia respecto a los sistemas de información ya que estos deben ser confiables puesto que son considerados para tomar decisiones en base a la información generada, debido a ello se da la necesidad de que se realicen auditorias de sistemas en base a normas las cuales permitan que los profesionales en contaduría pública se desarrollen en este campo el cual es muy importante en la actualidad.

Con relación a dicha necesidad, se ha elaborado está investigación, la cual se divide en cuatro capítulos:

El primero muestra los antecedentes de los sistemas informáticos, de la auditoría de sistemas y de la ISO 27000, la diferencia entre auditoría financiera y auditoría de sistemas, los recursos comparables entre la auditoria financiera y la de sistemas; importancia, características, ventajas y desventajas de auditoría de sistemas con enfoque ISO 27000; posteriormente se menciona la planeación de auditoría de sistemas en el cual se refleja el memorándum de planeación y por último la base técnica y legal.

El segundo capítulo detalla la metodología utilizada para llevar a cabo la investigación, especificando el tipo de estudio realizado, las unidades de análisis, el universo o población, la manera en como se determinó la muestra, los instrumentos y técnicas utilizadas, procesamiento y tabulación de datos y el diagnóstico de la investigación.

En el tercer capitulo se presenta la propuesta, la cual es el diseño de planeación de auditoría de sistemas con base a las normas ISO 27000 en las empresas industriales afiliadas a la ASI, el cual se ha dividido de la siguiente forma: se describe el check listt, por consiguiente se puntualiza los objetivos, responsabilidad, compromiso y términos de contratación, se explica el conocimiento del cliente, los cuestionarios de evaluación del sistema, la gráfica de riesgo de impacto y por último los programas de las diferentes áreas.

El capítulo cuatro presenta las conclusiones y recomendaciones que se derivan de la investigación presente y se describe específicamente las circunstancias que se enfrentan actualmente y las soluciones ante la problemática estudiada. Al final se presenta la bibliografía que se utilizó para desarrollar dicha investigación y los respectivos anexos.

CAPITULO I – MARCO TEÓRICO

1.1. Antecedentes

1.1.1. Los Sistemas Informáticos e Industria

Durante el año 1967, la Guerra Fría entre la Unión Soviética y Estados Unidos estaba en su máximo apogeo y la Agencia de Proyectos de Investigación Avanzada del Departamento de Defensa de Estados Unidos (DARPA), asignó el desarrollar un sistema de interconexión o red que protegiera los sistemas de logística e información en todos los centros y ciudades importantes en caso de caos nuclear. Las redes de comunicación de ese tiempo estaban diseñadas de modo que cada nudo de la red dependía del anterior.

La revolución industrial, se produjo a fines del siglo XVIII como un proceso de cambio constante y crecimiento continuo donde intervinieron varios factores: las invenciones técnicas (tecnología) y descubrimientos teóricos en donde las empresas buscaban otorgar un soporte adecuado al proceso productivo, el cual se caracteriza por la repetición de tareas específicas; es decir, no sólo con pocos objetivos muy bien definidos, sino que con una enunciación muy precisa de la metodología a seguir para alcanzarlos.

Desde esta perspectiva, fue claro que ciertas compañías de gran volumen, consideraron la inclusión de mecanismos computarizados, para que tomaran el control de algunas de estas tareas altamente repetitivas y de mínimo nivel de necesidad de usar "intelecto".

Otras empresas, consideraron el uso de elementos computarizados para el control y registro de volúmenes de producción. La aparición de estos elementos, que en su mayoría eran simples contadores mecanizados, trajo consigo un efecto que no se puede olvidar. Hasta antes que llegara la "máquina", había un ser humano haciendo ese trabajo.

Logrado el primer acercamiento de la computación a las empresas, rápidamente se empezó a ganar terreno dentro de la organización. Y el primer interesado en utilizar nuevas tecnologías, fueron los responsables de la administración y las finanzas. Y los proyectos en los que mayor disponibilidad había para invertir eran los de estas unidades.

1.1.2. Auditoria de Sistemas

En diversos países de Europa tales como Inglaterra e Italia, durante la edad media existieron asociaciones, las cuales ejecutaban funciones de auditoría, destacándose entre ellas los Consejos Londinenses (Inglaterra) en 1310, el Colegio de Contadores de Venecia (Italia) en 1581.

Posteriormente se dio la revolución industrial en la segunda mitad del siglo XVIII, la cual especifico nuevas direcciones especialmente en la misma. La palabra Auditoría proviene del latín auditorius y de esta se deriva el término auditor, que tiene la virtud de oír y revisar cuentas, pero debe estar encaminado a un objetivo especifico, el cual es el de evaluar la eficiencia y eficacia con que se está operando para que, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación.

La Auditoría de sistemas nace hace más de 35 años como un mecanismo para valorar y valuar la confianza que se puede depositar en los sistemas de información, ya que con el surgimiento de la innovación de la tecnología en el mundo digital, las entidades se vieron obligadas a adquirirlos como medida para contrarrestar el gran número de transacciones.

Por consiguiente, los Sistemas de Información presentan ventajas y desventajas para la entidad, ya que pueden existir errores del sistema, o por el procesamiento de datos, debido a ello las entidades se vieron en la necesidad de evaluar la situación de la misma debido a las siguientes circunstancias:

- Desconocimiento en la situación informática de la empresa.

- Falta total o parcial de seguridades lógicas y físicas, que garanticen integridad del personal, equipos e información.

Por lo que la auditoria de sistemas ha sido muy importante para identificar y prevenir este tipo de errores que ocasionen consecuencias a la entidad.

Para el caso de El Salvador, quizás el punto de mayor trascendencia en el transcurso de los años de la auditoria, fue el 2 de septiembre de 1999 en el que el Consejo de Vigilancia de la Profesión de la Contaduría Pública y Auditoria acordó establecer que en la realización de auditorias a los Estados Financieros, el auditor debe aplicar las Normas Internacionales de Auditoria dictadas por la Federación Internacional de Contadores (IFAC); el cual lo ratificó el 11 de Diciembre de 2003.

En cuanto a la auditoria de sistemas no existe ninguna obligación en las leyes nacionales que obliguen a las empresas a realizarlas; sin embargo las entidades salvadoreñas han ido optando en el trascurso de los años por implementarlas a fin de llevar un mayor control sobre sus sistemas informáticos y la información que estos generan.

1.1.3. Normativa ISO 27000

Como parte de la evolución de las ISO y la constante necesidad de las empresas de presentar información confiable y segura surge una normativa enfocada en satisfacer esta necesidad, es así como las normas ISO 27000 se dio a conocer en el año 2004 producto de los cambios en los modelos 9000 y BS 7799. [1]

En el 2005, no existía una normativa que permitiera autenticar alguna organización en cuanto a sus prácticas de seguridad de computación y las alternativas, en esos momentos se certificaba en normas inglesas (BS) o españolas (UNE). Hasta dicho año, el modelo más conocido era el 17799, pero con la limitación de ser un "código de prácticas" (information technology –security techniques– code of practice for information security management), en el momento que se publica su última revisión, se anuncia el desarrollo de una serie de estándares: ISO 27000, la cual estaba destinada exclusivamente a la seguridad informática. [2]

Partiendo de lo anterior se le da un nuevo alcance a la seguridad, porque no sólo es llevar mejores prácticas sino establecer un estándar certificable de forma similar al ISO 9000 el primero de esa serie en publicarse fue en el estándar 27000.

ISO (Organización Internacional de Estándares) e IEC (Comisión Internacional de Electrotecnia) conforman un especializado sistema para los estándares mundiales. Organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de Normas Internacionales a través de comités técnicos establecidos por la organización respectiva para tratar con los campos particulares de actividad técnica.

---

[1] ISO – IEC 27000 - Wikipedia, la enciclopedia libre.mht

[2] Generalidades ISO 27000 publicada en pagina web oficial de la norma, www.ISO27000.ES

Los comités técnicos de ISO e IEC colaboran en los campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en relación con ISO e IEC, también forman parte del trabajo.

En el campo de tecnología de información, ISO e IEC han establecido unir un comité técnico, ISO/IEC JTC 1 (Join Technical Committee Nº1). Los borradores de estas Normas Internacionales adoptadas por la unión de este comité técnico son enviados a los organismos de las diferentes naciones para su votación. La publicación, ya como una Norma Internacional, requiere la aprobación de por lo menos el 75% de los organismos nacionales que emiten su voto.

El estándar ISO/IEC 27000 es el nuevo estándar oficial, su título completo en realidad es: BS 7799-2:2005 (ISO/IEC 27001:2005). También fue preparado por este JTC 1 y en el subcomité SC 27, IT "Security Techniques"; 1870 organizaciones en 57 países han reconocido la importancia y los beneficios de esta nueva norma.

El conjunto de estándares que aportan información de la familia ISO-27000 que se puede tener en cuenta son:

- ✓ ISO/IEC 27000 Fundamentals and vocabulary
- ✓ ISO/IEC 27001 ISMS - Requirements (revised BS 7799 Part 2:2005) – Publicado el 15 de octubre del 2005

- ✓ ISO/IEC 27002 Code of practice for information security management - Actualmente ISO/IEC 17799:2005, publicado el 15 de junio del 2005
- ✓ ISO/IEC 27003 ISMS implementation guidance (bajo desarrollo)

- ✓ ISO/IEC 27004 Information security management measurement (bajo desarrollo)
- ✓ ISO/IEC 27005 Information security risk management (basado e incorporado a ISO/IEC 13335 MICTS Part 2) (bajo desarrollo)

Actualmente el ISO-27000 es el único estándar aceptado internacionalmente para la administración de la seguridad de la información y aplica a todo tipo de organizaciones, tanto por su tamaño como por su actividad

Desde el surgimiento de este nuevo estándar en Centroamérica en el año 2006, se empezó a vislumbrar cada vez con mayor fuerza su implementación, siendo la empresa Ricoh de Costa Rica una de las primeras en aplicar dicha norma; sin embarco a septiembre 2008 solamente existe una entidad con certificaron ISO 27000, quedando en suspenso la aplicabilidad de la misma en otras compañías del resto de los países centroamericanos. [3]

1.2. Diferencias entre Auditoría Financiera y Auditoría de Sistemas

Es necesario exponer en primer lugar la base de una auditoría de sistemas, la cual depende en gran medida de las normas ya conocidas e implementadas en la realización de un trabajo de esta índole; las cuales son en base a las auditorías financieras.

Con relación a lo anterior es importante establecer diferencias entre auditoría financiera y de sistemas:

a) La primera, se encarga de dar una opinión de la razonabilidad de las cifras de los estados financieros de una entidad y

b) La segunda, consiste en revisar, evidenciar, comprobar y adecuar los controles implantados en una empresa en relación al software, hardware, redes, recursos humanos, seguridad lógica, seguridad física y el procesamiento electrónico de datos.

[3] Revista It Now Tecnologia y Negocios en America Central y el Caribe, 37ª Edición 2008

1.3. Recursos comparables entre Auditoría Financiera y Auditoría de Sistemas

Financiera	Sistemas
➢ Sus técnicas son generales y puede hacerse manual o computarizadas. ➢ La evaluación del control interno se basa solamente en aspectos contables. ➢ Identifica errores en los estados financieros a través de los sistemas computarizados.	➢ Tiene su propia normativa, además tiene sus propias declaraciones dentro de las NIA`S. ➢ Toma en cuenta el uso apropiado de las técnicas de auditoría a través del computador. ➢ Evalúa más allá de lo contable pues toma aspectos como: flujo de información, normativa relacionada de las TIC (Norma Cobit); además considera el sistema contable y otras áreas relacionadas con seguridad de sistemas. ➢ Previene y corrige errores.

1.4. Consideraciones clave del estándar ISO 27000

Consideraciones para ser implementadas en el desarrollo de una Auditoria de Sistemas

La propuesta de esta norma, no está orientada a despliegues tecnológicos o de infraestructura, sino a aspectos netamente organizativos, es decir, la frase que podría definir su propósito es "Organizar la seguridad de la información", por ello propone toda una secuencia de acciones tendientes al "establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del ISMS (Information Security Management System)". El ISMS, es el punto fuerte de este estándar.

Los detalles que conforman el cuerpo de la norma, se podrían agrupar en tres grandes líneas:

a) Sistemas De Administración de la Seguridad Informática (ISMS).

Definición de la política de este ISMS, teniendo en cuenta:

- ✓ Establecimiento del marco y objetivos de la dirección y principales líneas de acción en temas de seguridad de la información.
- ✓ Consideración de requerimientos legales y de la empresa, y también obligaciones contractuales en aspectos relacionados a la seguridad.
- ✓ Establecer la alineación con el contexto de la estrategia de administración de riesgo de la empresa dentro del cual se establecerá y mantendrá el ISMS.
- ✓ Establecer los criterios contra los cuales se evaluarán los riesgos y si han sido evaluados por la dirección.

Para los criterios de este estándar internacional, la política del ISMS puede ser considerada como una parte del documento de "Política de seguridad" general de la empresa.

b) Valoración de riegos

Identificar la metodología de valoración de riesgo, la información de seguridad identificada de la empresa y los requerimientos y regulaciones legales, así como desarrollar un criterio para la aceptación de riesgo y los diferentes niveles de aceptación del mismo. Se incluyen:

- ✓ Descripción de la metodología que se aplica para la valoración de riesgos.
- ✓ Identificación de riesgos, los recursos que se encuentran dentro del ámbito del ISMS y los propietarios de los mismos, así como también las amenazas hacia los mismos. Identificar las vulnerabilidades que pueden ser explotados por esas amenazas y los impactos que la pérdida de confidencialidad, integridad y disponibilidad, pueden ocasionar sobre esos recursos.
- ✓ Análisis y evaluación de riesgos: Valorar el impacto del negocio hacia la organización que puede resultar desde cualquier fallo de seguridad, teniendo en cuenta la pérdida de confidencialidad, integridad y/o disponibilidad de los recursos.

- ✓ Probabilidad real de la ocurrencia de fallos de seguridad a la luz de las amenazas, vulnerabilidades e impacto asociado a esos recursos y los controles actualmente implementados.

- ✓ Estimación del nivel de riesgo. Determinación si un riesgo es aceptable o requiere el uso de algún tipo de tratamiento de los criterios de riesgo establecidos.

c) Controles

Aplicación de los controles apropiados: Conocimiento y objetividad para la aceptación de riesgos, proveyendo una clara satisfacción de ellos con la política y criterios de aceptación. Selección de controles objetivos para el tratamiento del riesgo.

Estos controles serán seleccionados e implementados de acuerdo a los requerimientos identificados por la valoración del riesgo y los procesos de tratamiento del riesgo.

En las Normas ISO 27000, se encuentra una detallada tabla de controles, los cuales quedan agrupados y numerados de la siguiente forma:

i. Política de seguridad: Este grupo está constituido por dos controles:

- Diseño, planificación, preparación, implementación y
- Revisiones de una Política de Seguridad

La Política de Seguridad, en realidad debería dividirse en dos documentos:

- Política de seguridad (Nivel político o estratégico de la organización):

Es la mayor línea rectora, la alta dirección. Define las grandes líneas a seguir y el nivel de compromiso de la dirección con ellas.

- Plan de Seguridad (Nivel de planeamiento o táctico): Define el

"Cómo". Es decir, baja a un nivel más de detalle, para dar inicio al conjunto de acciones o líneas rectoras que se deberán cumplir.

ii. Organización de la información de seguridad: Este segundo grupo de controles abarca once de ellos y se subdivide en:

- Organización Interna: Compromiso de la Dirección, coordinaciones, responsabilidades, autorizaciones, acuerdos de confidencialidad, contactos con autoridades y grupos de interés en temas de seguridad, revisiones independientes.

- Partes externas: Riesgos relacionados con terceros, gobierno de la seguridad respecto a clientes y socios de negocio.

Lo más importante a destacar de este grupo son dos cosas fundamentales que abarcan a ambos subgrupos:

- Organizar y Mantener actualizada la cadena de contactos (internos y externos), con el mayor detalle posible (Personas, responsabilidades, activos, necesidades, acuerdos, riesgos, etc.).
- Derechos y obligaciones de cualquiera de los involucrados.

iii. **Administración de recursos:** Se encuentra subdividido en:

- Responsabilidad en los recursos: Inventario y propietario de los recursos, empleo aceptable de los mismos.

- Clasificación de la información: Guías de clasificación y Denominación, identificación y tratamiento de la información.

Este grupo es eminentemente procedimental y no aporta nada al aspecto ya conocido en seguridad de la información, en cuanto a que todo recurso debe estar perfectamente inventariado con el máximo detalle posible, que se debe documentar el "uso adecuado de los recursos" y que toda la información deberá ser tratada de acuerdo a su nivel.

iv. **Seguridad de los recursos humanos:** se encuentra subdividido en:

- Antes del empleo: Responsabilidades y roles, verificaciones curriculares, términos y condiciones de empleo.
- Durante el empleo: Administración de responsabilidades, preparación, educación y entrenamiento en seguridad de la información, medidas disciplinarias.
- Finalización o cambio de empleo: Finalización de responsabilidades, devolución de recursos, revocación de derechos.

Tanto el inicio como el cese de cualquier tipo de actividad relacionada con personal responsable de manejo de información de la organización, son actividades muy fáciles de procedimental.

v. Seguridad física y del entorno: se encuentra subdividido en:

- Áreas de seguridad: Seguridad física y perimetral, control físico de entradas, seguridad de locales edificios y recursos, protección contra amenazas externas y del entorno, el trabajo en áreas e seguridad, accesos públicos, áreas de entrega y carga.
- Seguridad de elementos: Ubicación y protección de equipos, elementos de soporte a los equipos, seguridad en el cableado, mantenimiento de equipos, seguridad en el equipamiento fuera de la organización, seguridad en la redistribución o reutilización de equipamiento, borrado de información y/o software.

vi. Administración de las comunicaciones y operaciones: es el más extenso de todos y se divide en:

- Procedimientos operacionales y responsabilidades: Tiene como objetivo asegurar la correcta y segura operación de la información, comprende cuatro controles. Hace especial hincapié en documentar todos los procedimientos, manteniendo los mismos y disponibles a todos los usuarios que los necesiten, segregando adecuadamente los servicios y las responsabilidades para evitar uso inadecuado de los mismos.

Esta tarea en todas las actividades de seguridad (no solo informática), se suele realizar por medio de lo que se denomina Procedimientos Operativos Normales (PON) o Procedimientos Operativos de Seguridad (POS), y en definitiva consiste en la realización de documentos breves y ágiles, que dejen por sentado la secuencia de pasos o tareas a llevar a cabo para una determinada función. Cuanto mayor sea el nivel de desagregación de esta función, más breve será cada PON (también habrá mayor cantidad de ellos) y a su vez más sencillo y comprensible.

- Administración de prestación de servicios de terceras partes: Abarca tres controles, se refiere fundamentalmente, como su nombre lo indica, a los casos en los cuales se encuentran tercerizadas determinadas tareas o servicios del propio sistema informático.

Los controles están centrados en tres aspectos fundamentales de esta actividad:

• Documentar adecuadamente los servicios que se están prestando (acuerdos, obligaciones, responsabilidades, confidencialidad, operación, mantenimiento, etc.).

• Medidas a adoptar para la revisión, monitorización y auditoría de los mismos.
• Documentación adecuada que permita regularizar y mantener un eficiente control de cambios en estos servicios.
- Planificación y aceptación de sistemas: El objetivo es realizar una adecuada metodología para que al entrar en producción cualquier sistema, se pueda minimizar el riesgo de fallos.

- Protección contra código móvil y maligno: el objetivo de este apartado es la protección de la integridad del software y la información almacenada en los sistemas.

- El código móvil, es aquel que se transfiere de un equipo a otro para ser ejecutado en el destino final, este empleo es muy común en las arquitecturas cliente-servidor, y se está haciendo más común en las arquitecturas "víctima-gusano", por supuesto con un empleo no tan deseado.
- En cuanto al código malicioso, El estándar hace referencia al conjunto de medidas comunes que ya suelen ser aplicadas en la mayoría de las empresas, es decir, detección, prevención y recuperación de la información ante cualquier tipo de virus.

- Resguardo: El objetivo de esta apartado conceptualmente es muy similar al anterior, comprende un solo control que remarca la necesidad de las copias de respaldo y recuperación.

- Administración de la seguridad de redes: Los dos controles que conforman este apartado hacen hincapié en la necesidad de administrar y controlar lo que sucede en nuestra red, es decir, implementar todas las medidas posibles para evitar amenazas, manteniendo la seguridad de los sistemas y aplicaciones a través del conocimiento de la información que circula por ella. Se deben implementar controles técnicos, que evalúen permanentemente los servicios que la red ofrece, tanto propios como tercerizados.
- Manejo de medios: como "medio" debe entenderse todo elemento capaz de almacenar información (discos, cintas, papeles, etc. tanto fijos como removibles). Por lo tanto el objetivo de este grupo es, a través de sus cuatro controles, prevenir la difusión, modificación, borrado o destrucción de cualquiera de ellos o lo que en ellos se guarda.
- Intercambios de información: Este grupo contempla el conjunto de medidas a considerar para cualquier tipo de intercambio de información, tanto en línea como fuera de ella, y para movimientos internos o externos de la organización.
- Monitorización: Este apartado tiene como objetivo la detección de actividades no autorizadas en la red y reúne seis controles. Los aspectos más importantes a destacar son:
• Auditar Logs que registren actividad, excepciones y eventos de seguridad.

• Realizar revisiones periódicas y procedimientos de monitorización del uso de los sistemas.
• Implementación de robustas medidas de protección de los Logs de información de seguridad.
• La actividad de los administradores y operadores de sistemas, también debe ser monitorizada, pues es una de las mejores formas de tomar conocimiento de actividad sospechosa, tanto si la hace un administrador propio de la empresa (con o sin mala intención) o si es uno que se hace pasar por uno de ellos.
• Sincronización de tiempos: Hoy en día el protocolo NTP (Network Time Protocol) está tan difundido y fácilmente aplicable que es un desperdicio no usarlo.

Se debe implementar una buena estrategia de estratos, tal cual lo propone este protocolo, y sincronizar toda la infraestructura de servidores, tanto si se depende de ellos para el funcionamiento de los servicios de la empresa, como si no.

vii. **Control de accesos:** El control de acceso es posterior a la autenticación y debe regular que el usuario autenticado, acceda únicamente a los recursos sobre los cuales tenga derecho y a ningún otro, es decir que tiene dos tareas derivadas:
   - Encauzar (o enjaular) al usuario debidamente.
   - Verificar el desvío de cualquier acceso, fuera de lo correcto.

Para cumplir con este propósito, este apartado lo hace a través de veinticinco controles, que los agrupa de la siguiente forma:

- Requerimientos de negocio para el control de accesos
- Administración de accesos de usuarios
- Responsabilidades de usuarios
- Control de acceso a redes
- Control de acceso a sistemas operativos
- Control de acceso a información y aplicaciones

viii. **Adquisición de sistemas de información, desarrollo y mantenimiento:** Contiene los siguientes controles,

- Requerimientos de seguridad de los sistemas de información
- Procesamiento correcto en aplicaciones
- Controles criptográficos

- Seguridad en los sistemas de archivos
- Seguridad en el desarrollo y soporte a procesos
- Administración técnica de vulnerabilidades

ix. Administración de los incidentes de seguridad: Todo lo relativo a incidentes de seguridad queda resumido a dos formas de proceder:

- Proteger y proceder.
- Seguir y perseguir.

x. Administración de la continuidad de negocio: Este grupo cubre nuevamente cinco controles y los presenta a través de un solo grupo:

- Aspectos de seguridad de la información en la continuidad del negocio. Este grupo tiene como objetivo contemplar todas las medidas tendientes a que los sistemas no hagan sufrir interrupciones sobre la actividad que realiza la empresa.

xi. Cumplimiento (legales, de estándares, técnicas y auditorías)

En este caso está sometido acorde al país en el cual se aplique la normativa.

Los requerimientos de este estándar internacional, son genéricos y aplicables a la totalidad de las organizaciones.

Cualquier exclusión a los controles detallados por la norma y denominados como “necesarios” para satisfacer los criterios de aceptación de riegos, debe ser justificada y se debe poner de manifiesto, o evidenciar claramente los criterios por los cuales este riesgo es asumido y aceptado.

En cualquier caso en el que un control sea excluido, la conformidad con este estándar internacional, no será aceptable, a menos que dicha exclusión no afecte a la capacidad y/o responsabilidad de proveer seguridad a los requerimientos de información que se hayan determinado a través de la evaluación de riesgos, y sea a su vez aplicable a las regulaciones vigentes.

Ahora bien, el diseño e implantación de un Sistema de Gestión de Seguridad de la Información se encuentra influenciado por las necesidades, objetivos, requisitos de seguridad, los procesos, los empleados, el tamaño, los sistemas de soporte y la estructura de la organización, es así como la orientación de los procesos es importante dentro de la norma.

En el desarrollo de una auditoria de sistemas con enfoque ISO 27000, es importante relacionar a lo anteriormente expuesto el contenido de la ISO 27004; siendo esta norma parte fundamental del grupo de normas ISO 27000.

Consideraciones Adicionales:

a) **El modelo y método para las mediciones de seguridad.** Se debe desarrollar un programa de cómo ejecutar la medición de la seguridad de la información. El éxito de este programa, se basará en la asistencia o ayuda que estas mediciones aporten para adoptar decisiones, o determinar la eficiencia de los controles de seguridad.

Existen dos tipos de métodos para cuantificar los atributos:

- Subjetivos. Implica el criterio humano.

- Objetivos. Se basan en una regla numérica, que puede ser aplicada por personas o recursos automatizados. Los métodos de medición pueden abarcar varios tipos de actividades y un mismo método puede aplicar a múltiples atributos. Algunos ejemplos de métodos son:

  • Encuestas/indagaciones.
  • Observación.
  • Cuestionarios.
  • Valoración de conocimientos.
  • Inspecciones.
  • Re-ejecuciones.
  • Consulta a sistemas.
  • Monitorización ("Testing")
  • Muestreo.

b) Definición y selección de las mediciones en un SGSI. Se deben considerar las mediciones para poder cuantificar la eficiencia de un SGSI, sus procesos y controles.

Las mediciones están directamente relacionadas a:

• Procesos de sistemas de gestión (Ej.: ¿Se realizaron auditorías?, ¿Este manual cumple con los estándares?, etc.).

• Ejecución de controles de seguridad de la información (Ej.: Volumen de incidencias por tipo, acceso a tablas, etc.).

1.5. Importancia de Auditoría de Sistemas con Enfoque ISO 27000

En los últimos años los sistemas informáticos (hardware y software) han adquirido un mayor auge en las operaciones de las empresas permitiéndoles generar información la cual debe ser eficiente y que reúna y presente datos resumidos o bien detallados acerca de la actividad económica de una compañía. Sin embargo, estos mismos son fuentes de riesgos informáticos, tales como falta de seguridad lógica, física y la incursión de los hackers y crackers, que traen como consecuencia la necesidad de crear mecanismos que permitan minimizarlos. Debido ha estas circunstancias se ha recurrido a nuevas técnicas y herramientas que faciliten la eficacia y el nivel de calidad del desempeño de sus funciones.

Como consecuencia de los cambios producidos en las empresas por el avance tecnológico, las compañías van buscando la calidad en todos sus aspectos por lo que es importante contar con ciertos criterios enmarcados en el logro de los objetivos de estas. Las Auditorías del Sistema tratan no solo de poner de manifiesto la existencia de un correcto sistema de calidad documentado, sino también de que dicho sistema sea conocido por toda la organización; es así, como la certificación ISO 27000 es vista como un ejercicio de "impermeabilización de cara al futuro" permitiendo que la gestión de riesgos aumente el interés de los estándares convirtiéndose en una opción para cualquier organización.

Por tanto, representa un nuevo campo de aplicación que se extiende como un reto para los profesionales en contaduría publica en cuanto a la obtención de la información y aplicabilidad sobre las nuevas normas.

Actualmente, los profesionales en contaduría pública en su mayoría no se desarrollan dentro de este campo de acción; ya que dichas actividades están siendo ejercidas por otros profesionales; tal es el caso de los Ingenieros en Sistemas, Ingenieros Industriales, Administradores de Empresa, etc., que son los profesionales que ejercen dichas labores.

Por lo anterior, las limitaciones que se presentan a los profesionales en contaduría pública al margen de no poseer una especialización en esta área se ve agravada por la falta de información y ausencia de un modelo de planeación que permita aplicar estándares de calidad bajo el enfoque ISO 27000 en el desarrollo de una Auditoría de sistemas en una entidad.

En cuanto a la voluntad para ejercer la Auditoría de Sistemas, los profesionales en contaduría publica, se muestran en disposición profesional para ejercer en este campo en una forma ética, con mentalidad abierta, diplomática, observador, perspectiva, versátiles, tenaz y decididos y seguros de si mismo por consiguiente el campo de aplicación en la Auditoría de sistemas no es una limitante sino por el contrario es una oportunidad, en la cual se puede explotar el progreso de las actividades de los profesionales en

esta rama de la Auditoría, en la cual es necesario contar con herramientas adicionales que permitan sintetizar el desarrollo de este tipo de Auditoría. Ahora bien sumado al desarrollo de una Auditoría de sistemas esta la implementación de las normas de calidad ISO con un nuevo enfoque que es la ISO 27000 y que representa la evaluación de los sistemas de gestión de la seguridad informática.

Siendo la calidad uno de los factores esenciales de la competencia en cualquier actividad, se ha generado la necesidad de implementar sistemas normalizados de aseguramiento de la calidad de la información y por consiguiente es preciso que los profesionales en contaduría pública estén al tanto de las nuevas innovaciones de las normalizaciones y en su desarrollo.
Por tanto, si se tuviera una guía que contenga los pasos o lineamientos para el desarrollo de una Auditoría de sistemas con base a las normas de calidad ISO 27000, estas vendrían a dar un valor agregado a los servicios que prestan actualmente los profesionales en contaduría pública.

Por lo antes expuesto, la falta de un modelo de planeación de Auditoría de Sistemas desarrollado sobre la base de las normas ISO 27000 trae como consecuencia la no creación de nuevas áreas de trabajo relacionadas en la Auditoría de sistemas y que el profesional en contaduría publica sea menos competitivo en la prestación de servicios. Por tanto es necesario que al ser profesionales activos y en busca constante de la capacitación y mejora continua de los servicios que son prestados al público, sea preciso contar con nuevas herramientas.

1.6. Características de Auditoría de Sistemas con Enfoque ISO 27000

El desarrollo de una Auditoría de Sistemas con base a la normas ISO 27000 es potencialmente mejor que la desarrollada con un enfoque tradicional. Como consecuencia de los cambios producidos en las empresas por el avance tecnológico, las compañías van buscando la calidad en todos sus aspectos por lo que es importante contar con ciertos criterios enmarcados en el logro de los objetivos de estas.

Las Auditorías de Sistemas tratan no solo de poner de manifiesto la existencia de un correcto sistema de calidad documentado, sino también de que dicho sistema sea conocido por toda la organización. Es así como la certificación ISO 27000 permitirá que la gestión de riesgos aumente el interés de los estándares convirtiéndose en una opción para cualquier organización que opere en el sector industrial y que

representen un nuevo campo de aplicación que se extiende como un reto para los profesionales en contaduría publica en cuanto a la obtención de la información y aplicabilidad sobre las nuevas normas.

Dentro de las principales características de la norma ISO 27000 están:

i) Sirve para todo tipo de organizaciones, y asegura la selección de controles de seguridad adecuados, protegiendo a los activos y dando confianza a las partes interesadas.

ii) Especifica los requerimientos a establecer, poniendo en ejecución, funcionando, supervisando, repasando, manteniendo y mejorando la documentación del sistema de administración en la seguridad de la Información (ISMS), dentro del contexto de la totalidad de los riesgos del negocio.

iii) Especifica las métricas y técnicas de medida aplicables para determinar la eficiencia y efectividad de la implantación de un SGSI[4] y de los controles relacionados.

iv) Guía para la gestión del riesgo de la seguridad de la información[5].

v) La ISO ofrece un interesante alineamiento con otras normas también de sistemas de gestión, como la ISO 9001 de Calidad y la 14001 de Medio Ambiente, con el consiguiente beneficio de reducción de esfuerzos y costos en una implementación semi-integrada.

1.7. Ventajas y Desventajas de Auditoría de Sistemas con Enfoque ISO 27000

La aplicación de ISO 27000 en el desarrollo de una Auditoría de sistemas, representa para las entidades que buscan una posición con ventaja competitiva en el mercado, una mayor representatividad de la información y de los sistemas que estas poseen.

[4] Sistemas de Gestión de la Seguridad Informática
[5] ISO 2700, Ing. Jaime H. Rubio R., Noviembre 2006

Dentro de las ventajas y desventajas más significativas dentro de una planeación de Auditoría de sistemas con base a las normas ISO 27000 en las empresas industriales con sistemas informáticos están:

VENTAJAS AUDITORIA DE SISTEMAS CON ENFOQUE ISO 27000	DESVENTAJAS AUDITORIA DE SISTEMAS CON ENFOQUE ISO 27000
Establecimiento de una metodología de gestión clara y estructurada; que permita una mayor integridad, confidencialidad y confiabilidad de la información mediante la recomendación de seguridades y controles en el personal, datos, hardware, software e instalaciones.	Actualmente en el país no se están desarrollando este tipo de trabajos por la falta de un modelo de planeación de Auditoría de sistemas con enfoque en ISO 27000.
Reducción del riesgo de pérdida, robo o corrupción de información.	Limitación en el acceso a la información, así como también el costo de esta.
Confianza en planes estratégicos para una mejor garantía de calidad y confidencialidad comercial.	
Conocer la situación actual del área informática y las actividades y esfuerzos necesarios para lograr los objetivos propuestos.	
Ayudan a identificar las debilidades del sistema y las áreas a mejorar. Mediante capacitación y educación sobre controles en los Sistemas de Información	
Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.	

1.8. Planeación de Auditoría de Sistemas

Al igual que en una auditoria financiera, la auditoria de sistemas parte de la base de lo que se conoce del cliente. Es por eso que para poder planear adecuadamente un trabajo de auditoria de sistemas primero se debe conocer la situación actual del cliente o futuro cliente.

Para poder llevar a cabo lo anterior es necesario partir de una herramienta se conoce como “Check List”. Dentro del contenido del check list tenemos que incluir toda aquella información que se considera vital para el conocimiento del cliente y de los sistemas que posee; un ejemplo de estas son:

a) Tipo de sistemas con que cuenta la Compañía: la finalidad de esta interrogante es conocer el tipo de sistema con que cuenta la empresa, si es a la medida o es un sistema de paquete.
b) Conocer si los sistemas son integrado o no, si lo son es necesario conocer con cuantos módulos cuenta.
c) Saber si la empresa cuenta con una unidad de auditoria o no, al igual que sus áreas criticas si es que ya están identificadas.
d) Verificación de la propiedad del software.
e) Conocer si la empresa posee controles informáticos,
f) Otras generalidades que permitan conocer el ambiente informático y sistemas que posee la empresa.

Es importante que además de cubrir la parte de los sistemas como auditor es importante conocer si la empresa esta cumpliendo con la normativa legal, esto se puede lograr conociendo si:

a) La empresa ha legalizado el sistema contable,
b) Esta inscrita en la alcaldía, ISSS, AFP, etc.
c) Como se encuentra en cuando a la matricula de comercio,
d) La fecha de inicio de operaciones de la empresa.
e) Otras.

Al igual que es importante conocer el cumplimiento de la normativa legal, también es necesario conocer ciertos datos financieros, conocer las fuentes de ingresos de la entidad auditada, el valor de los inventarios, entre otras.

Una vez contestado el check list se procede a tomar datos cuantitativos que permiten elaborar la oferta de trabajo, así como también determinar el alcance del trabajo ha realizar.

1.8.1 Memorándum de Planeación

1.8.1.1. Objetivos y Términos de Contratación

En este apartado se establecen los objetivos tanto general como específicos del trabajo que se desarrollara en la entidad; de igual manera se evalúa el riesgo de auditoria y su alcance. Al establecer el alcance de la auditoria, se trabaja en las áreas seleccionas y dicho trabajo se realiza mediante pruebas selectivas de los datos del sistema según sea el caso. De igual forma se evalúa que la transabilidad de la información de tal forma que la información digital sea igual a la real.

Es importante en esta parte de la planeación de auditoria de sistemas revisar y evaluar el sistema de control interno informático de la entidad; dicha revisión y evaluación se realiza en la mayoría de los casos mediante la aplicación del modelo COSO, pero también es importante incluir la aplicación de las normas COBIT en dicho proceso. Dicho modelo y normas ayudaran en gran medida en el trabajo del auditor en el sentido de poder identificar mediante su aplicación, la situación del control interno de la entidad; ya que el una empresa sin un buen control interno se encuentra expuesta a diversas amenazas.

Por ultimo en esta parte del memorándum de planeación se establecen tanto la responsabilidad del auditor como la periosidad de los informes y el contenido de estos en términos generales, así como también la responsabilidad y compromisos del cliente para con el auditor.

1.8.1.2. Conocimiento del Cliente

Esta parte del memorándum de planeación se enfoca en conocer y tener respaldo de las siguientes generalidades del cliente:

a) Antecedentes
b) Naturaleza
c) Representación y fecha de fundación.

De igual manera es importante tener claro cuales son los objetivos de la institución y si esta posee planes estratégicos, si es el caso es necesario conocerlos y detallarlos en esta parte del trabajo de auditoria.

También es necesario conocer:

a) Datos Claves:
    i. Tipo de mercado en el que se desarrolla la entidad.
    ii. Principales Clientes
    iii. Principales Proveedores

iv. Ambiente de información.

b) Conocer el Informe de gestión: esta parta se refiere no necesariamente a que exista un informe ya escrito, si no al contenido de este, el cual podes armar partiendo de datos conocidos de la entidad como:
   i. Inflación
   ii. Cumplimiento de Presupuestos (en el caso que los posea)
   iii. Obsolescencia de quipos y programas

c) Leyes y Reglamentos especiales que competan a la entidad.

1.8.1.3. Cuestionario de Evaluación del Sistema

Estos cuestionarios constituyen los primeros papeles de trabajo de la ejecución y cuya secuencia depende de los resultados de una matriz FODA, por lo general dicha estructura es:

a) Cuestionario 1: Enfocado a la evaluación del sistema.
   En este tipo de cuestionario se hace referencia a las áreas físicas tales como el hardware, las instalaciones del centro de cómputo e incluso el perfil del personal encargado de dicha área.

b) Cuestionario 2: Enfocado a la evaluación del software.
   Es importante en este apartado conocer el modelo relacional del sistema que la entidad posee.

c) Cuestionario 3: Enfocado a la evaluación de políticas y procedimientos del Control Interno Informático.
   Este esta enfocado a básicamente en evaluar los mismos que en la auditoria financiera y se empieza del nivel más genérico, como por ejemplo saber si se poseen manuales de políticas y procedimientos, si se aplican y se divulgan en la entidad, etc.

1.8.1.4. Matriz de Evaluación de Control de Riesgo del Sistema

En toda auditoria de sistemas la evaluación del riesgo se hace partiendo de:

a) Cuestionario del Especialista
b) Matriz del riesgo de controles generales y de aplicación
c) Flujo grama o modelo relacional del programa que se esta auditando.

Dentro de la matriz de riesgos se tienen que evaluar básicamente:

a) Instalación del sistema,
b) Inicio del sistema,
c) Funcionalidad de módulos
d) Recopilación y respaldo de la información
e) Captura y verificación de datos
f) Desactualización de la información
g) Reportes e impresiones

Es importante tomar en cuenta y evaluar el tipo de controles que se poseen, los cuales pueden ser:

a) Preventivo
b) Detectivo
c) Correctivo

Dichos controles son evaluados en sus tres fases: Alto, Medio y Bajo

1.8.1.5. Programas de Auditoria

Los programas de la auditoria se desarrollan en base a las siguientes áreas:

- ✓ Software
- ✓ Hardware
- ✓ Procesamiento Electrónico de Datos
- ✓ Recursos Humanos

Es importante destacar que dichas áreas se evalúan y se plasman en cedulas analíticas, las cuales son respaldadas mediante evidencias, las cuales pueden ser manuales, escritos, comunicados como memorándums, evidencia digital y fotográfica.

1.8.1.5.1. Software

El Software lo componen los programas informáticos que son utilizados para propósitos generales de funciones específicas.

En este programa se evalúan aspectos importantes como:

a) Seguridad
b) Procesamiento
c) Legalidad del software

d) Origen y Modelo Relacional
e) Eficiencia y rutinas de seguridad
f) Capacidad y velocidad del sistema
g) Tipo de procesamiento que posee.

Una vez evaluado los términos generales del software se pasan a las áreas de cumplimiento de acuerdo a las Normas de Auditoria de Sistemas que son:

- ✓ Seguridad de acceso referencia al papel de trabajo
- ✓ Seguridad contra virus
- ✓ Seguridad de back-up
- ✓ legalización del sistema

Al finalizar en la cedula referente a la evaluación del software se saca una conclusión por cada área.

1.8.1.5.2. Hardware

El hardware lo componen los equipos informáticos que son utilizados en el PED, se identifican en está área las computadoras, el servidor, impresores, UPS, Scanner, Reguladores de voltaje y otros accesorios, se evalúan aspectos importantes como:

a) Capacidad y Eficiencia
b) Seguridad y Mantenimiento
c) Legalidad
d) Ambiente
e) Vida Útil
f) Recursos de redes

De igual forma es importante realizar un levantamiento de inventario físico de todo lo que se refiere al centro de cómputo o equipos que la empresa posea, detallando cada bien.

Se elaboran cedulas de soporte, tales como:

- ✓ Cedula de trabajo de descripción del hardware,
- ✓ Cedula de trabajo de tipo y periocidad del mantenimiento,
- ✓ Otras.

1.8.1.5.3. Procesamiento Electrónico de Datos

En esta área se evalúa básicamente la segmentación y confiabilidad del sistema; como parte importante de dicha evaluación se encuentra:

a) Evaluación de la integridad de los datos
b) El bacheo de documentos versus el sistema
c) El proceso de la información

Es importante evaluar el tipo de sistema y tipo de equipo que se posee, así como los niveles de seguridad de la información. Dentro de los principales componentes que evalúan están:

- ✓ Evaluando los componentes,
- ✓ Captura de datos Manual o digitalizado,
- ✓ Procesamiento de dato
- ✓ Salida de los datos

- ✓ Perfil del encargado del procesamiento electrónico
- ✓ Políticas del sistema de información
- ✓ Control interno
- ✓ Tipos de modelos que genera el sistema

1.8.1.5.4. Recursos Humanos

La verificación de los manuales si es que existen sobre las características que deben cumplir los empleados para los cargos que desarrollan dentro de las entidades, es una de los objetivos de esta área. En tal sentido se realizan pruebas que proporcionen evidencia para evaluar la razonabilidad del recurso humano y metodología asignado al sistema de información.

De igual forma en esta área se debe evaluar el nivel de seguridad o accesibilidad que el personal posee para ingresar al área del centro de cómputo, así mismo si la empres posee con políticas motivacionales para el personal de informática.

Dentro de las evaluaciones más importantes a realizarse en toda auditoria de sistemas están:

a) Eficiencia y Eficacia del personal
b) Organización del trabajo y el tiempo
c) Desarrollo y motivación
d) Capacitación

Es importante verificar el organigrama de la entidad y las planillas de pago afín de verificar la posición y verdadera instancia o contratación del personal encargado de los sistemas informatices de la entidad.

1.9. Base Técnica con Relación a la Auditoría de Sistemas

1.9.1 Normas Internacionales de Contabilidad

De acuerdo a la NIC 38 debe ser aplicada por todas la empresa al preceder a contabilizar activos intangibles.

Con relación al desarrollo de una auditoria de sistemas, es importante que el auditor verifique la legitimidad del software que las empresas poseen; así como también la aplicación contable de estos. Como todo trabajo de auditoria es indispensable partir de la adecuada aplicación de las normas técnicas y legales.

1.9.2. Normas Internacionales de Auditoría (NIAS)

- ✓ Planeación (NIA 300)

El auditor deberá planear el trabajo de auditoria de modo que esta sea desarrollada de una manera efectiva.

En una auditoria de sistemas, sea esta con enfoque ISO o no, es necesario tomar en consideración esta norma, debido a que el grado de planeación varia de acuerdo con el tamaño de la entidad, la complejidad de la auditoria, la experiencia del auditor con la entidad y su conocimiento con el negocio. En tal sentido, la planeación adecuada del trabajo de auditoria ayuda a asegurar que se presta atención adecuada a aéreas importantes de la auditoria, que los problemas potenciales son identificados y que el trabajo es llevado a cabo en forma limpia.

✓ Auditoría en un Ambiente de Sistemas de Información por Computadora,(NIA 401)

Existencia de un Ambiente de Sistemas de Información por Computadora (SIC)

Se considera la existencia de un ambiente Sistemas de Información por Computadora cuando esta involucrada una computadora de cualquier tipo o tamaño en el procesamiento por la entidad de información financiera de importancia para la auditoría, ya sea que dicha computadora sea operada por la entidad o por una tercera parte. El propósito de la auditoría en un ambiente de sistemas de información por computadora es "establecer normas y proporcionar lineamientos sobre los procedimientos que deben seguirse cuando se conduce una auditoría en un ambiente de sistemas de información computarizado (SIC)"[6].

1.10. Base Legal

1.10.1 Código Tributario

El uso legal de los programas de computación es aquel que esta respaldado por una licencia de uso emitida por las productoras de software, especificando las condiciones bajo las cuales se puede utilizar. El primero de enero del año dos mil uno, entro en vigencia el código tributario, mediante decreto legislativo numero 230 del 14 de diciembre de 2000, publicado en el Diario Oficial Nº 241, tomo 349, del 22 de diciembre de 2000 el cual contempla las siguientes disposiciones en cuanto a lo que son los sistemas contables computarizados:

i) Sección novena, Otros Deberes Formales, Art. 147 Inciso II del literal A), establece: Cuando la Contabilidad sea llevada en forma computarizada, deberán conservarse los medios magnéticos que contengan la información, al igual que los respectivos programas para su manejo. También deberá conservarse por un periodo de cinco años, los programas utilizados para facturar mediante sistemas computarizados; así como los documentos que se resguarden por medio de sistemas, tales como microfichas o microfilm.

El Reglamento del Código Tributario en su Capitulo VII, de la contabilidad formal sección primera, artículo 77 menciona lo siguiente:

i) De conformidad a lo establecido en el artículo 147 del Código, cuando un contribuyente adopte el sistema de registro computarizado de contabilidad, deberá conservar como parte integrante de la misma toda la documentación relativa al diseño del sistema, los diagramas del mismo y los programas

[6] Normas Internacionales de Auditoría, Sección 401, párrafo 1.

fuente cuando proceda, así como las bases de datos, por el plazo establecido en dicho precepto legal, los cuales pondrán a disposición de la Administración Tributaria, así como el equipo y sus técnicos, cuando esta lo requiere en el ejercicio de la facultad fiscalizadora.

En el proceso de una planeación de auditoria de sistemas con enfoque ISO 27000, es indispensable considerar lo expuesto anteriormente, con el objetivo de verificar el cumplimiento de la disposiciones que este código establece en relación con el tipo de auditoria que se esta llevando a cabo. Dentro de toda planeación de una auditoria de sistemas es necesario que el auditor conozca del cumplimiento o no de las leyes por parte de la entidad auditada.

1.10.2. Ley de Fomento y Protección de la Propiedad Intelectual

i) Art. 6. Los programas computarizados solo pueden ser usados o autorizados por su propio autor.
ii) Art. 7. Solo el autor puede recibir remuneraciones al vender o utilizar sus sistemas para que estos sean dados a conocer al público.
iii) Art. 10. Son titulares las personas naturales que hayan creado la obra, a cada uno de los autores cuando el invento es producto de varios y al primer editor cundo sea anónimo.
iv) Art. 13 Los programas de ordenador están protegidos originalmente así como las traducciones adaptaciones, transformaciones o arreglos que se les quiere efectuar.
v) Art. 43 Determinar la ilegalidad al hacer uso del logo que no ha sido autorizado por su autor.

1.10.3. Código Penal

i) Art. 226**.** El que a escala comercial reprodujere, plagiare, distribuyere al mayoreo o comunicare públicamente, en todo o en parte, una obra literaria o artística o su transformación o una interpretación o ejecución artística fijada en cualquier tipo de soporte o fuere comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios, será sancionado con prisión de dos a cuatro años.

ii) Art. 227. Será sancionado con prisión de cuatro a seis años, quien realizare cualquiera de las conductas descritas en el artículo anterior, concurriendo alguna de las circunstancias siguientes:

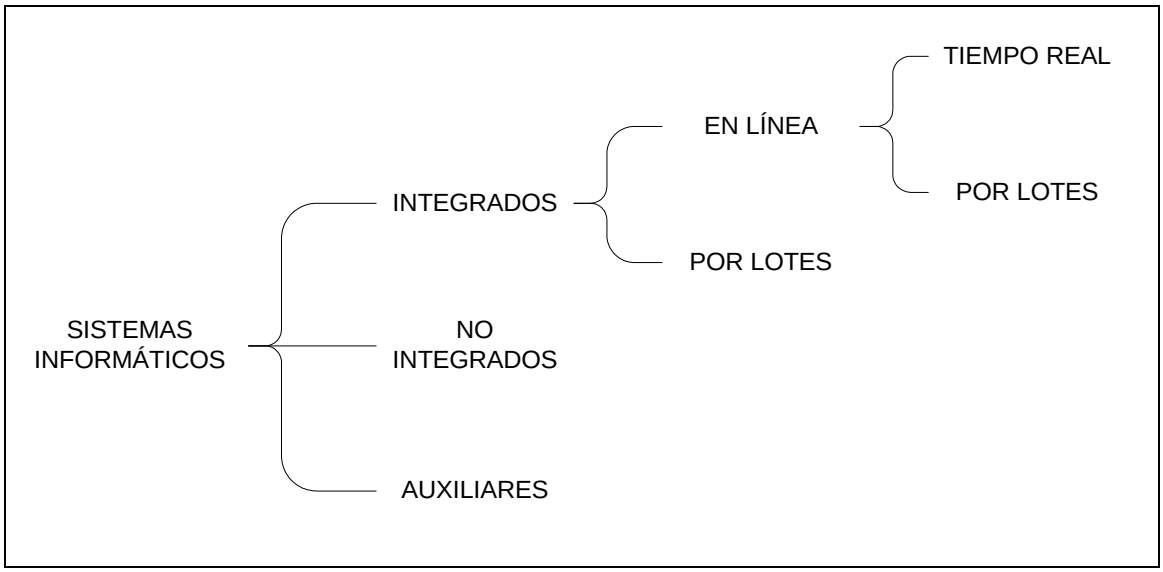
1) Usurpando la condición de autor sobre una obra o parte de ella o el nombre de un artista en una interpretación o ejecución;
2) Modificando sustancialmente la integridad de la obra sin autorización del autor; y,

3) Si la cantidad o el valor de la copia ilícita fuere de especial trascendencia económica.

1.11. Generalidades de los sistemas

✓ Clasificación de los Sistemas Informáticos

Existen diferentes tipos de sistemas informáticos, que pueden ser clasificados de la siguiente manera (ver cuadro 1):



Cuadro 1

Sistemas Integrados:

Implica el compartir información entre dos o más sistemas. Entre las razones por las cuales se establecen estos sistemas están:

- Eliminar redundancia de datos
- Generación de informes
- Facilitar la consulta de datos

Dentro del funcionamiento de un sistema integrado se deben distinguir las siguientes etapas:

a) Parámetros: Se refiere al grado de integración entre los módulos, niveles de seguridad, tipos de operaciones a realizar, códigos de cuentas, y otros.

b) Captura de la información: Se refiere al momento en el cual se transfieren las operaciones de un sistema a otro únicamente hasta el punto en que una operación registrada, aceptada por un sistema auxiliar.
c) Transferencia de la información: Ésta se realiza en forma automática o iniciada por algún usuario para que un sistema pueda ser considerado sistema integrado, debe existir alguna transferencia de información desde el lugar donde se originan los datos hasta el sitio donde serán centralizados conjuntamente con otra información y/o movimientos. El tipo de procesamiento puede ser: En línea o tiempo real, y por lotes
d) Controles sobre la Transferencia: Se clasifican dependiendo de si la transferencia es inmediata o al final del periodo si es inmediata: Se necesitan controles fuentes de tal forma que no permiten el ingreso de datos incompletos o no válidos inconsistentes.

   Si al final del periodo los datos deben ser validados o controles generalmente en el momento en que se corre el proceso de transferencia correspondiente.

Sistemas no Integrados

Un sistema no integrado o independiente es aquél que no esta interconectado o integrado a ningún otro sistema. La información es transferida al final de periodos previamente establecidos a través de movimientos resumidos. En este caso no existe el concepto de información compartida.

Por ejemplo: Un sistema de nómina, controla únicamente la nómina; uno de inventarios controla solamente los inventarios, no es necesario informarle si una venta se realizó de contado o a crédito puesto que ese sistema nada tiene que ver con el control de efectivo o con los clientes de la empresa.

Sistemas Auxiliares

Manejan operativamente todas las transacciones del negocio y tienen las características de ser distintos al sistema contable.

El trabajo de auditoria a realizar por el contador publico variara dependiendo del tipo de sistema de información que utilice la entidad, puesto que cada uno de estos presenta características especiales que el auditor deberá tomar en cuenta a la hora de planificar y ejecutar su trabajo.

Con relación a lo anterior los Sistemas Informáticos aplicados en las compañías dependen en gran medida a las necesidades de estas, en el caso de las empresas industriales son utilizados los Sistema Integrados, por los beneficios que este tipo de sistemas le proporcionan para el desarrollo de sus actividades.

CAPITULO I I – METODOLOGIA Y DIAGNOSTICO DE LA INVESTIGACION

2.1. Tipo de Investigación

El problema relacionado al diseño de planeación de una Auditoría de sistemas con base a normas ISO 27000 en las empresas industriales afiliadas a la Asociación Salvadoreña de la Industria, ha sido investigado mediante el enfoque hipotético deductivo, que busca comprobar teorías e inicia con conocimientos generales hasta llegar a la formulación de hipótesis que marcan el rumbo y orientan el resultado a obtener en el proceso investigativo. Analizando desde una perspectiva general los aspectos que pueden ser la causa fundamental en el surgimiento del problema. Con el propósito de descubrir realidades o elementos específicos de comprobación que permitan plantear una alternativa de solución o control.

2.2. Tipo de Estudio

La investigación se basó en un estudio de tipo correlacional, en el que se analizó sus posibles causas, características, variables y elementos, estudiando la forma en que una variable ejerce influencia sobre la otra, la vinculación entre las variables y la causa principal que da origen al problema en estudio.

2.3. Unidades de Análisis

Las unidades de análisis consideradas en la investigación están constituidas por los Profesionales autorizados por el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría que al 31 de diciembre de 2007 se encontraban inscritos a fin de analizar, el conocimiento y aplicación técnica de una Auditoría de sistemas con enfoque ISO 27000 y que deseen agregar valor a los servicios que ofrecen.

2.4. Universo o Población

La población para esta investigación está formada por el total de los profesionales autorizados por el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría que al 31 de diciembre de 2007 se encontraban inscritos, los cuales fueron publicados en el diario oficial el 09 de abril de 2008, y presentan una población total de 3382 profesionales con las características antes citadas.

2.5. Muestra

La determinación de la muestra se efectúo de forma aleatoria simple a través del método "selección sistemática de elementos muéstrales" aplicable sobre los profesionales que reunieron las características previamente definidas para la población en estudio y su determinación, por tratarse de una población finita se efectúo mediante la formula estadística siguiente:

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

Donde:

n = tamaño de la muestra =?

N = tamaño de la población = 3382

Z = coeficiente de confianza al cuadrado = 1.96

e = margen de error = 0.10

P = probabilidad de éxito = 0.90

Q = probabilidad de fracaso = 0.10

Sustituyendo en la formula:

$$n = \frac{(1.96)^2\,(0.90)(0.10)\,(3382)}{(1.96)^2\,(0.90)\,(0.10) + (3382-1)\,(0.10)^2}$$

$$n = \frac{(3.84)\,(0.90)\,(0.10)\,(3382)}{(3.84)\,(0.90)\,(0.10) + (3381)\,(0.01)}$$

$$n = \frac{(3.46)\;\;(338.20)}{(0.35)\;+\;(33.81)}$$

n = 33

Al aplicar valores a la fórmula se obtuvo que la cantidad de profesionales en contaduría pública a considerar en la muestra de la investigación sea de treinta y tres.

2.6. Instrumentos y Técnicas Utilizadas en la Investigación

El instrumento que se utilizó para la recolección de datos es el cuestionario con preguntas abiertas y cerradas, dicho instrumento fue distribuido a profesionales en contaduría pública según las condiciones de la asignación de la muestra; a través de su utilización se recolecto la información de campo necesaria para demostrar que la problemática planteada existe y que requiere solución.[7]

Las técnicas utilizadas en el desarrollo de la investigación son las siguientes:

a) Metodología Bibliográfica, se efectuó una recopilación de la información bibliográfica disponible en la parte legal y técnica, mediante la utilización de las distintas fuentes, tanto primarias como segundarias.
b) Metodología de Campo, se diseño un cuestionario dirigido a los profesionales inscritos en el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría al 31 de diciembre de 2007.

2.7. Procesamiento y Tabulación de Datos

El procesamiento de la información se efectuó por medio del paquete utilitario EXCEL, mediante un programa diseñado para la tabulación de los datos, la elaboración de las graficas y el cruce de las variables que fueron necesarias. Las interpretaciones de los resultados se muestran en términos absolutos y relativos.

2.8. Diagnostico de la Investigación

Se segmenta la información en dos partes, la correspondiente al modelo de planeación de Auditoría de sistemas con enfoque ISO 27000 y a los profesionales en contaduría publica; mediante el cruce de variables y la asociación de preguntas y respuestas relacionadas, se elaboraron unos cuadros que reflejan en cantidades y porcentajes los resultados obtenidos.

Dichas partes se refieren a:

- ✓ Conocimiento que el Contador Público Tiene Sobre la Normativa ISO 27000.

[7] Anexo 1

- ✓ Importancia del Desarrollo de Auditoria de Sistemas Con Enfoque ISO 27000.
- ✓ Importancia de Contar con un Modelo de Planeación de Auditoria de Sistemas Con Base a Normas ISO 27000.

A continuación se desarrolla cada área en las que se ha segmentado el diagnóstico de la investigación, para los cuales se han elaborado cuadros con datos obtenidos a partir de la tabulación de los mismos, los cuales sirvieron de base para la elaboración del diagnóstico, de igual forma se presentan en forma grafica.[8]

2.8.1. Conocimiento que el Contador Público Tiene Sobre la Normativa ISO 27000

Actualmente son pocos los profesionales en contaduría pública que conocen acerca de las nuevas normas ISO 27000, y su aplicación en el área de sistemas, por consiguiente en los trabajos de auditoria de sistemas que prestan.

Es importante en el ámbito competitivo contar con las herramientas necesarias que permitan estar a la vanguardia de las nuevas normativas y sus beneficios tanto para las empresas, en este caso las empresas industriales y para los profesionales en contaduría pública que envista de las nuevas normas les permitirá brindar un servicio de auditoria con un enfoque ISO.

El uso e implementación de un nuevo modelo de planeación de auditoria basado en las normas ISO 27000, permitirá que los profesionales en contaduría publica incursionar en una área poco aprovechada por estos, la nueva norma como tal es importante para los sistemas de las empresas industriales y mas aun para los auditores al ser incorporada como base de un modelo de planeación de auditoria en el cual se evaluaría a las entidades con mira a una posible calificación ISO, siendo el trabajo y resultados del auditor un punto de partida importante para dichos objetivos.

Por lo tanto, es de gran ayuda contar con un modelo de planeación que permita conocer e implementar una auditoría de sistemas en base a la norma ISO 27000. (Ver cuadro 1).

---

[8] Anexo 2

CUADRO No.1: CONOCIMIENTO DEL CONTADOR PÚBLICO ACERCA DE LA NORMATIVA ISO 27000 EN UNA AUDITORIA DE SISTEMAS

No. PREG.	CRITERIOS	CONTADORES PUBLICOS ENCUESTADOS	FRECUENCIA RELATIVA
3	Conocimiento acerca de la Norma ISO 27000		
	Profesionales en Contaduría Publica que conocen acerca de la Normativa ISO 27000.	5	15.15%
	Profesionales en Contaduría Publica que no conocen acerca de la Normativa ISO 27000.	33	84.85%
4	Proceso de planeación de la auditoria que permita a los profesionales de Contaduría Publica conocer e implementar una auditoria de sistemas en base a Normas ISO 27000.		
	Contadores Públicos que les gustaría contar con un modelo de planeación que les permita conocer e implementar una Auditoria de Sistemas	27	96.43%
4ª	Motivos por los cuales les gustaría contar con un modelo de planeación en base a ISO 27000		
	Por el uso e implementación de un nuevo estándar conveniente para el desarrollo de una auditoria mas completa.		
	Obtener nuevos conocimientos		
	Permite evaluar basado en estándares de calidad		
	Especializarse		
5	Capacitaciones sobre Normas ISO que los profesionales en Contaduría Publica han recibido.		
	Profesionales en Contaduría Publica que han recibido capacitación sobre normas ISO	10	30.30%

En el Cuadro anterior, se refiere al conocimiento que el contador público tiene acerca de la normativa ISO 27000 en la auditoría de sistemas, de acuerdo a la investigación realizada, se puede observar que un 84.85% de los profesionales en contaduría publica encuestados, no tienen conocimiento acerca de la

Normativa ISO 27000 y de acuerdo a la ponderación de la frecuencia solamente un 15.15% conoce acerca de la normativa ISO 27000.

Respecto a los Proceso de planeación de la auditoria que permita a los profesionales de Contaduría Publica conocer e implementar una auditoria de sistemas en base a Normas ISO 27000, un 96.43% reconoce que les gustaría contar con dicho modelo de planeación; esto es sumamente importante debido a que ésta auditoría les permite evaluar con mayor eficacia y eficiencia todos aquellos procedimientos que se dan dentro de las rutinas del software que ejecuta o procesa la información.

En función de lo antes mencionado, los motivos por los cuales les gustaría a los profesionales en contaduría pública contar con un modelo de planeación en base a Normas ISO 2700 se encuentran:

- ✓ El uso e implementación de un nuevo estándar conveniente para el desarrollo de una auditoria mas completa,
- ✓ Obtener nuevos conocimientos,
- ✓ Permite evaluar basado en estándares de calidad
- ✓ Especializarse

Es importante mencionar que en nuestro país dichas norma son bastante nuevas y que su publicación asido un poco limitada, en tal sentido son pocos los profesionales en contaduría publica los que han tenido la oportunidad de conocer el contenido de dichas normas; así como también la importancia de estas en los sistemas de información y la incidencia de estas en los trabajos que los profesionales en contaduría publica desarrollan en una auditoria de sistemas. Las normas como se menciona en el capitulo I, son parte de la evolución de las ISO y la constante necesidad de las empresas de presentar información confiable y segura.

Es importante recordar que actualmente el ISO-27000 es el único estándar aceptado internacionalmente para la administración de la seguridad de la información y aplica a todo tipo de organizaciones, tanto por su tamaño como por su actividad, y por consiguiente como profesionales en contaduría publica es importante conocer dichas normas, la información sobre la normas es muy escasa en nuestro país sin embargo esta si existe y puede ser utilizada plenamente en el desarrollo de una auditoria de sistemas con un enfoque tradicional, mas sin embargo en la actualidad no existe un modelo de planeación con dicho enfoque.

2.8.2. Importancia del Desarrollo de Auditoria de Sistemas Con Enfoque ISO 27000

En una auditoria de sistemas implementando normas de calidad ISO, son importantes algunos aspectos entre ellos podemos están:

- ✓ La obtención de resultados confiables, ya que de ello depende tomar decisiones correctas, así mismo mejorar los sistemas y competitividad en las empresas entre otras.

- ✓ Las mejoras en los sistemas y la información que estos generan, partiendo de los resultados de la auditoria con enfoque ISO 27000 las empresas pueden mejorar los puntos o aéreas consideradas deficientes.

- ✓ Calidad, la calidad de la información que los sistemas generan es de vital importancia para toda empresa y mayor aun para las empresas industriales cuyos resultados son importantes en la productividad y toma de decisiones en esta área, es así como los profesionales en contaduría publica sabedores de estos aspectos tan importantes están en busca de la mejora de sus servicios y la implementación de nuevas normas para brindar un mejor servicio a sus clientes.

Conforme al párrafo anterior los profesionales en Contaduría conforme a resultados obtenidos de la investigación de campo consideran que los factores de mayor importancia en el desarrollo de auditoria de sistemas partiendo de una norma de calidad como la nueva normativa ISO 27000 son la obtención de resultados, así como las mejorar de los sistemas y competitividad de las empresas, que pueden partir de los resultados de la auditoria de sistemas con base a las normas ISO 27000 que realicen. (Ver cuadro 2)

CUADRO No.2: IMPORTANCIA DEL DESARROLLO DE LA AUDITORIA DE SISTEMAS RELATIVOS A LA NORMA ISO 27000

No. PREG.	CRITERIOS	CONTADORES PUBLICOS ENCUESTADOS	FRECUENCIA RELATIVA
7	Factores que el contador público considera que son importantes en el desarrollo de una auditoria de Sistemas implementando Normas de Calidad.		
	Obtención de resultados confiables	9	34.62%
	Mejorar los Sistemas y Competitividad en las empresas	8	30.76%
	Calidad de la información	6	23.07%
	Otras	3	11.54%
8	Capacidad de los Profesionales en Contaduría Publica de realizar auditorias de sistemas con enfoque ISO 27000		
	Profesionales en Contaduría Publica que consideran que no han recibido capacitación para realizar auditorias de sistemas con enfoque ISO	28	84.85%

En ésta Parte del diagnóstico, se evalúa la importancia del desarrollo de la auditoria de sistemas implementando normas ISO 2700 tal y como se muestra en el Cuadro anterior, donde el 23.07% de la muestra dice que uno de los factores mas importantes dentro del desarrollo de una auditoria de sistemas con enfoque ISO 27000, es que permite cumplir con la calidad de la información. Los profesionales en un 34.62% consideran que dichas auditorias proporcionarían la obtención de resultados confiables. También, un 30.76% consideran que este tipo de trabajos ayudaría a mejorar los sistemas y la competitividad en las empresas. Por otra parte, los profesionales en contaduría publica en un 84.85% opinan que no se encuentran capacitados para realizar este tipo de auditorias.

2.8.3. Importancia de Contar con un Modelo de Planeación de Auditoria de Sistemas Con Base a Normas ISO 27000

Partiendo del ambiente competitivo en el cual el profesional en contaduría publica se desarrolla es importante contar con un modelo de planeación de auditoria de sistemas con base a normas ISO 27000 el cual permitirá a los profesionales en Contaduría Pública estarían incursionar en el desarrollo en trabajos de auditorías de sistemas bajo dicho enfoque.

El párrafo anterior esta basado en los resultados obtenidos de la investigación de campo en la cual los profesionales en contaduría publica consideran que es de gran relevancia contar con dicho modelo puesto que es novedoso, y ayudaría a evaluar con eficacia la seguridad de la información debido a que cada día es importante realizar auditorias de sistemas que garanticen la confiabilidad de la información. (Ver cuadro 3).

Así mismo, los profesionales en Contaduría Pública hacen énfasis en que si existiera un modelo de Planeación de auditoria de sistemas con base a ISO 27000 lo tomarían en cuenta, ya que dicho modelo les daría la oportunidad de desarrollarse en este campo mas ampliamente y con base a una norma de calidad ISO la cual utilizarían para profundizar cada uno de los puntos o etapas de la auditoria de sistemas con el complemento de evaluarlos con base a los lineamientos que las normas ISO 27000 establece como por ejemplo los controles apropiados, el conocimiento y objetividad para la aceptación de riesgos en los sistemas, la funcionalidad de los mismos entre otros.

Considerando lo anterior los profesionales en contaduría publica expresaron que dicho modelo de planeación permitiría agregar valor a los servicios que ofrecen. (Ver cuadro 3ª)

CUADRO No.3: INCURSIONARÍA EN EL DESARROLLO DE TRABAJOS DE AUDITORIA DE SISTEMAS BAJO UN ENFOQUE ISO 27000 CONSIDERANDO LA IMPORTANCIA DE CONTAR CON UN MODELO DE ESTE TIPO.

No. PREG.	CRITERIOS	CONTADORES PUBLICOS ENCUESTADOS	FRECUENCIA RELATIVA
6	Consideración de los Profesionales en Contaduría Publica en cuanto a tomar en cuenta el ambiente competitivo y su decisión en Incursionar en el desarrollo de trabajos de auditoria de sistemas bajo un enfoque ISO 27000	32	96.97%
9	Profesionales en Contaduría Publica que consideran que es Importante contar con un **Modelo de Planeación de Auditoria de Sistemas con Enfoque ISO 27000**	32	96.97%
10	Consideración de los Profesionales en Contaduría Publica de que si se implementara un modelo de planeación con base a ISO 27000 la información será más confiable.		
	La información seria verificada bajo un estándar de calidad, el cual le daría un voto de confianza adicional	10	31.26%
	Verificación Continua bajo un estándar de este tipo	5	15.62%
	Por ser trabajos con enfoque de calidad la información tendrá una verificación adicional y Se estandarizan los procesos	9	28.12%
	Se aplican lineamientos de otros países, los cuales ya están aprobados y sobre el cual se evalúa la calidad.	4	12.5%
	Se aplican ciertos estándares que permiten asegurar la confiabilidad de la información.	4	12.5%

En el Cuadro anterior, se refiere a que si el contador público incursionaría en una auditoria de sistemas con normativa ISO 27000, de acuerdo a la investigación realizada, se puede observar que un 96.97% de los profesionales en contaduría publica encuestados, consideran que tomando en cuenta el ambiente competitivo en el cual se desarrollan estarían dispuesto a considerar aplicar normas de calidad ISO 27000 en el desarrollo de sus auditorias de sistemas. Así mismo partiendo de lo anterior se observa en el cuadro que un 96.97% de los profesionales encuestados manifestaron su interés por contar con un modelo de planeación de auditoria de sistemas con un enfoque ISO 27000.

En función de lo anteriormente expuesto, las razones por las cuales los profesionales en contaduría pública estarían dispuestos a implementar un **modelo de planeación de auditoria de sistemas con base a Normas ISO 27000** son:

- ✓ La información seria verificada bajo un estándar de calidad, el cual le daría un voto de confianza adicional.
- ✓ Por ser trabajos con enfoque de calidad la información tendrá una verificación adicional y se estandarizan los procesos.

- ✓ Se aplican lineamientos de otros países, los cuales ya están aprobados y sobre el cual se evalúa la calidad.
- ✓ Verificación Continua bajo un estándar de este tipo

- ✓ Se aplican ciertos estándares que permiten asegurar la confiabilidad de la información.

Es importante tomar en cuenta que las ventajas de la implantación de las Normas ISO 27000 en una auditoria de sistemas viene a reforzar el trabajo de los profesionales en contaduría publica en cuanto a la verificación de los sistemas y su concordancia con el estándar de calidad en cuanto al establecimiento de un metodologías de gestión y que permitan una mayor integridad, confidencialidad y confiabilidad de la información mediante la recomendación de seguridades y controles en el personal, datos, hardware, software e instalaciones, así mismo contribuir a identificar las debilidades del sistema y las áreas a mejorar.

La norma ISO 27000 especifica los requerimientos a establecer, poniendo en ejecución, funcionando, supervisando, repasando, manteniendo y mejorando la documentación del sistema de administración en la seguridad de la Información dentro del contexto de la totalidad de los riesgos del negocio, los profesionales en contaduría publica encuestados saben que un estándar con dichas características es importante tomarlo en cuenta, si bien es cierto y conforme a los datos arrojados de la presente investigación son muy pocos los profesionales en contaduría publica los que conocen sobre ISO 27000, esto no exime al resto de conocer y saber de la importancia que toda norma ISO tiene y su incidencia al ser implementada en un negocio o en el desarrollo de un trabajo en especifico.

Como complemento a lo anteriormente expuesto se presenta la opinión de los encuestados en cuanto a que:

2.8.3.1. Si existiera un Modelo de Planeación con base a dicha norma, Tomaría la Decisión de Tomarlo en Cuenta para Ejecutar sus Auditorias de Sistemas".

CUADRO No. 3A: SI EXISTIERA UN MODELO DE PLANEACIÓN CON BASE A DICHA NORMA, TOMARÍA LA DECISIÓN DE TOMARLO EN CUENTA PARA EJECUTAR SUS AUDITORIAS DE SISTEMAS

No. PREG.	CRITERIOS	CONTADORES PUBLICOS ENCUESTADOS	FRECUENCIA RELATIVA
12	Profesionales en Contaduría Publica que Tomarían en cuenta un Modelo de Planeación en base a ISO 27000 en la Ejecución de Auditorias de Sistemas.	32	96.97%
17	Consideración de los profesionales encuestados en cuanto a que existe la oportunidad de aprovechar este campo de auditoria de sistemas con base a ISO, para desarrollarse ampliamente.	27	81.82%
19	La elaboración de un documento como un Modelo de planeación para la auditoria de sistemas con base a normas ISO 27000, seria útil para agregar valor a los servicios que ofrece el Profesional en Contaduría Publica.	32	96.97%

En el Cuadro anterior, podemos observar la opinión de los profesionales encuestados en cuanto a que tomarían en cuenta la ejecución de auditoria de sistemas con base a un modelo de planeación con base en las normas ISO 27000, representando un 96.97% de los encuestados que respondieron afirmativamente ha dicho planteamiento.
Así mismo un 81.82% de los encuestados opinaron que este tipo de auditorias representan un campo de aplicación en el cual se puede tener la oportunidad de aprovecharlo para desarrollarse ampliamente.

Actualmente en el país no se están desarrollando este tipo de trabajos por la falta de un modelo de planeación de Auditoría de sistemas con enfoque en ISO 27000, los profesionales que han decidido incursionar en dicho campo son Administradores de Empresas o Ingenieros en Sistemas, así como también otros profesionales capacitados en el área de ISO, los cuales son pocos en el país; es por eso que dicho campo se plantea como un nuevo reto para los profesionales en contaduría publica.

Como complemento a lo anteriormente expuesto se les planteo a los encuestados la interrogante de que si la elaboración de un modelo de planeación de auditoria de sistemas con base a normas ISO 27000 seria útil para agregar valor a los servicios que ofrecen los profesionales en contaduría publica, respondiendo afirmativamente a dicha interrogante un 96.97% de los encuestados.

En tal sentido, en el Capitulo III de este trabajo de investigación se proporcionará un modelo de planeación de auditoria de sistemas con base a las Normas ISO 27000.

CAPITULO III DISEÑO DE PLANEACION DE AUDITORIA DE SISTEMAS CON BASE A LAS NORMAS ISO 27000 EN LAS EMPRESAS INDUSTRIASLES AFILIADAS A LA ASI

Como parte esencial de toda auditoria, la planeación del trabajo es una base fundamental para todo auditor; en las auditorias de sistemas la planeación del trabajo a realizar es muy compleja y completa a la vez, siendo este el punto de referencia que el auditor de sistemas toma para la ejecución de un trabajo optimo.

La planeación de una auditoria de sistemas esta básicamente dividida en cinco partes:

MP1: Objetivos, responsabilidad, compromiso y términos de contratación.

MP2: Conocimiento del cliente

MP3: Evaluación de los sistemas

MP4: Grafica de Riesgo de Impacto

MP5: Programas de auditoria

Con relación al párrafo anterior, además de las cinco partes en las cuales esta dividido un memorándum de planeación de auditoría de sistemas, se agrega fundamentalmente un cuestionario conocido como ANALISIS DE CHECK LIST, el cual permite conocer en forma generalizada el tipo de sistema informático con el que cuenta la empresa a ser auditada; entre otras aspectos de interés para el auditor; si bien es cierto que existen modelos de planeación de auditoria que cumplen con todas las partes anteriores, ninguno de ellos considera el impacto que las nuevas normas de calidad ISO 27000 están ejerciendo en los sistemas informáticos de las empresas.

Lo anteriormente expuesto se refiere básicamente a que día a día las nuevas tecnologías hacen que las empresas industriales actualicen y mejoren los sistemas que ayudan a buscar la excelencia de sus actividades y que los modelos de auditoria implementados en la actualidad no consideran que las normas de calidad ISO son cada ves mas importantes en las empresas, en tal sentido las evaluaciones que los profesionales en contaduría publica en su calidad de auditores de sistemas realizan, necesitan un nuevo impulso que les permita realizar su trabajo considerando las nuevas normas de calidad. Una auditoria de sistemas que considera las normas ISO27000 permitirá realizar un trabajo en busca de observaciones con

vistas a mejoras en la seguridad de los sistemas de las empresas, específicamente en este caso de las empresas industriales. Una auditoria con base a ISO27000 será una herramienta mas para poder opinar sobre los sistemas informáticos en lo referente a que las compañías puedan contar con una base que les permita organizar la seguridad de la información que generan sus sistemas.

A continuación se presenta un diseño de planeación de auditoria de sistemas dividido en cinco partes, basado en las normas de calidad ISO27000:

MP

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PUBLICOS

Cliente:
Direcciòn:
Telefono:

Descripción	Referencia
ANALISIS DE CHECK LIST	**Ch-list**
PLANEACION	
OBJETIVOS Y TERMINOS DE CONTRATACION	**MP1**
CONOCIMIENTO DEL CLIENTE	**MP2**
CUESTIONARIOS EVALUACION DE SISTEMAS	**MP3**
GRAFICA DE RIESGO DE IMPACTO	**MP4**
PROGRAMAS	**MP5**

3.1. Análisis de Check Listt

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PUBLICOS

Ch-list 1/2

MP

ANALISIS DE CHECK LIST

1. Tipo de sistemas informático con que cuenta la compañía?
2. ¿Si es integrado con cuantos módulos cuenta?
3. ¿Cuenta con la unidad de auditoría interna?
4. ¿Si cuenta cuales son sus planes y cuales son sus áreas críticas?
5. ¿Si es staff, funcional o lineal?
6. El software que se utiliza es propio?
7. Si ésta en outsourcing el software verifique las características del contrato, el plazo y el tiempo?
8. ¿Qué cantidad de hardware posee y en que condiciones?
9. El procesamiento es en línea o en lotes?
10. Que área tiene mayor riesgo para efecto de realizar sus funciones?
11. Tiene medios digitalizados para la captura de datos?
12. Su empresa cuenta con controles internos ? ¿Por quien han sido aprobados?
13. ¿Qué políticas se tienen en el área de sistemas?
14. ¿Cuentan con plan de contingencias?
15. ¿Conocen sobre las normas ISO 27000 aplicables a los sistemas informáticos?
16. Posee controles sobre la información procesada y que genera el sistema informático de la empresa?
17. Poseen controles sobre el acceso a los sistemas informáticos de la empresa?

NOTA: Una vez contestado el check list se procede a tomar datos cuantitativos para efecto de formular la oferta y delimitar el alcance a través de una grafica de riesgos de impacto

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PUBLICOS

Ch-list 2/2

MP

ANALISIS DE CHECK LIST

Como complemento a lo anteriormente expuesto es necesario conocer aspectos legales de la empresa, para lo cual se recure al siguiente cuestionario:

1. Se ha legalizado el sistema contable de la empresa?
2. Se encuentra la empresa Inscrita en la alcaldía municipal?
3. La sociedad esta inscrito en el Ministerio de Hacienda y Ministerio de Trabajo?
4. Se ha tramitado las matriculas de comercio de la empresa.
5. Se ha inscrito en el ISSS y AFP`S?
6. Existe personal extranjero laborando para la empresa, se han verificado sus permisos de permanencia y de trabajo en el país.
7. Fecha de inicio de operaciones

Datos financieros

1. Los archivos de compras se encuentran en forma correlativa?
2. Los archivos de ventas se encuentran en forma correlativa?
3. Numero de facturas a Consumidor Final que se emiten al mes
4. Cuantos documentos de CCF se emiten al mes
5. Valor los ingresos brutos al año

Valor de inventarios

1. Se cuenta con sistemas mecanizados para el inventario y cual método utilizan?
2. El método de depreciación de los activos es constante o variable?
3. Se cuenta con auxiliares de activo fijo?
4. Cual es la política de descargo de los activos fijos?
5. Se realizan inventarios de los activos fijos y cual es la periocidad?

3.2. MP1 Objetivos, responsabilidad, compromiso y términos de contratación.

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 1
1/4

MP

MEMORANDO DE PLANEACIÓN

OBJETIVO Y TÉRMINOS DE CONTRATACIÓN

Objetivo General

Emitir una opinión y una valoración del (alcance) a través de que (de las operaciones vinculadas) del sistema (de la empresa) durante un período de (tiempo de realización de la auditoria) con base a las normas ISO 27000.

Objetivos específicos

- Evaluar el procesamiento electrónico de datos.
- Corroborar y verificar la legalidad del software instalado.
- Determinar el grado de cumplimiento de la seguridad electrónica tanto del hardware como del software.
- Verificar si existen copias de respaldo y cerciorarse que dicho respaldo puedan recuperarse.

Verificar que la Información Financiera suministrada por los sistemas sea confiable a los intereses de los distintos usuarios de información.

NOTA: Los objetivos específicos se hacen en base al objetivo general y luego de cumplimiento a:

a) Riesgo
b) Respaldo
c) Proceso administrativos
d) Emitir opinión

Alcance de la auditoria

Por lo general se secciona en tres partes. Entradas, Procesamientos y Salidas.
Ej.:

El alcance de nuestro trabajo es realizar una auditoria sobre:

1) Evaluación de la integridad, objetividad y eficiencia del modelo relacional.
2) Evaluar y determinar que el software tiene relación con el modelo relacional y se cumple.
3) Evaluar que el PED, cumpla con los objetivos de confiabilidad y comparabilidad de la información procesada.
4) Evaluar que el hardware sea compatible con el software

Una vez seleccionado el alcance se tiene que trabajar en cada área:

1. El trabajo se realiza con muestras selectivas de los datos del sistema a través de las siguientes técnicas:

   Con el modelo relacional se tiene que:

   - Conocer y comprender la ruta critica de cada uno de las llaves principales a sus diferentes módulos
   - Verificar que la ruta critica de los datos actualice las bases de datos pertinentes
   - Evaluar la correlación del modelo relacional

2. Evaluar la transabilidad de la información de tal forma que la información digital sea 100/1 con la información real.

3. Cerciorarse que la compañía cuente con los documentos administrativos de referencias
   - Determinar la exactitud y cumplimiento de lo descrito en el manual versus su impacto en el sistema

De cumplimento.

Revisar y evaluar el control interno informático en lo que respecta al software u al PED:

- Verificar que el PED conlleve las expectativas de la compañía.
  Se tiene que respaldar mediante una carta de salvaguarda para el auditor

Durante la evaluación del sistema de información de la compañía pueden existir incumplimientos e irregularidades relacionados con el procesamiento de la información los cuales no pueden ser cubiertas al momento del análisis por lo tanto las pruebas de cumplimientos sustantivas y de control del trabajo se documentaran con las evidencias virtuales necesarias y las bases de datos fuentes AL MOMENTO DEL EXAMEN por lo tanto las valoraciones de la opinión del auditor se centran en esta documentación de referencia.

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 1
3/4

MP

Responsabilidad de la firma y del auditor

Durante el desarrollo de la auditoria la firma de auditoria o el auditor responsable se compromete a remitir a la gerencia las cartas, informes y reportes que sustentan la realización de un examen sistemático, a si mismo ha emitir una opinión sobre el trabajo desarrollado.

. - Contenido de los informes

1- Descripción de la situación actual de los sistemas de información
(se debe elaborar la grafica de riesgo de impacto y se debe evaluar el grado de importancia con el propósito de encaminar posprogramas cuestionarios y procedimientos para el alcance definido).

2- Descripción detallada de los problemas detectados, posibles causas, repercusiones que pueda tener las alternativas de solución.
Se analiza la grafica de riesgos luego se redacta un resumen administrativo que debe contener 500 palabras y este será el que se envié a la gerencia.

3- Opiniones sobre la razonabilidad de los sistemas
Se evalúa básicamente si el sistema es confiable y en esta parte se le tendrá que decir al cliente la calidad del procesamiento que tiene el sistema de tal forma que la compañía pueda confiar en el resultado del procesamiento de la información.

El informe se hará con base a las NIAS, DIPAS, NORMAS DE AUDITORIA DE SISTEMAS (NIAS) ya que dichas normas se requiere que se ejecute a través de **planeación y evaluación del cont**rol interno Y PROCEDIMIENTOS DE CAPTURA, **PROCESAMIENTO Y SALIDA DE LA INFORMACIÓN.**

Los informes a emitir son:

a) Resumen Ejecutivo
b) Carta a la Gerencia
c) Informe Preliminar
d) Informe Definitivo

Es importante que cada uno de los informes emitidos sea discutido con el personal que la administración de la empresa auditada designe para tal efecto.

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 1
4/4

MP

Compromisos del cliente

La responsabilidad del cliente consistirá en proporcionar las bases de datos, la información impresa, formatos y formularios, manuales y cualquier otro documento que sustente el trabajo a fin de justificar cualquier deficiencia o irregularidad.

Plazo para presentación y discusión de informe

Se debe establecer claramente el tiempo de presentación de los informes, los cuales deberán ser discutidos con la gerencia de la empresa, el plazo de entrega dependerá de los acuerdos y necesidades de la empresa; es decir los plazos quedan a criterio de la firma de auditoria/auditor.

Personal Asignado

El personal que participara en la auditoria deberá estar debidamente identificado para efectos de tener acceso a las áreas mas delicadas de la empresa, así mismo en esta parte del memorandum se deben de anexar los curriculum de los auditores

NOTA: Todo hallazgo encontrado se lleva a una cedula denominada **"Cedula de Hallazgos",** en lazando con hipervínculos e identificando a que MP pertenecen.

Es importante que los papeles de trabajo estén debidamente identificados, por lo cual las referencias se entrelazan unas con otras, es decir partiendo del índice del memorándum todas las hojas que de trabajo subsecuentes deben estar referenciadas. En auditoria de sistemas las referencias se escriben con color rojo, detallando la parte del memo en la que se esta trabajando por ejemplo: MP 1, así mismo el numero de paginas que lo integran 1/4, 2/4,… etc. En el MP 1, es importante tomar en cuenta que cada empresa es como un individuó diferente a los demás, por lo tanto los objetivos, alcance y metodología a seguir dependerá del tipo de compañía con la que se este trabajando; partiendo de los objetivos, requisitos de seguridad, los procesos, los empleados , el tamaño, los sistemas de soporte y la estructura de la organización aun a simple vista o simple inspección se puede hacer una idea de cómo se orientara la auditoria y que cuyas dudas se deben aclarar con el desarrollo de la segunda parte del memorándum de planeación el cual es denominado precisamente como "Conocimiento del Cliente" y se reconoce en el memorándum con las iníciales MP 2.

3.3. MP2 Conocimiento del Cliente

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 2
1/2

MP

CONOCIMIENTO DEL CLIENTE

- Antecedentes.
- Actividad económica
- Estructura accionaria
- Junta Directiva
- Naturaleza
- Representación
- Fecha de fundación
- Domicilio

Lo anterior solo es una pequeña parte de lo que debe contener el memorándum de plantación; por lo tanto en el MP2 es importante conocer y detallar aspectos como:

- Estructura organizativa
  (Colocar nombre y cargo; y marcar con color amarillo en el organigrama los departamentos que tienen relación con la auditoria para hacer una matriz de responsabilidades administrativas)
  Ej.:

Nombre	Cargo
Laura Molina	Contador

Datos claves como:
- mercado nacional
- mercado internacional
- clientes importantes
- proveedores
- ambiente de información

Informe de gestión
- Inflación
- Cumplimiento de presupuesto
- Incremento de los aranceles de importación
- Incremento en los costos de producción
- Obsolescencia de quipos y programas

Esta sección del MP2 debe estar detallada conforme a los resultados que la empresa industrial ha reflejado históricamente, esto para efecto de conocer si los informes o resultados pasados han sido tomados en cuenta para sucesos futuros

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 2
2/2

MP

Leyes y reglamentos especiales

Se debe verificar en esta parte del memorándum, el cumplimiento de las leyes y reglamentos, tanto en lo relativo ha aspectos generales como también aquellas leyes especificas asociadas con las empresas industriales.

Conforme al párrafo anterior se encuentran:

1. Leyes tributarias, tales como: IVA, LISR, Código Tributario y otros.
2. Leyes especificas.

Tomar en cuenta el tipo de empresa que se esta auditando; por ser empresas industriales se debe verificar el cumplimiento de las leyes especificas que se encuentren relacionadas a ella.

3. Ley de fomento al propiedad intelectual
4. Norma Internacional De Contabilidad 38 “Activos Intangibles”

Aspectos Importantes a Considerar

Partiendo de el conocimiento general de la empresa es importante en el caso de las empresas industriales considerar:

- Tamaño de la empresa
- Actividad Económica
- Unidades Sensibles o vulnerables

Es importante conocer el tamaño de la empresa, así como también la actividad económica en el sentido que los centros de costos y gastos se encuentran o no en línea, integrados en el sistema informático de la compañía.

La característica más común por lo general en las empresas industriales es la estrecha relación entre los diferente departamentos que hace que la información y movimientos de las actividades las vuelva mas sensibles.

Se debe detallar en esta parte la relación de los departamentos de la empresa en forma de esquema, considerando su relación en el sistema y el flujo de la información.

Así mismo, especificar en detalle la fecha y número que lo acredita como integrante de la Asociación Salvadoreña de Industria, así mismo las obligaciones y beneficios de esta.

En esta parte del memorándum es importante realizar una descripción de la situación actual del ambiente de los sistemas informáticos, partiendo de las primeras visitas de los auditores a la empresa, para tal efecto se utiliza el siguiente formato:

Nombre del Sistema:
Modelo Relaciona: si posee no posee
Manuales Existentes:
Desde hace cuando existen estos manuales:
En que ambiente esta elaborado el sistema:
Se vale de programas Auxiliares:
Pierde Registros, No cuadra registros, etc.

Se debe realizar una descripción detallada de los problemas detectados, esta parte se complementa con la tercera parte del memorándum: “Cuestionario de Evaluación del Sistema” y se identifica con las iníciales MP 3.

3.4. MP3 Cuestionarios de evaluación del sistema

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 3
1/7

MP

CUESTIONARIO DE EVALUACIÓN DE SISTEMAS

En esta parte del Memorando de Planeación se elaboran y circulan los cuestionarios de evaluación de control interno informático, por lo general siguen las siguientes secuencias:

- Evaluación del hardware
- Evaluación del software
- Evaluación de sistemas

NOTA: Estos cuestionarios constituyen los primeros papeles de trabajo de la ejecución.

Empresa:
Nombre / puesto: **Fecha:**
Nombre de la persona: **Auditor:**

Nº	DESCRIPCIÓN	SI	NO	N/A	COMENTARIOS
	H A R D W A R E				
1	¿Posee la empresa una política de seguridad con respecto al equipo informático?				Verificar la existencia de política de seguridad, respecto al nivel de planeación ante siniestros
2	¿Posee la empresa un detalle de los equipos del área informática? Si es SI, pida el detalle firmado por el Contador.				Verificar la clasificación de la información ya sea por medio de guías, identificación, etc.
3	¿El Departamento de auditoria interna realiza inspecciones físicas al equipo de computo? ¿con que frecuencia es el mantenimiento?				Verificar la existencia de políticas de seguridad y si estas fueron debidamente aprobadas por la Junta Directiva y si verificar si estas han sufrido cambios.
4	¿La empresa realiza o proporciona mantenimiento al equipo de computo?				Verificar los controles de organización interna por parte de la dirección.

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 3
2/7

MP

Empresa:
Nombre / puesto: **Fecha:**
Nombre de la persona: **Auditor:**

Nº	DESCRIPCIÓN	SI	NO	N/A	COMENTARIOS
	H A R D W A R E				
5	Existe una persona responsable del manejo del Hardware?				Verificar el manual de procedimientos a la persona autorizada y verificar la responsabilidad de la dirección
6	La empresa posee clasificadas o identificadas el equipo de computo para cada actividad?				Verificar la organización interna mediante la clasificación de los recursos
7	La empresa proporciona capacitaciones al personal sobre el uso adecuado del equipo?				Verificar los planes de capacitación al personal así como la responsabilidad de la organización interna
8	El equipo de computo es propio o arrendado?				Verificar la administración de los recursos
9	¿Cuentan con un departamento de informática?				Verificar el diseño y planeación de la organización interna de la empresa mediante el compromiso de la dirección
10	¿Existe seguridad en el Voltaje y el cableado en todo el departamento y las terminales conectadas a ella?				Verificar los manual de seguridad por medio de los niveles de planeamiento
11	La empresa posee personal, ya sea interno o externo que efectúe mantenimiento al área del hardware?				Verificar las políticas existentes respecto al mantenimiento del equipo informático
12	Cada cuanto realizan mantenimiento al equipo informático?				Verificar si existe un control de visitas efectuadas al departamento de informática.

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 3
3/7

MP

Empresa:
Nombre / puesto: **Fecha:**
Nombre de la persona: **Auditor:**

Nº	DESCRIPCIÓN	SI	NO	N/A	COMENTARIOS
	S O F T W A R E				
1	¿El software que posee la empresa es enlatado o a la medida?				Conocer el tipo de software que la empresa utiliza y si este es idóneo para las actividades del negocio y su accesibilidad a cambios.
2	En que calidad posee el software? - Propio - Outsourcing - Otros				Se pedirá la licencia o contrato ya que es relevante conocer puesto que pueden enfrentarse a riesgos con terceros.
3	¿El software está acorde a las necesidades de la empresa?				Se verificara esta parte con especial cuidado ya que se debe de evaluar si se administran los recursos en cuanto a los beneficios y costos que representan a la entidad.
4	Cual es la política del procesamiento de información? - En línea - Por lote				Se sugiere que se realice en línea, debido a que la seguridad que representa es mayor.
5	¿Existe modelo relacional impreso?				Si es si, se pedirá una copia y analizará detenidamente la integridad de los saldos a través de las llaves principales, ya que es relevante debido a que se necesitan revisiones independientes por si existen errores.
6	Existe asesoria en el manejo del software? - Manual - Verbal - Informal				Si posee un manual se pedirá una copia digitalizada de este y se revisará si efectivamente explica el manejo, debido a que el correcto manejo del software es parte de la seguridad de la información.

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 3
4/7

MP

Empresa:
Nombre / puesto: **Fecha:**
Nombre de la persona: **Auditor:**

Nº	DESCRIPCIÓN	SI	NO	N/A	COMENTARIOS
	S O F T W A R E				
7	¿Se realizan actualizaciones del sistema?				Se debe mantener actualizado ya que es una responsabilidad para asegurar la información.
8	¿Los reportes generados del sistema contienen los requisitos mínimos de control?				Se pedirá un reporte para verificar si cumplen con los requisitos mínimos de control ya que es una responsabilidad de la dirección que los reportes satisfagan la necesidad de la empresa.

Nº	DESCRIPCIÓN	SI	NO	N/A	COMENTARIOS
	EVALUACIÓN DEL PROCESAMIENTO ELECTRÓNICO DE DATOS				
1	¿Cuenta la entidad con políticas y procedimientos para el procesamiento electrónico de datos?				Se solicitarán ya que forma parte del plan de seguridad y se describen las acciones a llevar a cabo.
2	Cual es la política del procesamiento electrónico de datos? - Línea - Lote				Se sugiere que se haga en línea, debido a que representa mayor seguridad para la información.
3	¿Se verifica que no haya algún error después de procesar los datos?				Se deben realizar revisiones independientes para organizar la información de seguridad.

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 3
5/7

MP

Empresa:
Nombre / puesto: **Fecha:**
Nombre de la persona: **Auditor:**

Nº	DESCRIPCIÓN	SI	NO	N/A	COMENTARIOS
EVALUACIÓN DEL PROCESAMIENTO ELECTRÓNICO DE DATOS					
4	¿El personal encargado del procesamiento electrónico de datos esta capacitado adecuadamente?				Se revisará los programas de capacitación, ya que se debe tomar en cuenta los riesgos que se puedan enfrentar.
5	¿Cumple con los requisitos de la empresa el modelo que genera el sistema?				Los modelos deberán cumplir con las necesidades de la entidad.
6	¿Se realiza periódicamente un back up de la información procesada?				Se debe resguardar la información para la seguridad de la misma.
7	¿Las partidas que se encuentran en el nivel de diario están en orden?				Debido a que se podrían dar riesgos relacionados con terceros.
8	¿Posteriormente procesados los datos se puede realizar alguna modificación en los mismos?				Se deben de poseer autorizaciones para llevarlas a cabo si la hubieran.
9	¿Quién autoriza las modificaciones si las hubieran?				Se deben delegar responsabilidades para asegurar la información.
10	¿Posee la empresa manuales que pueden identificar inconsistencias en los datos?				Se solicitará manuales ya que a través de los mismos se prevén medidas para corregirlos

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 3
6/7

MP

Empresa:
Nombre / puesto: **Fecha:**
Nombre de la persona: **Auditor:**

Nº	DESCRIPCIÓN	SI	NO	N/A	COMENTARIOS
EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA - CONTROL INTERNO					
1	¿Posee la empresa políticas para proteger la información en los sistemas?				Se revisarán las políticas de control interno informático
2	¿Posee la empresa manuales para el resguardo de la Seguridad informática?				Se verificará la existencia de políticas alternativas para prevenir fallas en los sistemas de información.
3	Existe una persona encargada o responsable de la seguridad en el área de informática?				Verificar el manual de procedimientos a la persona autorizada
4	La empresa posee planes para detectar movimientos de siniestros o fuga de la información?				Verificar la existencia de políticas para prevenir fallas en los sistemas de información
5	La empresa utiliza contraseñas o claves para el ingreso de la información al sistema?				Verificar los niveles de responsabilidad en la organización interna por medio de acceso para cada usuario
6	La empresa posee backup o resguardo de la información en caso de fallo?				Verificar la existencia de políticas de resguardo y recuperación de la información ya sea en sitios virtuales o resguardados en lugares externos de las instalaciones
7	Con que periocidad realiza backup de la información?				Verificar el plan de seguridad por medio del manual de procedimientos de control interno informático

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 3
7/7

MP

Empresa:
Nombre / puesto: **Fecha:**
Nombre de la persona: **Auditor:**

Nº	DESCRIPCIÓN	SI	NO	N/A	COMENTARIOS
EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA - CONTROL INTERNO					
8	Posee planes de contingencia para el robo, fraude de información o en caso de un evento catastrófico?				Verificar el manual de seguridad del sistema.
9	La empresa realiza confrontación de datos digitalizados con lo manual?				Verificar por medio de la organización y clasificación de la información una prueba selectiva para verificar la integridad de los datos.
10	Cada cuanto realiza este tipo de confrontaciones?				Verificar las políticas de seguridad del control interno respecto al mantenimiento de equipo informático.
11	Posee la empresa programas que midan el acceso en líneas al sistema por los usuarios en los puntos de redes?				Verificar si existen políticas de control interno informático preventivo. Se debe revisar las diferentes bitacoras,y los niveles de acceso al sistema
12	¿Existen políticas documentadas con respecto a la seguridad lógica?				Los manuales de seguridad del sistema deben ser solicitados y verificar si estos están acorde a los movimientos y uso del sistema
13	¿Se cuenta con programas antivirus para el sistema de información?				Verificar la legitimidad y legalidad de los antivirus en cada maquina y su adecuado mantenimiento o actualización en línea.
14	¿Se efectúa algún tipo de mantenimiento del sistema en las terminales o redes donde está establecido el software?				Revisar los contratos existentes respecto al mantenimiento del equipo informático.

Mediante los cuestionarios anteriormente expuestos se debe tener siempre en mente que la verificación del auditor esta encaminada a los controles existentes de la empresa, la organización de la información mediante los compromisos de la administración, su coordinación y responsabilidad son fundamentales en el control interno de las empresas. De igual forma estas herramientas permiten conocer los riesgos y vacios en la seguridad de los sistemas que poseen las compañías.

El personal involucrado en cada fase deberá ser identificado y verificado conforme a las asignaciones que la administración ha realizado.

Entre los aspectos que se verifican con la evaluación del control de los sistemas están:

- ✓ **Confidencialidad:** Asegurar de que la información es accesible sólo a personal autorizado
- ✓ **Integridad:** Verificación de que exista una garantía de exactitud y completitud de información y métodos de procesado de la información.
- ✓ **Disponibilidad:** Asegurar que los autorizados tengan acceso cuando lo necesiten a la información y que sus claves para entrar al sistema sean las adecuadas.

El MP3 es fundamental para poder establecer una matriz de Riesgos o grafica de riesgos partiendo de los resultados, esta grafica de riesgos es en esencia poner en una balanza las debilidades y fortalezas que la empresa posee en sus sistemas informáticos. Por tanto esta parte se desarrolla ampliamente en la cuarta parte del memorándum de planeación “Grafica de riesgo de Impacto” identificada como MP4.

3.5. MP4 Grafica de riesgo de impacto

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 4
1/2

MP

GRAFICA DE RIESGO DE IMPACTO

La evaluación del riesgo en la auditoria de sistemas se hace partiendo de:

- Cuestionarios

.- Flujo grama o modelo relacional del programa que se esta auditando

.- Grafica de Riesgo de Impacto

En esta parte del memorandum se debe identificar la metodología de valoración de riesgos; así como los diferentes niveles de aceptación .

Análisis y Evaluación de Riesgos

Se valoran los impactos del negocio hacia la organización que puede resultar de cualquier tipo de falla en la seguridad, teniendo en cuenta las perdidas de las confidencialidades, la integridad y disponibilidad de los recursos de las empresas.

INTERRUPCION DEL NEGOCIO					FALLAS DE SEGURIDAD LOGICA Y FISICA										FALLA DE INTEGRIDAD DE DATOS							AUDITORIA AL SCG			
25%					25%										50%							100%			
Catastrofes Naturales	Interrupción de Operaciones	Daño a Equipos	Disturbios sociales	Virus y/o ataques informaticos	Pérdida de Hardware	Perpetuidad de las Claves de Acceso	Inadecuada Instalación	Manipulación de Datos	Interrupción en las redes y comunicaciones	Fallas en Equipo de UPS	Falta de Respaldos	Espionaje y Fraude	Falta de Roles y privilegios de acceso	Fallas de seguridad en la computadora	Falta de Validación de la Integridad Referencial	Diseño de BDD no Normalizado	Fallas en la programación	Inadecuada segregación de funciones	Fallas de funcionamiento de los programas	Digitación incorrecta de Datos	Información erronea	INTERRUPCION DEL NEGOCIO	FALLAS DE SEGURIDAD LOGICA Y FISICA	FALLA DE INTEGRIDAD DE DATOS	
1	2	3	4	5	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	1	2	3	
3.00	1.47	2.00	2.00	3.00	1.18	2.08	2.84	2.00	2.00	2.00	2.00	2.34	3.00	2.00	1.71	1.71	3.00	1.84	1.53	2.29	1.05	2.29	2.15	1.92	0.0
#¡N/D	24%	50%	50%	#¡N/D	9%	54%	95%	50%	50%	50%	50%	67%	100%	50%	36%	36%	#¡N/D	42%	26%	64%	3%	65%	58%	46%	0%
2.29					2.15										1.92							2.07			
65%					58%										46%							53%			
MEDIO					MEDIO										MEDIO							MEDIO			

Calificación del Nivel impacto del Factor de Riesgo				
	1	*Bajo*	*(1.00-1.66)*	*(0.00 - 33.33) %*
	2	*Medio*	*(1.67-2.33)*	*(33.33 - 66.67) %*
	3	*Alto*	*(2.34-3.00)*	*(66.67 - 100) %*

En el grafico anterior se consideran aspectos como el impacto de fallas de seguridad, probabilidad realista de que el fallo ocurra, considerar controles ya en funcionamiento o implantados, estimar niveles de riesgo, y determinar cuando el riesgo es aceptable o requiere tratamiento

En la parte izquierda de la grafica se deben ubicar los aspectos ya mencionados, teniendo en cuenta: organización, tecnología, objetivos del negocio y procesos, amenazas identificadas, efectividad de los controles implantados y eventos externos (cambios de legislación, contratos, etc.)

Una vez efectuada la evaluación del riesgo por cada sector y aspectos del sistema y su entorno, se deben de identificar los riesgos en cada área, así mismo estimar un nivel de ocurrencia de fallas de seguridad, se debe partir de las vulnerabilidades encontradas.

Vulnerabilidades Encontradas	Áreas				
	Software	Hardware	Seguridad Lógica y física	Integridad en datos	R.R.H.H.
	2	1	4	1	1

Dichas vulnerabilidades encontradas deberán ser detalladas a fin de evaluar las áreas con dichas observaciones, mediante la creación y puesta en marcha de los programas de auditoria acordes a cada área de trabajo, poniendo un especial énfasis en las áreas detectadas como con riesgos de impacto mediano y alto.

3.6. MP5 Programas

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
1/1

MP

PROGRAMACIÓN DE LA AUDITORIA DE SISTEMAS EN LAS ÁREAS DE:

SW	**:**	**Software**
HW	**:**	**Hardware**
RH	**:**	**Recursos Humanos**
PED	**:**	**Procesamiento Electrónico de Datos**
SE	**:**	**Seguridad Electrónica**

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
SW 1/7

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento

Componente:

ÁREA SOFTWARE

En este programa se evalúan aspectos importantes como:

- Seguridad
- Procesamiento
- Legalidad
- Eficiencia del Software
- Capacidad y Velocidad del Sistema
- Tipos de procedimientos
- Requerimientos de Seguridad
- Controles

No.	Descripción	Ref	Si	No	N/A	Observación
1	Verifique si existen requerimientos de seguridad de los sistemas informáticos.					Consiste en verificar la existencia de manuales, su conocimiento y aplicación de los mismos, por parte de los usuarios de los sistemas.
2	Verifique el procesamiento correcto de los datos.					Mediante observación describa en una cédula analítica la capacidad del sistema en cuanto a procesamiento y velocidad de transferencia de la información; así como también el cumplimiento de comprobaciones técnicas del sistema. (Cotejar lo digitalizado contra lo físico, mediante muestra selectiva).

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
SW 2/7

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento
Componente:

AREA SOFTWARE

No.	Descripción	Ref	Si	No	N/A	Observación
3	Verifique el tipo de procesamiento del sistema y las rutinas del manejo de medios.					Consiste en verificar el tiempo de traslado de la información de una terminal al servidor, el tiempo prudencial es de 3 segundos. En cuanto a las rutinas se refiere a la existencia de respaldos de la información, ya sea en discos, cintas, papeles, compact disk, etc. esto se plantea en una cédula a parte como cédula analítica. (ver los programas de las áreas de cumplimiento).
4	Cerciórese de la seguridad en los sistemas de archivos.					Se debe revisar el tipo de protección que poseen los datos y la privacidad de la información, la protección de registros y la prevención y regulación de controles criptográficos.
5	Cerciórese de la existencia de códigos de protección al sistema.					Se realiza una verificación a los controles físicos de entrada a los sistemas, los perímetros de seguridad y las claves de acceso.
6	Verifique la compatibilidad del software con el tipo de red existente.					Verificar la existencia de cambios en las redes, que pudieran afectar al sistema en general, el acceso a las redes por parte de los usuarios y sus autorizaciones a los sistemas.

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
SW 3/7

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento

Componente:

ÁREA SOFTWARE

No.	Descripción	Ref	Si	No	N/A	Observación
7	Verificar si existen métodos de medida de la eficiencia del software y su aceptación por parte del personal.					Realizar entrevistas, o mediante el uso de cuestionarios indagar con el personal que utiliza el software si este es satisfactorio para el desarrollo de sus funciones y su facilidad en el manejo de los modulos
8	Identificar la administración continua del negocio, es decir sus compromisos con aspectos de seguridad.					Considerar particularmente: a) Compromiso de la dirección con la seguridad de la información. b) Coordinación de la seguridad del sistema y la información. c) Asignación de Responsabilidades. d) Monitoreo.
9	Verificar que el software de instalación sea coherente con el sistema de información implementado a fin de dar cumplimiento a la norma ISO 27000					
10	Evalué que la salida de información cumpla con las características indicadas en el manual de operación del sistema					Es importante evaluar que lo establecido en el manual sea coherente con lo realizado.
11	Evalué el análisis y gestión de los registros que se procesa en el sistema de información					
12	Elabore una cedula de confrontación para. evaluar el intercambio físico de la información y la generada por el sistema.					
13	Verifique los errores presentados en el sistema, con el fin de identificar y establecer las mejoras continuas en el sistema.					

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
SW 4/7

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento
Componente:

ÁREA SOFTWARE

No.	Descripción	Ref	Si	No	N/A	Observación
14	Elabore una cédula narrativa donde se identifique las posibles respuestas a los errores del sistema de información					
ÁREA DE CUMPLIMIENTO - SEGURIDAD DE BACK-UP						
15	Cerciórese que la base de datos cree un archivo de respaldo de las principales aplicaciones del Sistema de Información					Es importante evaluar si quedan registros de respaldo de las aplicaciones del sistema para efecto de seguridad.
16	Verifique si existe backup en línea. Si existe, asegúrese que cumpla con las necesidades básicas para posibles restauraciones.					identificar si los back up son totales o parciales; es decir si son por aéreas o terminales, ó si es un respaldo de las operaciones en su conjunto.
17	Cerciórese que la información de las copias de respaldo cumplan con los requerimientos establecidos por las Normas de Auditorias de Sistemas (NAS)					
18	Verifique que las copias de respaldo virtual cumplan con los requerimientos mínimos de la seguridad lógica de los sistemas de información					
19	Verifique si hay planes de contingencia que prevenga las posibles pérdidas de información de manera oportuna y eficaz					La norma establece que deben existir planes de contingencia; es importante verificar si la empresa los posee y si estos son oportunos.
20	Evalué mediante la observación al departamento de ventas y contabilidad si el resguardo de la información se efectúa en medios efectivos y seguros					Es necesario incluir al área de producción, en el caso que esta se encuentre formando parte del sistema.
21	Asegúrese que los planes de contingencia estén escritos y se cumplan					

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
SW 5/7

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento
Componente:

ÁREA SOFTWARE

No.	Descripción	Ref	Si	No	N/A	Observación
ÁREA DE CUMPLIMIENTO - SEGURIDAD DE BACK-UP						
22	Cerciórese que los planes de continuidad estén aprobados por la Junta Directiva y por el profesional competente					
ÁREA DE CUMPLIMIENTO - SEGURIDAD CONTRA VIRUS						
23	Verifique los requerimientos de seguridad para poder realizar cambios, adiciones o eliminaciones al sistema					Identificar la accesibilidad al sistema mediante inspección a las actividades relacionadas.
24	Cerciórese que exista la seguridad lógica adecuada para el envió y captura de información por correo electrónico					Es necesario verificar las líneas de intercambio de información, las cuales deben ser seguras
25	Verifique la adición y modificación de soporte en línea de sistema de información					Identificar la accesibilidad y uso de paswords
26	Elabore una cédula de confrontación para evaluar el intercambio físico de la información					
27	Verifique que la comunicación de los errores en los sistemas se evalué de forma recurrente.					Realizar con el propósito de identificar la mejora continua de los sistemas de información
28	Elabore una cédula narrativa donde se identifiquen las posibles respuestas que se le han dado a los errores del sistemas de información					

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
SW 6/7

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento

Componente:

ÁREA SOFTWARE

No.	Descripción	Ref	Si	No	N/A	Observación
ÁREA DE CUMPLIMIENTO - SEGURIDAD CONTRA VIRUS						
29	Cerciórese que la empresa tenga implementado un plan de continuidad a fin de seguir y perseguir dados validos e inválidos					Identificar si estos existen por escrito y su aplicabilidad, solicitar copias.
30	Cerciórese que la base de datos y sistemas de información general estén protegidos contra códigos maliciosos y códigos de captura móvil de información.					
ÁREA DE CUMPLIMIENTO - LEGALIDAD						
31	Verificar el medio por el cual fue adquirido el sistema.					solicitar copia de la licencia y de los comprobantes de compra.
32	Verifique que los sistemas públicamente de datos cumplan con los requerimientos legales y contractuales del país.					
33	Verifique la legalidad del software mediante la licencia del mismo.					Se deben verificar los cambios o trasformaciones en el sistema y la responsabilidad asumida por la gerencia en la aprobación de dichos cambios así como también la vigencia de contratos relacionados con el mismo.

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
SW 7/7

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento
Componente:

AREA SOFTWARE

No.	Descripción	Ref	Si	No	N/A	Observación
	ÁREA DE CUMPLIMIENTO - LEGALIDAD					
34	Verifique que la administración este comprometida con el cumplimiento de normas y leyes vigentes del país, así como su cumplimiento.					
35	Cerciorarse que el módulo de contabilidad del sistema se encuentre debidamente identificado, a fin de corroborar la no duplicidad de datos.					Inspeccionar el uso adecuado del modulo de contabilidad, verificar el modulo relacionar
	ÁREA DE CUMPLIMIENTO - UNIDAD INFORMÁTICA					
36	Verificar el compromiso de la unidad informática con el sistema de gestión de calidad					
37	Verificar que las sugerencias hechas por el equipo de auditoria anterior hayan sido tomadas en cuenta como parte de la mejora continua.					Solicitar informe de auditoria de sistemas, (si existe) y hacer inspección sobre los puntos críticos identificados.
38	Verificar que los planes de mantenimiento preventivo para el área del software exista					Evaluar si son los mas adecuados.
39	Verificar que los cambios de personal que se han realizado en el departamento de informática hayan adoptado la filosofía del modelo					Indagar si existen adiestramiento al nuevo personal.
40	Evalúe el compromiso de la gerencia					
41	Confronte si es coherente lo establecido en el manual de control de calidad con las expectativas del software de la mejora continua y en su conjunto del sistema de calidad					Si no existe un manual de control de calidad, observar en los pts. dicha ausencia.
42	Verificar la independencia de la unidad de informática					
43	Cerciórese que la unidad informática cumpla con los requerimientos mínimos establecidos de la gerencia					Cotejar lo establecido en los manuales y notificaciones (ordenes establecidas por la gerencia) con el ambiente y uso en la unidad informática.

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
HW 1/4

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento

Componente:

ÁREA HARDWARE

En este programa se evalúan aspectos importantes como:

- Capacidad
- Seguridad
- Derechos y Obligaciones
- Mantenimiento
- Vida Útil
- Ambiente
- Comunicación

No.	Descripción	Ref.	Si	No	N/A	Observación
1	Cerciórese de la procedencia del equipo de hardware, verifique si el hardware está codificado. Los requerimientos de seguridad del hardware deben ser identificados.					Deberá de Revisarse detenidamente la documentación de respaldo del equipo
2	Realice un del listado del hardware e identifique el más importante.					Anexe la lista y se marca con color el equipo más relevante (servidor, redes, protocolos, terminales e impresor). La clasificación del hardware por su nivel de importancia colaborará a identificar su nivel y grado de obsolescencia.
3	Realice una cédula de trabajo en la cual describa las condiciones en las cuales se encuentra el hardware identificado como más importante.					

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
HW 2/4

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento
Componente:

ÁREA HARDWARE

No.	Descripción	Ref.	Si	No	N/A	Observación
4	Elabore una cédula principal que incluya las áreas a evaluar de cada componente y se define por prioridades.					En dicha cédula se deben incluir aspectos como: modelo, marca, velocidad o capacidad, vida útil, compatibilidad, partes modificadas, aspectos añadidos, etc.
5	Determine mediante una entrevista si existe vigilancia en el centro de computo. Obtenga un croquis de la ubicación del hardware dentro de la compañía.					Este aspecto servirá para determinar uno de los aspectos de seguridad que la norma establece, en la cual se deben de contar con medidas de seguridad a la protección del activo fijo.
6	Haga una inspección al Centro de Computo y evalué las condiciones del ambiente.					Se hace una narrativa y los puntos que más se evalúan son los siguientes: - Aire Acondicionado bajo 16º - Espacio entre una maquina y otra (1 metro) - Cables con técnica de ratón (no a la vista) - Ingreso al centro de computo (verificar si no hay restricciones, si esta delimitada el área, etc.). Hay que detallar cada una de las condiciones encontradas a fin de identificar vulnerabilidades

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
HW 3/4

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento
Componente:

ÁREA HARDWARE

No.	Descripción	Ref.	Si	No	N/A	Observación
7	De la inspección identifique las no conformidades en cuanto a la eficiencia y eficacia de la realización de cada hardware que encuentre.					
8	Investigue el tipo de mantenimiento que se le da al hardware - Definir si es interno o externo - Frecuencia con que se le da mantenimiento - Si el mantenimiento es preventivo, correctivo o emergente.					En este punto deberá ser identificado en forma clara y detallada el tipo de mantenimiento que posee la empresa y la responsabilidad de la administración ante las vulnerabilidades por la carencia de mantenimiento al equipo.
9	Identifique el nivel de compromiso de la administración para con el área del centro de computo o equipo que poseen en cuanto a las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad del equipo.					Principalmente: - Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores; - Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
HW 4/4

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento
Componente:

ÁREA HARDWARE

No.	Descripción	Ref.	Si	No	N/A	Observación
10	Verifique que el acceso a las partes internas del hardware estén con seguridad, es decir verificar que los discos duros de las máquinas se encuentren resguardados.					Se refiere a que se debe verificar que estén resguardados mediante sellos en las Unidades Centrales de Procesamiento.
11	Revisión de protección y tendido adecuado de cables y líneas de comunicación para evitar accesos físicos.					
12	Análisis de la Seguridad de Acceso a cada área o departamento diferente de la asignada.					Inspeccionar el área y su accesibilidad

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
RH 1/4

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento

Componente:

ÁREA RECURSOS HUMANOS

En este programa se evalúan aspectos importantes como:

- Obligaciones
- Ambiente
- Derechos
- Cualidades
- Responsabilidades
- Comunicación

No.	Descripción	Ref	Si	No	N/A	Observación
1	Cerciórese que la empresa posea un organigrama general de cada departamento o área.					Solicitar organigramas
2	Realizar visitas a cada área y verificar los procedimientos en los departamentos.					
3	Verificar que existan manuales de organización y descripción de cada uno de los departamentos.					Identificar en los manuales si se encuentran detalladas las actividades del personal.
4	Verifique que exista una adecuada segregación de funciones dentro de la empresa.					
5	Verifique si hay planes de contingencia por parte de los empleados que prevenga las posibles pérdidas de información de manera oportuna y eficaz.					Indagar con los empleados si estos conocen las medidas a tomar en caso de sucesos imprevistos en el sistema.
6	Evalúe mediante la observación a los departamentos si los puestos de trabajo son adecuados a las necesidades y objetivos que tiene cada área para llevar a cabo sus funciones					

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
RH 2/4

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento

Componente:

ÁREA RECURSOS HUMANOS

No.	Descripción	Ref	Si	No	N/A	Observación
7	Cerciórese que los empleados de la empresa poseen conocimientos y comprensión de las políticas y procedimientos establecidos					
8	Cerciórese que los empleados de la empresa se encuentran capacitados para utilizar el equipo de computo					Verificar la existencia de planes de capacitación y su periocidad y desarrollo.
9	Verificar que los cambios que el sistema ha sufrido han sido explicados a los usuarios del sistema					Indagar con los empleados la adecuada comprencion del sistema y los cambios sufridos.
10	Cerciórese que la empresa imparte formación entre los empleados sobre los nuevos procedimientos que se van a implantar					
11	Verificar que la empresa establece un programa de concientización de la seguridad de la información entre el personal					Verificar su periodicidad
12	Cerciórese que los usuarios involucrados reciben la formación adecuada que les capacite para desempeñar su papel en los mismos.					
13	Verificar que el personal para el desarrollo de las funciones del área es suficiente					
14	Cerciórese que se realicen todas las actividades con el personal asignado					

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
RH 3/4

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento

Componente:

ÁREA RECURSOS HUMANOS

No.	Descripción	Ref	Si	No	N/A	Observación
15	Verificar que el trabajo realizado es eficaz y que sea adecuada la calidad del mismo					
16	Verificar si el personal es discreto en el manejo de la información confidencial					Indagar sobre incidentes anteriores
17	Identificar si existen necesidades actuales y futuras de capacitación del personal del área					Tomar en cuenta la comprensión y manejo del sistema por parte del personal.
18	Cerciórese que los resultados de los programas de capacitación sean evaluados y conocidos.					Identificar si son evaluados y conocidos por los superiores a fin de mejorar el desempeño actual
19	Verificar si la supervisión de las actividades del personal es de acuerdo a las políticas de la empresa					
20	Cerciórese que las condiciones ambientales del área de trabajo son adecuadas para el desarrollo de las actividades					
21	Verificar si el personal de la empresa posee conocimientos sobre la responsabilidad y el compromiso de cumplir con un sistema de calidad					

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
RH 4/4

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento

Componente:

ÁREA RECURSOS HUMANOS

No.	Descripción	Ref	Si	No	N/A	Observación
22	Cerciórese que exista formación que ayude a completar con una labor de sensibilización a base de charlas, reuniones y carteles, y con la exigencia de la documentación que acredite la correcta gestión de su actividad.					
23	Verificar que el personal en todos los niveles de la organización se encuentre comprometido (S) y utilizadas en beneficio de la empresa					
25	Determinar si la competencia necesaria para el personal que interviene en los procesos para la realización del producto conforme a los procedimientos					

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
PED1/7

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento

Componente:

ÁREA PROCESAMIENTO ELECTRÓNICO DE DATOS

En el procesamiento electrónico de datos se debe evaluar la segmentación y confiabilidad del sistema, en tal sentido los aspectos básicos son:

1) Integridad
2) Bacheo
3) Proceso de Información

No.	Descripción	Ref.	Si	No	N/A	Observación
1	En una cédula describa el tipo de sistema que posee la empresa.					Especificar el tipo de procesamiento, el tipo de indexa miento y las rutas de impresión.
2	Describir la capacidad del disco duro de la maquina y la calidad del procesamiento, así como también la compatibilidad del sistema operativo y de las aplicaciones.					
3	En una cédula especifique el tipo de modelo relacional del sistema y verifique las tablas en SQL.					
4	Investigué la existencia de separación de funciones dentro del PED. Así mismo verificar el acceso a la información y programas.					Es decir si existe una separación entre los programadores y los operadores.
5	Detallar en una cédula la periodicidad de las revisiones de los informes en uso.					Se refiere a los registros históricos.
6	Verifique si existe mantenimiento de los registros de transacciones y controles de lotes, así como también las entradas en línea.					

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
PED2/7

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento

Componente:

ÁREA PROCESAMIENTO ELECTRÓNICO DE DATOS

En el procesamiento electrónico de datos se debe evaluar la segmentación y confiabilidad del sistema, en tal sentido los aspectos básicos son:

1) Integridad
2) Bacheo
3) Proceso de Información

No.	Descripción	Ref.	Si	No	N/A	Observación
7	Verifique que las políticas y manuales relacionadas con el PED han sido comunicadas por el personal involucrado en el área y su adecuada implementación.					Cada área involucrada en la captura de datos deberá conocer sobre las políticas y manuales por lo tanto es importante indagar en cada una de ellas.
8	Verificar si la empresa cuenta con claves de usuario diferentes para cada empleado					
9	Verificar que existan claves de acceso dependiendo de los niveles jerárquicos					
10	Verificar si cada clave o password asignado permite la realización de todas las funciones del sistema					
11	Cerciorarse de las políticas de acceso a la red e Internet por parte de los usuarios					
12	Verificar si el personal posee acceso al sistema operativo					
13	Verificar si los usuarios del sistema poseen acceso a cambios de contraseña o password					
14	Verificar el acceso a los archivos o bibliotecas de la información					

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
PED3/7

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento
Componente:

ÁREA PROCESAMIENTO ELECTRÓNICO DE DATOS

No.	Descripción	Ref.	Si	No	N/A	Observación
15	Cerciorarse que existan controles de software para limitar el acceso al sistema por personal no autorizado					Inspeccionar que los controles existentes están funcionando.
16	Averigüe que tipo de restricciones se han implantado al acceso de los usuarios.					Compruebe que solo tengan acceso las personas autorizadas a la información que se maneja
	CAPTURA DE LA INFORMACIÓN					
17	Obtenga el modelo relacional y verifique la forma de captura de la información					
18	Verifique como es que se realiza la captura de datos y que medios de captación utiliza.					Como por ejemplo: Manual, digital o ambos a fin de medir el grado de confiabilidad
19	Verificar la captación de datos por parte de las personas encargadas					
20	Cerciórese que la captación de datos se está haciendo de acuerdo a las políticas y procedimientos de la empresa					
21	Cerciórese que la captura de datos se está haciendo a través del modulo y de las opciones adecuadas a fin de alimentar los diferentes módulos interrelacionados					
22	Verificar sobre la forma de trabajar en el área de captación de datos e indique si existen órdenes de trabajo.					

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
PED4/7

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento
Componente:

ÁREA PROCESAMIENTO ELECTRÓNICO DE DATOS

No.	Descripción	Ref.	Si	No	N/A	Observación
23	Verifique si existe un programa de trabajo en el área de captación de datos.					Señalar las prioridades de la información.
24	Investigue si existen lineamientos por escrito respecto al tratamiento que se le debe dar a la información no válida, ya sea por falta de firmas legibles, no corresponden las cifras de control, etc.					
25	Verificar que la captura de datos coincida con los documentos fuentes reales.					Cotejar y llenar cedula
26	Verifique que los documentos de compra ingresados en el sistema, estén de acuerdo a los comprobantes de crédito fiscal físicos.					Realizar captura de pantallas de ser necesario para respaldar lo encontrado.
27	Verifique que el procesamiento de las órdenes de producción esté en función de los datos reales.					
28	Verifique que el ingreso del producto terminado esté función del proceso de costeo en el modulo de costos.					
29	Verificar si la empresa posee políticas de control sobre la captura y envío de la información procesada					
PROCESAMIENTO DE LA INFORMACIÓN						
30	Revisar el manual de usuarios del sistema y verificar que se utilice de acuerdo a lo establecido.					

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
PED5/7

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento
Componente:

ÁREA PROCESAMIENTO ELECTRÓNICO DE DATOS

No.	Descripción	Ref.	Si	No	N/A	Observación
31	Investigue que los módulos funcionen adecuadamente, tal como lo establece el manual.					
32	Verifique que el sistema tenga rutinas de costeo, indexa miento o autorización automática.					
33	Verifique que una vez digitados los datos existe un respaldo interno a través de un archivo DLL ; que se pueda recuperar la información.					El archivo DLL es un archivo oculto que se genera en el sistema, son como una biblioteca de funciones compartida.
34	Verificar si la información que se migra de los módulos se hace adecuadamente.					
35	Cerciórese que la información procesada dentro del sistema es confiable.					La información que ha sido procesada no se pueda modificar o alterar cifras a su conveniencia
36	Realizar pruebas del procesamiento electrónico para monitorear el tráfico de la información					
37	Verifique los reportes del sistema, de tal forma que el reporte contenga lo que el usuario necesita					

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
PED6/7

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento
Componente:

ÁREA PROCESAMIENTO ELECTRÓNICO DE DATOS

No.	Descripción	Ref.	Si	No	N/A	Observación
38	Verifique la frecuencia con que se generan los reportes					
39	Verifique si los reportes coinciden con lo que se ve en pantalla, con lo procesado, con lo grabado versus lo real					Realizar captura de pantallas
40	Verifique si los traslados de la información de inventario y de costos es coherente con el modulo contable					Cotejar información
41	Verificar las operaciones qué haya hecho en línea sean conforme a los requerimientos de la compañía					
42	Verifique que los datos digitados por el personal correspondan al producto que se está elaborando					
43	Verifique que las compras que se han procesado concuerden con los documentos reales de IVA					
44	Verifique que las averías, los desperdicios o las salidas por ajuste estén registradas adecuadamente en el sistema.					En función de los códigos y a la ocurrencia
45	Verifique que las variaciones calculadas en el sistema sean coherentes versus la real					

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
PED7/7

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento
Componente:

ÁREA PROCESAMIENTO ELECTRÓNICO DE DATOS

No.	Descripción	Ref.	Si	No	N/A	Observación
	SALIDA DE LA INFORMACIÓN					
46	Verifique que el personal haga un backup					Los backup deben guardarse adecuadamente y ser entregados a la administración
47	Verifique que la administración tenga una bitácora o un archivo seguro					Partiendo del punto de programa anterior hay que dar seguimiento a la protección de los respaldos.
48	Verifique si hay seguro que cubra el equipo electrónico y que cubra ante cualquier pérdida de información					
49	Verifique que la salida de datos en pantalla, impresa, o en disquete sea coherente en función del sistema					
50	Verifique que se pueda restaurar la información					Se refiere a que haya una llave de seguridad para restaurar el sistema
51	Verifique que por seguridad, la información no se pueda extraer por cualquier medio magnético flexible					principalmente que el proceso de salida de sistema esté autorizado
52	Verifique la impresión de los documentos después de cierta revisión del personal autorizado					

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
SE 1/5

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento
Componente:

ÁREA DE SEGURIDAD ELECTRÓNICA

En la seguridad electrónica se debe basar desde dos puntos de vista:

1) Seguridad Lógica

2) Seguridad Física

No.	Descripción	Ref.	Si	No	N/A	Observación
1	Verificar la existencia de políticas y procedimientos sobre la seguridad al equipo, software y la información para garantizar su integridad; además, de un plan de contingencias para la restauración del sistema					
2	Verificar si se cuenta con instructivos o manuales para uso del sistema y si se proporciona a las personas que intervienen en la operación rutinaria que procesa la información de la compañía contratante					
3	Verificar la protección del equipo de cómputo contra fallas en el sistema eléctrico					Cerciórese si ante cualquier falla en el flujo eléctrico del sistema, éste no se cierra sin antes haber guardado toda la información que se estaba procesando en ese momento y para que evite daños físicos a los equipos por parte del personal
4	Verificar si cada estación de trabajo cuenta con su propio UPS.					Es importante que cada UPS cuenta con un tiempo mínimo de duración de 10 minutos, con una capacidad de 500 VA

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
SE 2/5

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento
Componente:

ÁREA DE SEGURIDAD ELECTRÓNICA

No.	Descripción	Ref	Si	No	N/A	Observación
5	Verificar si se cuentan con los planos de instalación eléctrica actualizados					
6	Cerciórese que las instalaciones eléctricas del equipo de computo este independiente de otras instalaciones eléctricas					
7	Verificar si el personal conoce las medidas de seguridad en caso de incidentes.					Verificar si la empresa cuenta con alarmas
8	Cerciórese que el personal de la empresa se encuentre adiestrado en la forma en que deben de desalojar las instalaciones en caso de emergencia					
9	Verificar si se cuenta con copias de los archivos en un lugar distinto al de la computadora					Considerar si la información almacenada se encuentre debidamente actualizada e identificada
10	Verificar si se encuentran registradas las violaciones a los procedimientos con el fin de llevar estadísticas y frenar las tendencias a mayores					
11	Verificar las acciones de los operadores con el fin de evitar que realicen acciones que puedan dañar el sistema					

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
SE 3/5

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento

Componente:

ÁREA DE SEGURIDAD ELECTRÓNICA

No.	Descripción	Ref	Si	No	N/A	Observación
12	Verificar si se controla el trabajo fuera de horarios					
13	Cerciórese que los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos					
14	Comprobar si se cuenta con los derechos de autor de los sistemas a ser utilizados					
15	Averigüe que tipo de restricciones se han implantado al acceso de los usuarios.					Compruebe que solo tengan acceso las personas autorizadas a la información que se maneja
16	Verificar si se da cumplimiento a lo establecido sobre la realización de evaluaciones periódicas al sistema					
17	Verificar cada cuanto se crea el backup de la información utilizada					
18	Verificar si se comunica oportunamente sobre las modificaciones a los programas de trabajo					
19	Revisar el procedimiento que se efectúa al momento de almacenar la información en el sistema					
20	Cerciórese que las tareas asignadas en el área de cómputo se desarrollan según lo establecido en los manuales.					Se refiere a los manuales de descripción de puestos en cuanto a la seguridad de la información

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
SE 4/5

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento
Componente:

ÁREA DE SEGURIDAD ELECTRÓNICA

No.	Descripción	Ref	Si	No	N/A	Observación
21	Verificar que la seguridad en el manejo de la información procesada no sea riesgosa					
22	Cerciórese que todos los medios magnéticos de respaldo no se encuentren almacenados en un mismo lugar.					Esto con el fin de que en caso de contingencia no se tenga el riesgo de perder parte o la totalidad de la información
23	Verifique que el acceso al área de almacenamiento o de respaldo sea restringido					
24	Cerciórese que el operador no pueda modificar los datos de entrada					
25	Cerciórese que las llaves de acceso se encuentren encriptados.					Con el objetivo de averiguar que ayude a reducir el riesgo de acceso por otras personas
26	Verifique que el acceso al software del sistema operativo este restringido					
27	Cerciórese que existan normas que definan el contenido de los instructivos de captación de datos					
28	Verificar si existe control por el personal sobre las entradas de documentos fuentes.					
29	Verifique si la empresa cuenta con procedimientos de control sobre la información antes del proceso de captura de datos					
30	Verifique los procedimientos a seguir en caso de que exista infamación inválida					

XYZ Y ASOCIADOS, S.A. DE C.V.
CONTADORES PÚBLICOS

MP 5
SE 5/5

MP

Empresa Auditada :
Fecha Inicio:
Fecha de Finalización:
Fase de Ciclo de Vida de los Sistemas: En Funcionamiento
Componente:

ÁREA DE SEGURIDAD ELECTRÓNICA

No.	Descripción	Ref	Si	No	N/A	Observación
31	Cerciórese que la empresa posea un registro de anomalías en la información debido a la mala codificación y como solucionar dichos problemas					
32	Verifique si existe un registro de los documentos que han sido ingresados en el sistema					
33	Verifique si la empresa realiza reportes diarios y si son confrontados con los documentos físicos					
34	Verifique si existe un control que asegure la justificación de los procesos en el computador					
35	Cerciórese que la empresa posea procedimientos para evitar las corridas de programas no autorizadas					

CAPITULO IV - CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Se concluye que a pesar que el Contador Público considera importante el desarrollo profesional en el área de una auditoria de sistemas, la mayoría no los incluye dentro sus servicios, aún cuando las empresas utilizan sistemas de información para el procesamiento de datos; además consideran que para evaluar el entorno informático es necesario la ayuda de un experto. Todo lo anterior se debe a que no se tiene personal capacitado para explotar las áreas de auditorías de sistemas con dicho enfoque, con herramientas que proporcionen lineamientos mínimos a seguir en una auditoría de sistemas de dicha índole.

2. Se concluye que el profesional de la contaduría pública necesita de una herramienta que le permita conocer los lineamientos básicos tanto a nivel teórico como a nivel práctico sobre normas de calidad ISO 27000, a efectos de poder efectuar una auditoría de sistemas con base a dicha norma en empresas industriales que poseen sistema de información, lo cual constituye el primer obstáculo para desarrollarse en este campo y consecuentemente dificulta la competitividad de sus servicios.

3. En conclusión el poco conocimiento del profesional en lo relativo a esta área de la auditoria con base a normas de calidad ISO 27000, se debe a la escasa difusión en lo que respecta a la normativa técnica que la rigen en relación a planeación, ejecución e informe de la misma, por tanto se encuentran al margen de las innovaciones sobre áreas de interés que le competen al contador publico y dejan de ejercerlas lo cual permite que otros profesionales distintos a este estén desarrollándolos.

RECOMENDACIONES

En base a las conclusiones antes expuestas, se formulan las siguientes recomendaciones:

1. Se recomienda la capacitación por parte de los profesionales en contaduría pública referente a las auditorias especializadas como lo es la auditoria de sistemas, los conocimientos adquiridos se enriquecerán y ampliaran mediante las capacitaciones y la educación continua.

2. Se recomienda el uso e implementación de un modelo de planeación de auditoria de sistemas con base a las normas de calidad ISO 27000; como herramienta que le permita incursionar en el campo de las auditorias de sistemas en base a las normas de calidad ya mencionadas.

3. Recomendamos que es exista una mayor difusión de las normas de calidad ISO 27000 por parte de las autoridades competentes, tanto en la rama de los profesionales en contaduría publica como de aquellos organismos interesados en la mejora continua de las empresas, en tal sentido el instituto de profesionales en contaduría publica y la asociación salvadoreña de industrias.

BIBLIOGRAFÍA

Asamblea Legislativa de El Salvador. Año 2006. "*Código Tributario".* Editorial Jurídica Salvadoreña. San Salvador, El Salvador

Asamblea Legislativa de El Salvador. Año 2006. *"Ley de Renta".* Editorial Jurídica Salvadoreña. San Salvador, El Salvador.

International Accounting Standards Board. Año 2006. "Normas Internacionales de Auditoría". Departamento de Publicaciones IASB. Londres. Inglaterra.

Jovel Jovel, Roberto Carlos. Año 2008. "Guía Básica para Elaborar Trabajos de Investigación". Imprenta Universitaria, U.E.S., El Salvador.

Lamprecht, James L. Año 2000. Segunda Edición. "ISO 9000, Manual de Implementación". Editorial Panorama. España.

Martínez Mendoza, Licda. María Margarita. Año 2007. *"Apuntes de Cátedra impartida en Auditoría de Sistemas"*. Universidad de El Salvador. San Salvador, El Salvador.

Rothery, Brian. Año 1993. Segunda Edición. *"ISO 9000".*
Editorial Panorama. España.

Rubio, Ing. Jaime H. Año 2006. *"Conociendo ISO 27000"*
Universidad de Colombia. Colombia.

www.geocities.com/gehg48/Aef27.html

www.iso27000.es/iso27000.html

A N E X O S

CONTENIDO DE LOS ANEXOS:

ANEXO 1	**ENCUESTA**
ANEXO 2	**TABULACIONES**
ANEXO 3	**RESUMEN ISO 27000**
ANEXO 4	**GLOSARIO DE TERMINOS**

ANEXO 1 ENCUENTA

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE CONTADURIA PÚBLICA

Encuesta dirigida a los profesionales inscritos en el consejo de vigilancia de la profesión de contaduría pública y auditoria que al 31 de diciembre hayan actualizado sus datos.

Los datos que nos proporcionará en esta encuesta, son de carácter confidencial y de mucha utilidad para la realización del trabajo de investigación titulado: "DISEÑO DE PLANEACIÓN DE AUDITORIA DE SISTEMAS CON BASE A LAS NORMAS ISO 27000 EN LAS EMPRESAS INDUSTRIALES AFILIADAS A LA ASI".

Objetivo: Conocer la opinión de los profesionales en contaduría publica respecto de la auditoria de sistemas con enfoque ISO 27000 en las empresas industrias, las causas que influyen en el desarrollo del tema y los elementos que debe contener un modelo de planeación referente al tema en mención.

Indicaciones: Se le solicita por favor marcar con una "X", y complementar en su caso, las preguntas que a continuación se le presentan.

Le agradecemos de antemano su valiosa colaboración.

1. ¿Considera que es necesario la realización de auditoria de Sistemas dentro de las empresas?

   - Si ( )
   - No ( )

   ¿Por que?

   _____

2. ¿Alguna vez ha realizado o ha estado involucrado en el desarrollo de una Auditoría de Sistemas?

   - Si ( )
   - No ( )

3. ¿Conoce acerca de la Norma ISO 27000?

   - Si ( )
   - No ( )

4. Si su respuesta anterior es No, ¿Le gustaría contar con un modelo de planeación que le permitiera conocer e implementar en una auditoría de sistemas?

   - Si ( )
   - No ( )

   ¿Por que? _____

5. ¿Ha recibido Usted alguna capacitación sobre las Normas ISO?

   - Si ( )
   - No ( )

   ¿Por que?_____

6. Tomando en cuenta el ambiente competitivo de los profesionales en Contaduría Pública ¿Incursionaría en el desarrollo de trabajos de auditoria de sistemas bajo un enfoque ISO 27000?

   - Si ( )
   - No ( )

7. ¿Por qué cree usted que es importante desarrollar una Auditoria de Sistemas implementando Normas de Calidad?

   _____ _____

   _____ _____

8. ¿Considera que los profesionales en Contaduría Pública están capacitados para realizar auditorias de Sistemas con enfoque ISO?

   - Si ( )
   - No
   - ( )

9. Actualmente, ¿Considera usted que sería importante contar con un modelo de planeación de Auditoría de Sistemas con enfoque ISO 27000?

   - Si ( )
   - No
   - ( )

10. ¿Cree usted que al implementar este modelo la información será más confiable?

    - Si ( )
    - No ( )

    ¿Por que?_____

11. ¿Considera usted que los modelos actuales utilizados por los profesionales para el desarrollo de la Auditoría de Sistemas son los mas adecuados considerando la implementación de las nuevas normas ISO?

- Si ( )
- No ( )

12. ¿Si existiera un modelo de planeación con dicho enfoque, tomaría la decisión de tomarlo en cuenta para ejecutar sus auditorias?

- Si ( )
- No ( )

13. ¿Considera que únicamente las empresas ya certificadas en ISO pueden ser evaluadas mediante una auditoría de sistemas con enfoque ISO 27000?

- Si ( )
- No ( )

14. ¿Cree usted que la auditoria de sistemas con enfoque ISO 27000 disminuiría la manipulación malintencionada de información en las entidades?

- Si ( )
- No ( )

15. ¿Considera usted que los gremios o las entidades encargadas de difundir esta temática proporcionan las herramientas necesarias para realizarlo?

- Si ( )
- No ( )

16. ¿Por qué considera que la mayoría de profesionales en Contaduría Pública se especializan en auditoria financieras o fiscales y no en auditorias especializadas?

- No hay una base para ejecutarlas ( )
- Poco Interés ( )
- Los costos de capacitación son elevados ( )
- Otros ( )

17. ¿Considera usted que el profesional en contaduría pública tiene la oportunidad de aprovechar este campo de auditoría para desarrollarse ampliamente?

- Si ( )
- No ( )

18. ¿Considera que al profesional en contaduría pública le beneficiaría implementar la auditoría de sistemas con enfoque ISO 27000 para desarrollarse en dicho campo?

- Si ( )
- No ( )

19. ¿Cree usted, que la elaboración de un documento diseñado como un modelo de planeación para la auditoria de sistemas con base a normas ISO 27000, seria útil para agregar valor a los servicios que ofrece?

- Si ( )
- No ( )

20. ¿Considera que los profesionales en Contaduría Pública le están dando cumplimiento a la norma de educación continua (40 horas)?

- Si ( )
- No ( )

ANEXO 2 TABULACIONES

Cuadro 1: ¿Considera que es necesario la realización de auditoria de Sistemas dentro de las empresas?

Objetivo: Indagar si los encuestados consideran necesaria la realización de auditorías de sistemas dentro de las entidades

ALTERNATIVA	FRECUENCIA	
	ABSOLUTA	RELATIVA
SI	33	100.00%
NO	0	0.00%
TOTALES	**33**	**100.00%**

Como podemos observar en el cuadro anterior el 100%de los encuestados consideran que es necesaria la realización de auditorias de sistemas dentro de las empresas, la población encuestada en su totalidad coincidieron afirmativamente a la interrogante planteada.

Lo anterior tiene como complemento la siguiente interrogante ¿Por qué Consideran que es necesaria la realización de auditorias de sistemas dentro de las empresas?; ya sea que los encuestados hallan contestado afirmativamente o no. Los encuestados respondieron esta interrogante planteando las siguientes razones por las cuales consideran que son necesarias las realizaciones de auditorias de sistemas dentro de las instituciones y de los cuales se han agrupado considerando su frecuencia y similitudes dentro de las alternativas planteadas por los profesionales en contaduría publica encuestados:

a) Nos permite efectuar Revisiones y evaluaciones de Procedimientos Informáticos.
b) Permite Actualizar los procedimientos informáticos y Evitar manipulaciones
c) Los resultados permiten dar un boto de confianza

d) Ayuda a la Verificación y Corrección

e) Los riesgos informáticos son mayores y se debe estar actualizado.

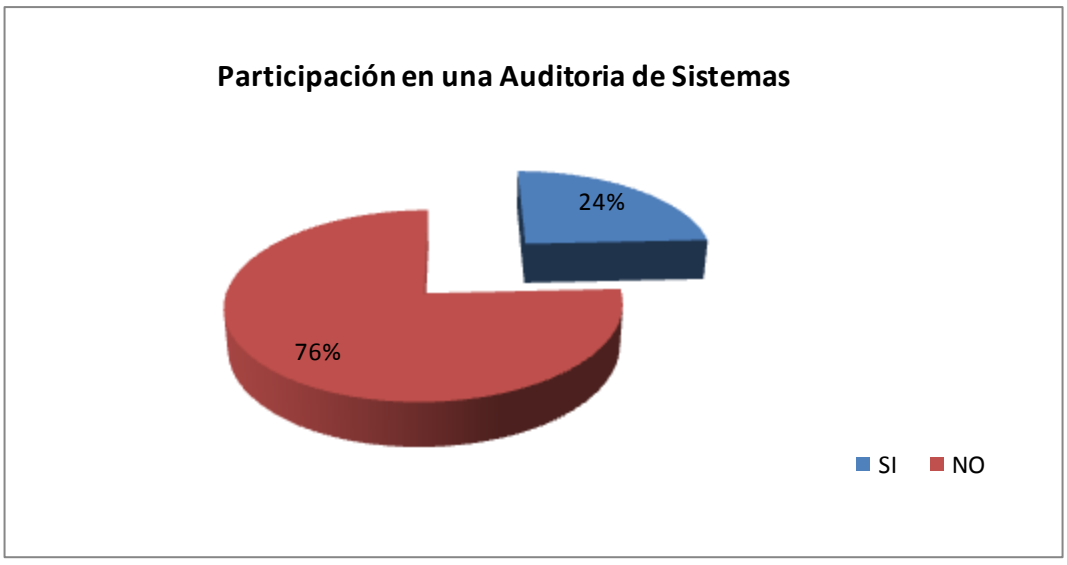
f) Mejorar el control interno de la compañía

Las opiniones arrojadas planteadas en las encuestas permiten concluir en esta interrogante que las auditorias de sistemas son importantes dentro de las empresas que poseen sistemas informáticos en el desarrollo de sus actividades y de la información que estos generan, el control interno es una de las causas por las cuales consideran que las auditorias de sistemas son importantes; así mismo las verificaciones que se realizan con el desarrollo de este tipo de auditoria contribuye a identificar riesgos informáticos y de seguridad dentro de la manipulación de la información que los mismos sistemas generan.

Cuadro 2: ¿Alguna vez ha realizado o ha estado involucrado en el desarrollo de una Auditoría de Sistemas?

Objetivo: Conocer si los encuestados ha realizado o han estado involucrados en el desarrollo de auditorias de sistemas.

ALTERNATIVA	FRECUENCIA	
	ABSOLUTA	RELATIVA
SI	8	24.24%
NO	25	75.76%
TOTALES	**33**	**100.00%**

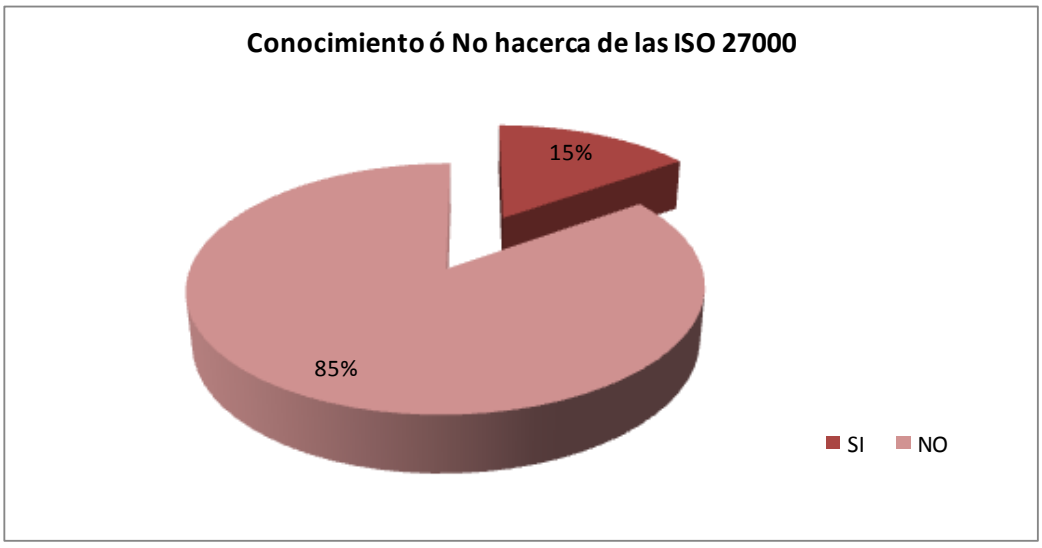


En el cuadro anterior se observa que el 76% de los profesionales en contaduría publica encuestados no han tenido ningún tipo de participación en auditorias de sistemas, caso contrario el 24% de los encuestado manifestaron que en alguna ocasión han participado o se han visto relacionados con el desarrollo de auditorias de sistemas.

Cuadro 3: ¿Conoce acerca de la Norma ISO 27000?

Objetivo: Indagar si los profesionales en contaduría pública encuestados conocen acerca de las nuevas normas ISO 27000.

ALTERNATIVA	FRECUENCIA	
	ABSOLUTA	RELATIVA
SI	5	15.15%
NO	28	84.85%
TOTALES	33	100.00%



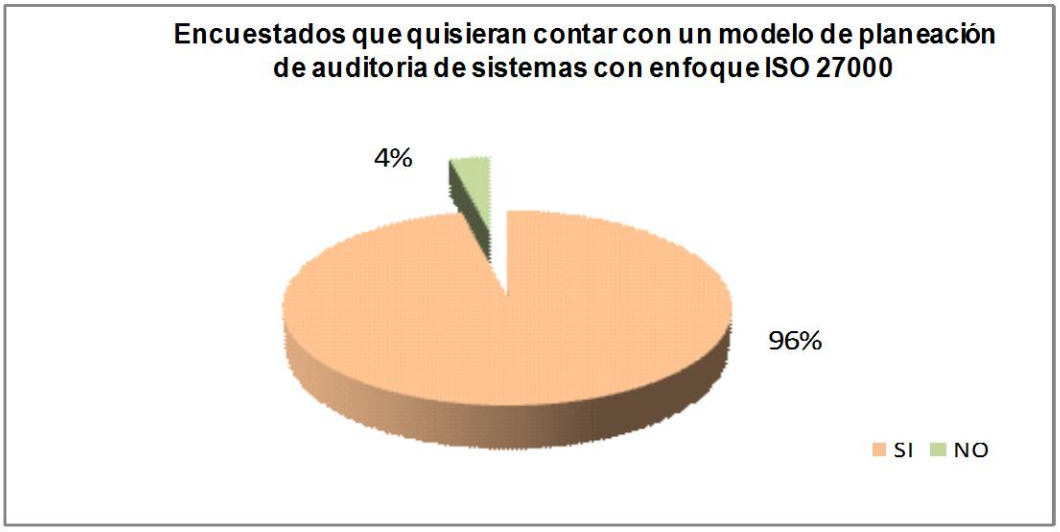
Partiendo de un 100% de los encuestados, en esta oportunidad se observa en el cuadro anterior que el 85% de los profesionales en contaduría publica, no conocen harca de las nuevas normas ISO 27000, caso contrario el 15% de los encuestados manifestaron su conocimiento referente a las ya bitadas normas de calidad.

Lo anterior nos permite replantear una nueva interrogante, la cual se presenta en el cuadro siguiente:

Cuadro 4: Si su respuesta anterior es No, ¿Le gustaría contar con un modelo de planeación que le permitiera conocer e implementar en una auditoría de sistemas?

Objetivo: Conocer si los profesionales en contaduría publica que no conocen las normas ISO 27000 les gustaría contar con un modelo de planeación que les permita conocer e implementar estas normas en una auditoria de sistemas.

ALTERNATIVA	FRECUENCIA	
	ABSOLUTA	RELATIVA
SI	27	96.43%
NO	1	3.57%
TOTALES	28	100.00%



En el cuadro anterior podemos observar que de un 100% de encuestado que respondieron negativamente en el cuadro3, el 96% manifestaron su interés por contar con un modelo de planeación que les permita conocer e implementar este tipo de normas de calidad en una auditoria de sistemas.

Lo anterior tiene como complemento la siguiente interrogante ¿Por qué le gustaría contar con un modelo de planeación de este tipo?:

Los profesionales en contaduría pública manifestaron que:

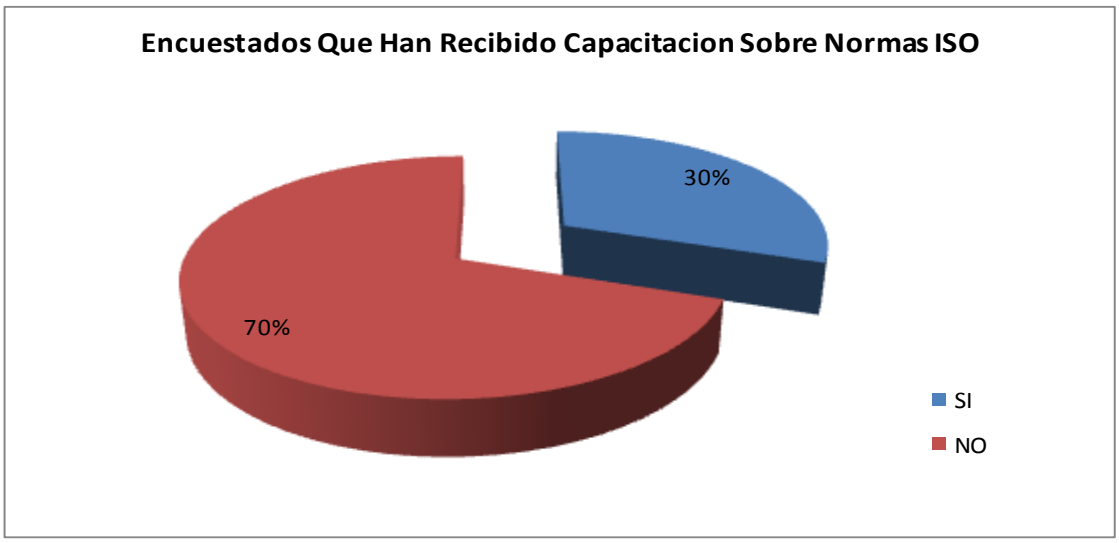
a) Por el uso e implementación de un nuevo estándar conveniente para el desarrollo de una auditoria mas completa.
b) Conocerlo e implementarlo en un futuro
c) Obtener nuevos conocimientos
d) Permite evaluar basado en estándares de calidad
e) Es necesario contar con un modelo
f) Especializarse

Lo anterior se basa en las respuestas manifestadas por los encuestados y que generan seis tipos de opiniones unificadas, partiendo de las diferentes opiniones de los profesionales en contaduría pública que participaron en las encuestas, y que se resumen en las alternativas planteadas en el párrafo anterior.

Cuadro 5: ¿Ha recibido Usted alguna capacitación sobre las Normas ISO?

Objetivo: Indagar si los encuestado han tenido algún tipo de capacitación sobre las normas ISO

ALTERNATIVA	FRECUENCIA	
	ABSOLUTA	RELATIVA
SI	10	30.30%
NO	23	69.70%
TOTALES	**33**	**100.00%**



Como podemos observar en el cuadro anterior se plantean las diferentes frecuencias arrojadas de las encuestas, en donde el 70% de los encuestados manifestaron que no ha recibido ningún tipo de capacitación sobre las normas de calidad ISO; por el contrario el 30% de los encuestados si han recibido este tipo de capacitación.

Lo anterior tiene como complemento la siguiente interrogante ¿Por qué ha recibido o No capacitación sobre las normas ISO?:

Esta interrogante se sub divide en las siguientes interrogantes:

a) ¿Por qué razones ha recibido capacitación sobre las Normas ISO?
b) ¿Por qué razones No ha recibido capacitación sobre las Normas ISO?

Por lo que los encuestados según fue el caso manifestaron lo siguiente:

a) ¿Por qué razones ha recibido capacitación sobre las Normas ISO?

- ✓ Para tener conocimientos sobre patrones de calidad para la ejecución de auditorias
- ✓ Respecto de las normas en general ya que la empresa esta certificada.
- ✓ Empresa en proceso de Certificación

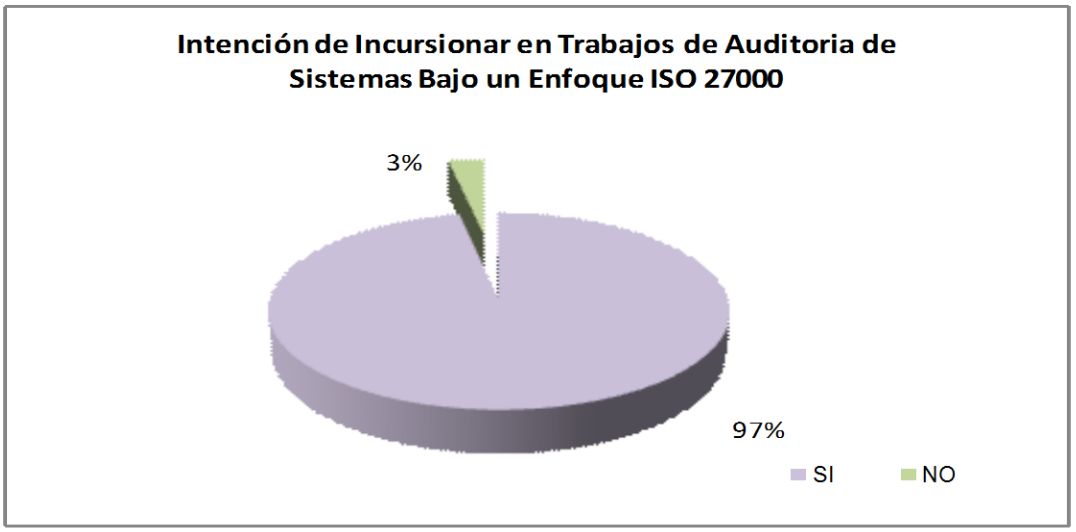
b) ¿Por qué razones No ha recibido capacitación sobre las Normas ISO?

- ✓ Por los Costos
- ✓ No se ha presentado la oportunidad de asistir a una capacitación sobre dichas normas
- ✓ Es una institución autónoma y para implementarlo tendría que ser a nivel gubernamental y no independiente
- ✓ Poca Disponibilidad de los mismos

Cuadro 6: Tomando en cuenta el ambiente competitivo de los profesionales en Contaduría Pública ¿Incursionaría en el desarrollo de trabajos de auditoria de sistemas bajo un enfoque ISO 27000?

Objetivo: Indagar si los encuestados incursionarían en una auditoría de sistemas bajo el enfoque ISO 27000, considerando el ambiente competitivo en el que se desarrollan.

ALTERNATIVA	FRECUENCIA	
	ABSOLUTA	RELATIVA
SI	32	96.97%
NO	1	3.03%
TOTALES	33	100.00%

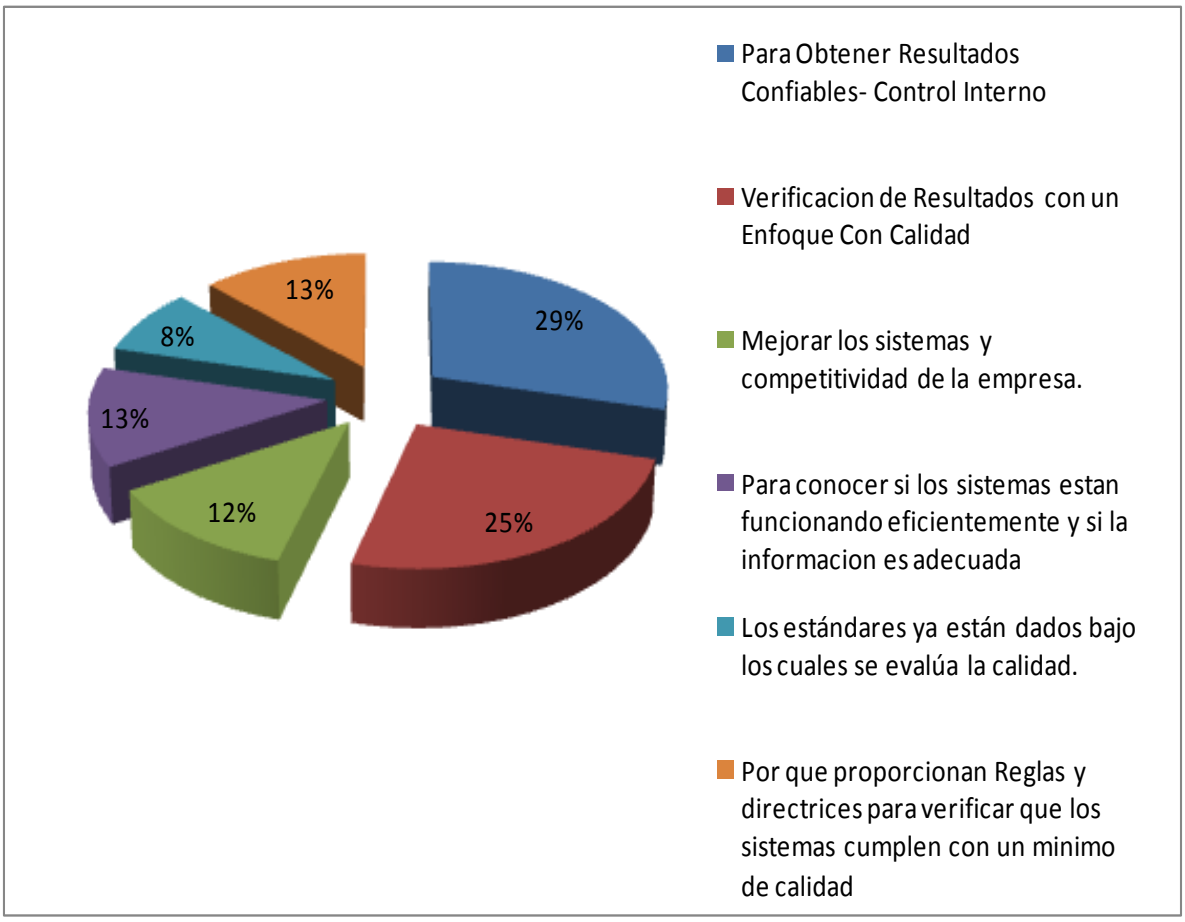


En el cuadro anterior se refleja que la mayor representatividad de los encuetados esta dada por el 97% de la muestra, los cuales sostiene que tomando en cuenta el ambiente competitivo de los profesionales en Contaduría Publica, estarían dispuestos a desarrollar trabajos de auditoría de sistemas bajo un enfoque ISO 27000, y solamente un mínimo del 3% sostuvieron lo contrario.

Cuadro 7: ¿Por qué cree usted que es importante desarrollar una Auditoria de Sistemas implementando Normas de Calidad?

Objetivo: Conocer las razones por las cuales consideran que es importante el desarrollo de auditorías de sistemas implementando normas de calidad, a criterio de los encuestados.

ALTERNATIVA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Para Obtener Resultados Confiables-Control Interno	9	34.62%
Verificacion de Resultados con un Enfoque Con Calidad	6	23.08%
Mejorar los sistemas y competitividad de la empresa.	3	11.54%
Para conocer si los sistemas estan funcionando eficientemente y si la informacion es adecuada	3	11.54%
Los estándares ya están dados bajo los cuales se evalúa la calidad.	2	7.69%
Por que proporcionan Reglas y directrices para verificar que los sistemas cumplen con un minimo de calidad	3	11.54%
TOTALES	**26**	**100.00%**

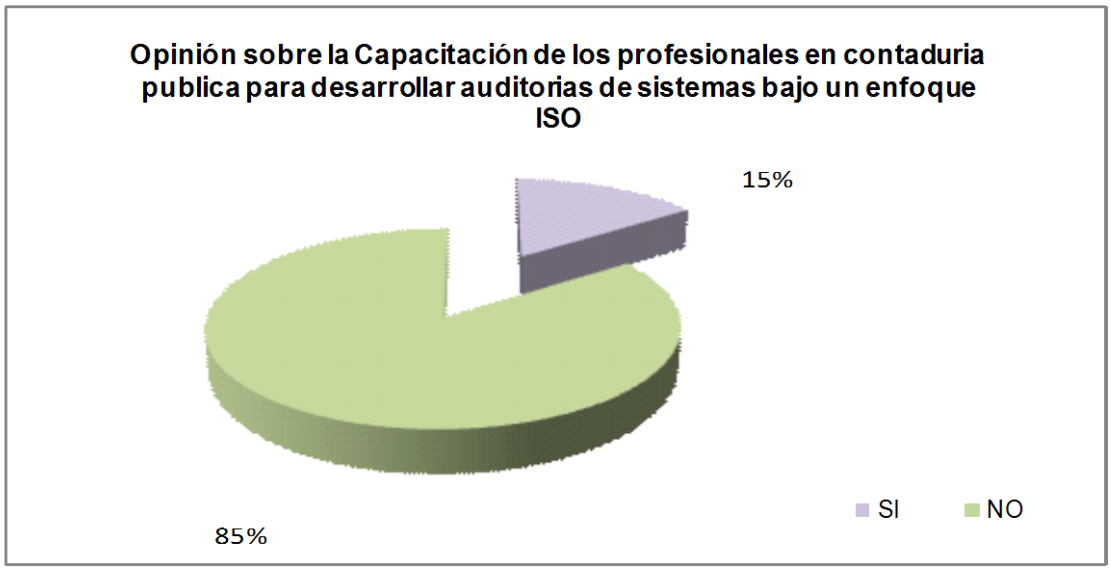


El grafico anterior nos refleja las diferentes razones que expusieron los encuestados, en cuanto a la importancia de desarrollar auditorías de sistemas con normas de calidad; por tanto el 35% coincidió en que es importante para poder obtener resultados confiables sumados al control interno. El 23% manifestó que la verificación de resultados con un enfoque con calidad es una de las razones por las cuales es importante desarrollar auditorias de sistemas con calidad; el 12% manifestó que proporcionan reglas y directrices para verificar que los sistemas cumplen con un mínimo de calidad. Un 11% coincide en que mejorar los sistemas y competitividad de la empresa y otro 11% para conocer si los sistemas están funcionando eficientemente y si la información es adecuada son razones por las cuales es importante desarrollar auditorías de sistemas con calidad.

Cuadro 8: ¿Considera que los profesionales en Contaduría Pública están capacitados para realizar auditorias de Sistemas con enfoque ISO?

Objetivo: Indagar sobre si los profesionales en contaduría pública están capacitados para realizar auditorias de sistemas con enfoque ISO

ALTERNATIVA	FRECUENCIA	
	ABSOLUTA	RELATIVA
SI	5	15.15%
NO	28	84.85%
TOTALES	33	100.00%

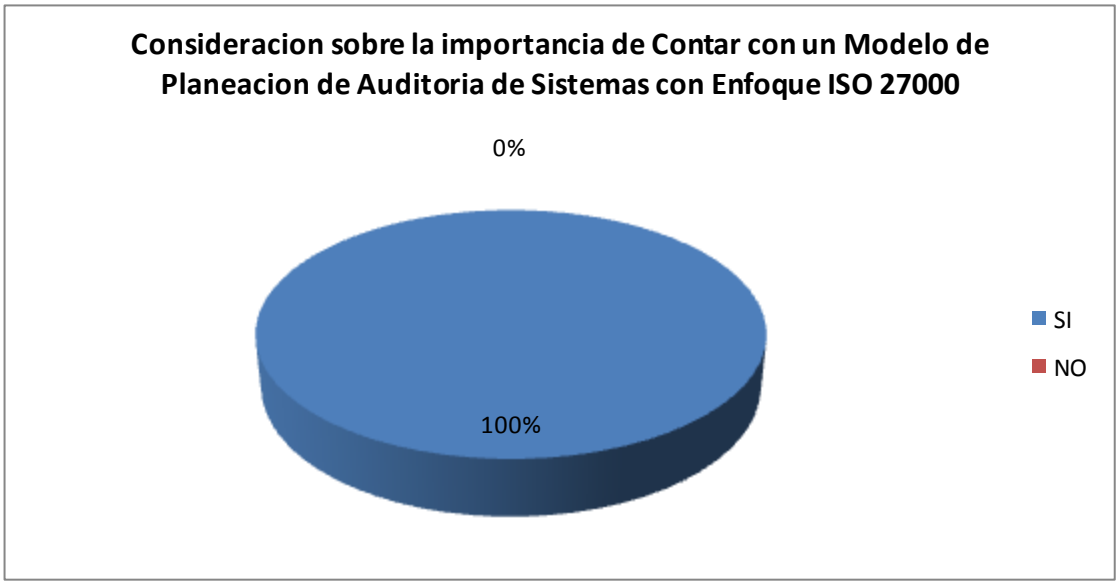


El cuadro anterior nos refleja que el 85% de los encuestados coincidieron en que los profesionales en contaduría pública no están capacitados para realizar auditorias de sistemas con un enfoque ISO; caso contrario el 15% de los encuestados manifestaron que si se encuentran capacitados para desarrollar auditorias de sistemas bajo un enfoque ISO.

Cuadro 9: Actualmente, ¿Considera usted que sería importante contar con un modelo de planeación de Auditoría de Sistemas con enfoque ISO 27000?

Objetivo: Indagar si los encuestados consideran importante contar con un modelo de planeación de auditoria de sistemas con enfoque ISO 27000.

ALTERNATIVA	FRECUENCIA	
	ABSOLUTA	RELATIVA
SI	32	96.97%
NO	1	3.03%
TOTALES	**33**	**100.00%**

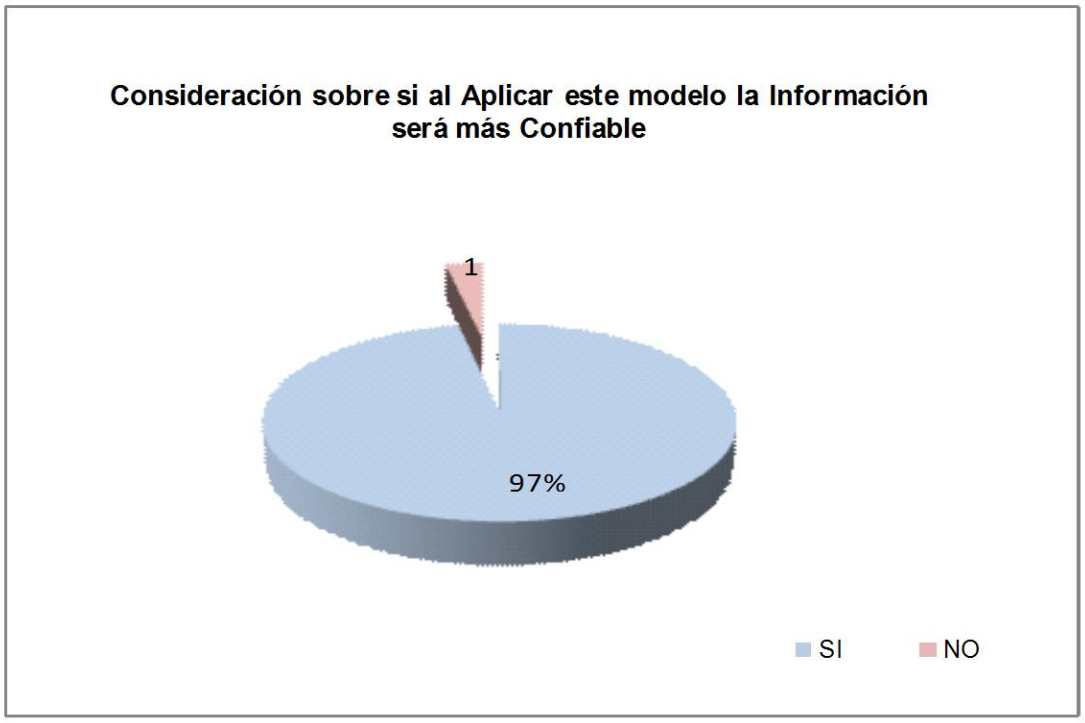


En el grafico anterior se presenta la tendencia de los resultados de los profesionales en contaduría publica que fueron encuestados, de loas cuales el 97% manifestaron que si es importante contar con un modelo de planeación de auditoria de sistemas con enfoque ISO 27000; solamente un 3% de los encuestados manifestó que no es importante.

Cuadro 10: ¿Cree usted que al implementar este modelo la información será más confiable?

Objetivo: Conocer la opinión de los encuestados sobre si al implementar un modelo de planeación de auditoria de sistemas con enfoque ISO 27000 y al poner en practica, la información seria mas confiable.

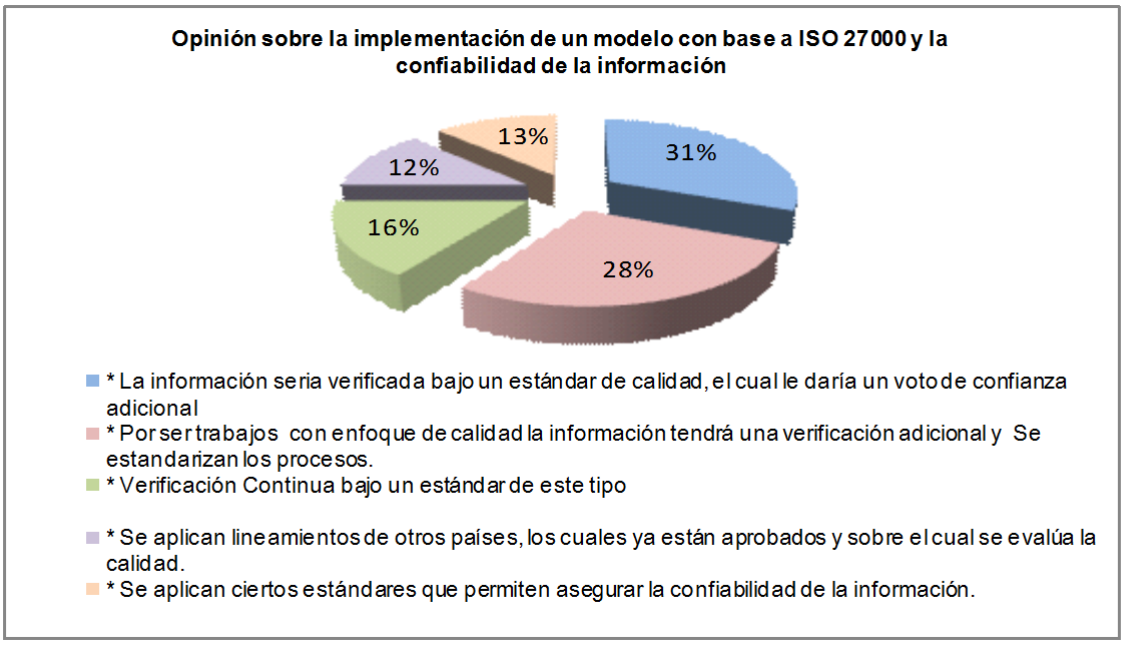
ALTERNATIVA	FRECUENCIA	
	ABSOLUTA	RELATIVA
SI	32	96.97%
NO	1	3.03%
TOTALES	**33**	**100.00%**



En el cuadro anterior se refleja que el 97% de los encuestados coincidieron en que al aplicar un modelo de planeación de auditoria de sistemas con enfoque ISO 27000 la información seria más confiable, y solamente un 3% manifestó lo contrario.

Lo anterior tiene como complemento la siguiente interrogante, ¿Por qué Cree usted que al implementar este modelo la información será mas confiable?

OPINIONES	FREC.
* La información seria verificada bajo un estándar de calidad, el cual le daría un voto de confianza adicional	10
* Por ser trabajos con enfoque de calidad la información tendrá una verificación adicional y Se estandarizan los procesos.	9
* Verificación Continua bajo un estándar de este tipo	5
* Se aplican lineamientos de otros países, los cuales ya están aprobados y sobre el cual se evalúa la calidad.	4
* Se aplican ciertos estándares que permiten asegurar la confiabilidad de la información.	4

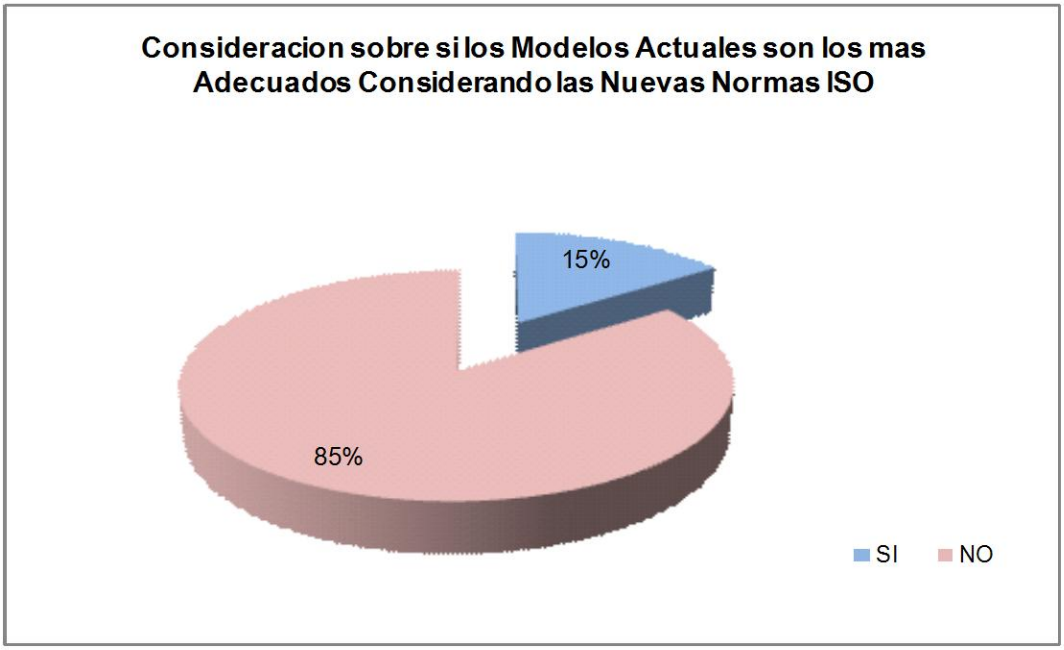


La opinión de los encuestados ante la interrogante anterior se encuentra reflejada en el cuadro anterior, en el cual podemos observar que el 31% de los encuestados opinan que la información seria verificada bajo un estándar de calidad, el cual le daría un voto de confianza adicional, y un 28% que por ser trabajos con enfoque de calidad la información tendría una verificación adicional y se estandarizarían los procesos.

Cuadro 11: ¿Considera usted que los modelos actuales utilizados por los profesionales para el desarrollo de la Auditoría de Sistemas son los más adecuados considerando la implementación de las nuevas normas ISO?

Objetivo: Conocer la opinión de los encuestados en cuanto a los modelos existentes sobre auditoria de sistemas considerando la implementación de las nuevas normas de calidad ISO 27000

ALTERNATIVA	FRECUENCIA	
	ABSOLUTA	RELATIVA
SI	5	15.15%
NO	28	84.85%
TOTALES	33	100.00%

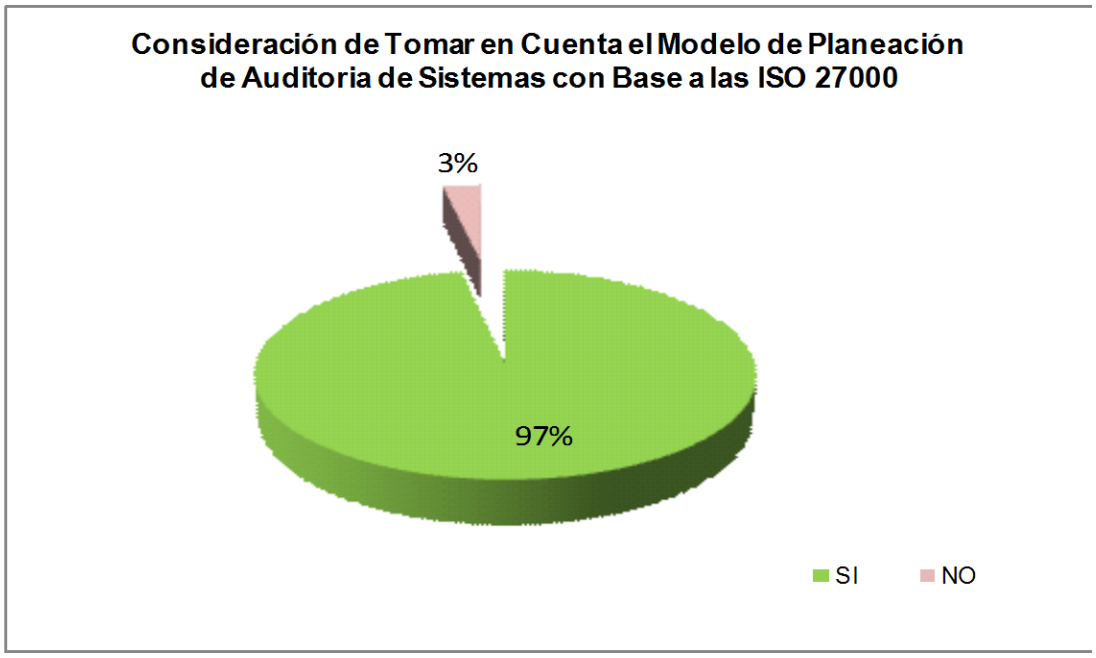


En el cuadro anterior se plantea que el 85% de los encuestados consideran que los modelos actuales no son los más adecuados considerando las nuevas normas de calidad ISO, esto para las auditorias de sistemas, por el contario un 15% de los profesionales en contaduría pública encuestados manifiestan que si son adecuados los modelos actuales.

Cuadro 12: ¿Si existiera un modelo de planeación con dicho enfoque, tomaría la decisión de tomarlo en cuenta para ejecutar sus auditorias?

Objetivo: Conocer la opinión que los encuestados tienen sobre si tomarían la decisión de ejecutar sus auditorias con un modelo de planeación de auditoría de sistemas con enfoque ISO 27000

ALTERNATIVA	FRECUENCIA	
	ABSOLUTA	RELATIVA
SI	32	96.97%
NO	1	3.03%
TOTALES	33	100.00%

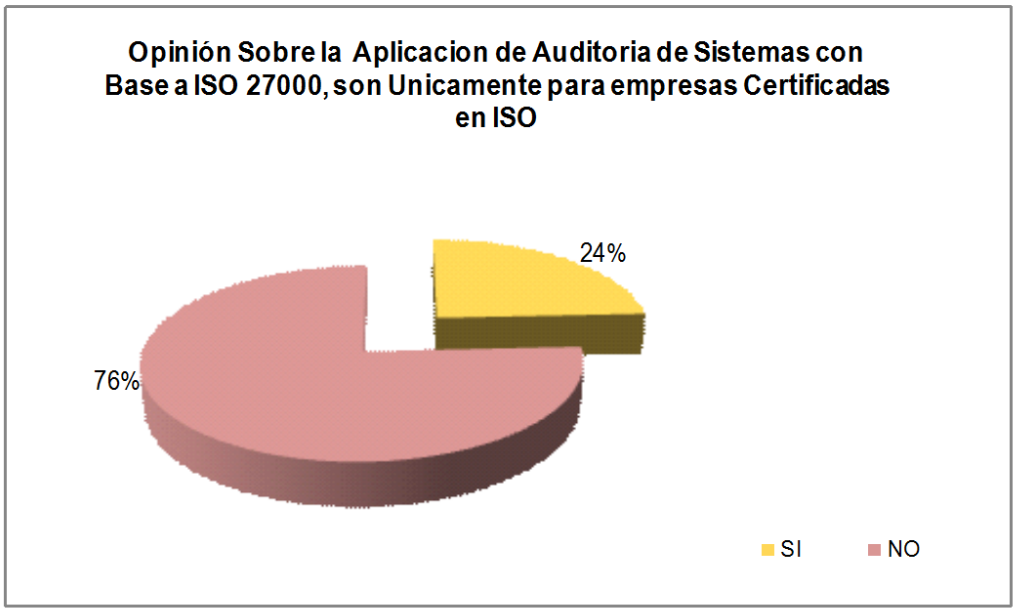


En el grafico anterior se muestran los resultados de la opinión de los encuestados en cuanto a que si ellos tomarían en cuenta un modelo de planeación de auditoria de sistemas con base a normas ISO 27000 en el desarrollo de sus auditorias, por lo cual el 97% manifestó que lo tomaría en cuenta, y un 3% de los profesionales en contaduría publica encuestados manifestó lo contrario.

Cuadro 13: ¿Considera que únicamente las empresas ya certificadas en ISO pueden ser evaluadas mediante una auditoría de sistemas con enfoque ISO 27000?

Objetivo: Indagar si los encuestados consideran que únicamente las empresas que ya están certificadas en ISO pueden ser evaluadas mediante una auditoria de sistemas con enfoque ISO 27000

ALTERNATIVA	FRECUENCIA	
	ABSOLUTA	RELATIVA
SI	8	24.24%
NO	25	75.76%
TOTALES	**33**	**100.00%**



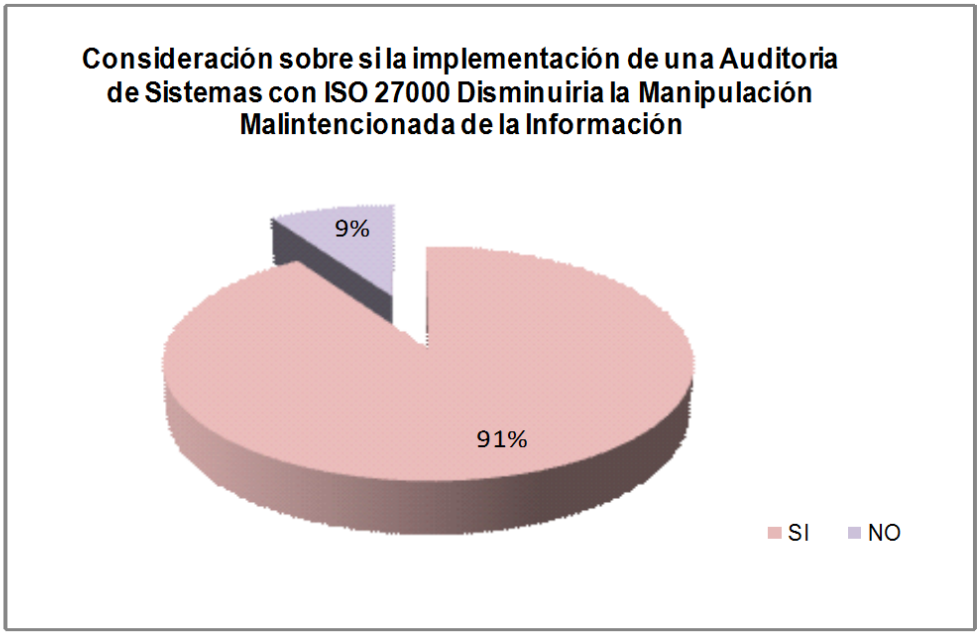
En el cuadro anterior se presentan las frecuencias de las opiniones de los encuestados, en la cual el 76% de ellos opinaron que No solo las empresas que se encuentran certificadas con normas de calidad ISO pueden desarrollarse auditorias de sistemas con base ISO 27000.

El 24% de los encuestados manifestaron que solo las empresas que ya poseen certificación ISO pueden tener auditorias de sistemas con dicho enfoque.

Cuadro 14: ¿Cree usted que la auditoria de sistemas con enfoque ISO 27000 disminuiría la manipulación malintencionada de información en las entidades?

Objetivo: Conocer la opinión que los profesionales en contaduría pública encuestados tienen respecto a si la auditoria de sistemas con enfoque ISO 27000 disminuiría la manipulación malintencionada de información en las empresas.

ALTERNATIVA	FRECUENCIA	
	ABSOLUTA	RELATIVA
SI	30	90.91%
NO	3	9.09%
TOTALES	33	100.00%

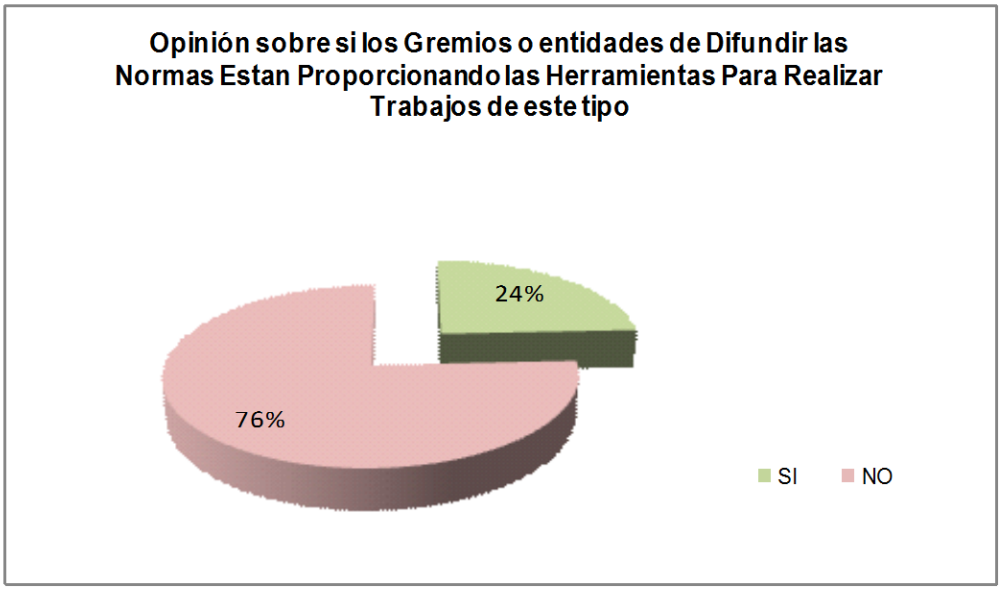


En el cuadro anterior se observa que el 91% de los encuestados manifestaron que una auditoria de sistemas con enfoque ISO 27000 ayudaría a disminuir la manipulación malintencionada de la información dentro de las empresas, caso contrario un 9% de los encuestados consideran que no ayudarían a disminuir la manipulación de la información dentro de las entidades.

Cuadro 15: ¿Considera usted que los gremios o las entidades encargadas de difundir esta temática proporcionan las herramientas necesarias para realizarlo?

Objetivo: Indagar sobre la opinión de los profesionales en contaduría pública encuestados tienen sobre si los gremios o entidades encargadas de difundir las normas de calidad ISO 27000 y su incursión en las auditorias de sistemas están proporcionando las herramientas necesarias para realizar este tipo de trabajos.

ALTERNATIVA	FRECUENCIA	
	ABSOLUTA	RELATIVA
SI	8	24.24%
NO	25	75.76%
TOTALES	**33**	**100.00%**

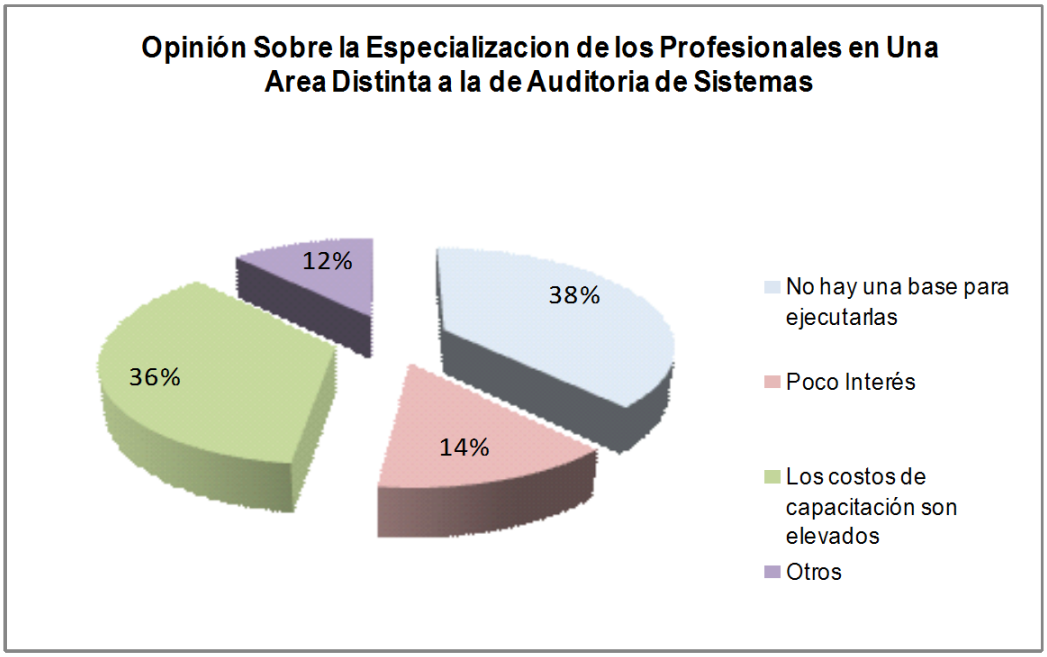


En el grafico anterior podemos observar que el 76% de los encuestados manifestaron que los gremios o entidades encargadas de difundir esta temática no lo están llevando acabo y tan solo un 24% consideran que si lo están haciendo.

Cuadro 16: ¿Por qué considera que la mayoría de profesionales en Contaduría Pública se especializan en auditoria financieras o fiscales y no en auditorias especializadas?

Objetivo: Indagar sobre la opinión de los encuestados en cuanto a que por que los profesionales en contaduría publica se especializan en auditorias financieras o fiscales y no en auditorias especializadas.

ALTERNATIVA	FRECUENCIA	
	ABSOLUTA	RELATIVA
No hay una base para ejecutarlas	19	38.00%
Poco Interés	7	14.00%
Los costos de capacitación son elevados	18	36.00%
Otros	6	12.00%
TOTALES	50	**100.00%**

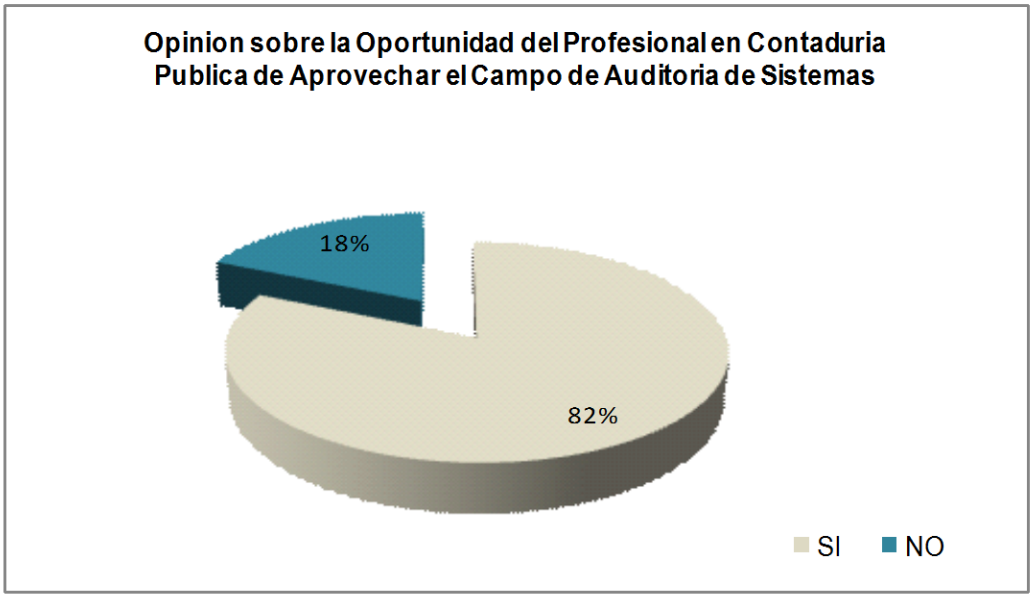


En el grafico anterior podemos observar que el 38% de los encuestados opinan que no hay una base para ejecutar auditorias especializadas y un 36% que los costos de capacitación son muy elevados para poder ejecutar auditorias especializadas.

Cuadro 17: ¿Considera usted que el profesional en contaduría pública tiene la oportunidad de aprovechar este campo de auditoría de sistemas para desarrollarse ampliamente?

Objetivo: Conocer la opinión de los encuestados en cuanto a que si se puede aprovechar el campo de auditorias de sistemas para que el profesional en contaduría publica se pueda desarrollar ampliamente.

ALTERNATIVA	FRECUENCIA	
	ABSOLUTA	RELATIVA
SI	27	81.82%
NO	6	18.18%
TOTALES	33	100.00%

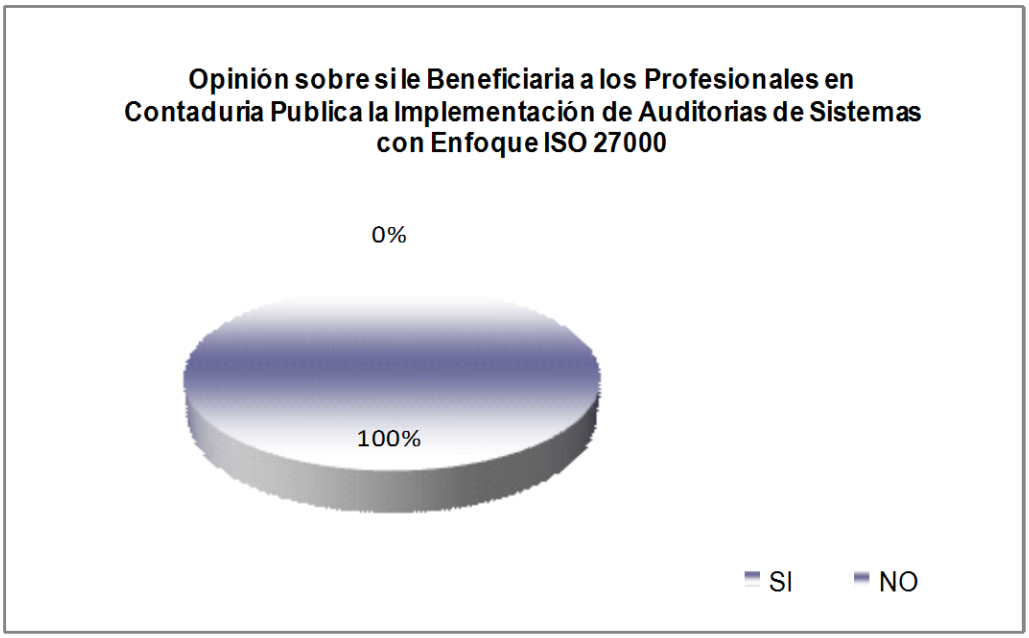


En el cuadro anterior podemos observar que el 82% de los encuestados opinaron que es posible que los profesionales en contaduría pública puedan aprovechar ampliamente el campo de auditoría de sistemas para desarrollarse ampliamente; un 18% de los encuestados opinaron lo contrario.

Cuadro 18: ¿Considera que al profesional en contaduría pública le beneficiaría implementar la auditoría de sistemas con enfoque ISO 27000 para desarrollarse en dicho campo?

Objetivo: Indagar la opinión de los encuestado en cuanto a que si consideran que a los profesionales en contaduría pública les beneficiaria implementar auditorias de sistemas con enfoque ISO para desarrollarse en este tipo de campos de aplicación para la profesión.

ALTERNATIVA	FRECUENCIA	
	ABSOLUTA	RELATIVA
SI	33	100.00%
NO	0	0.00%
TOTALES	**33**	**100.00%**

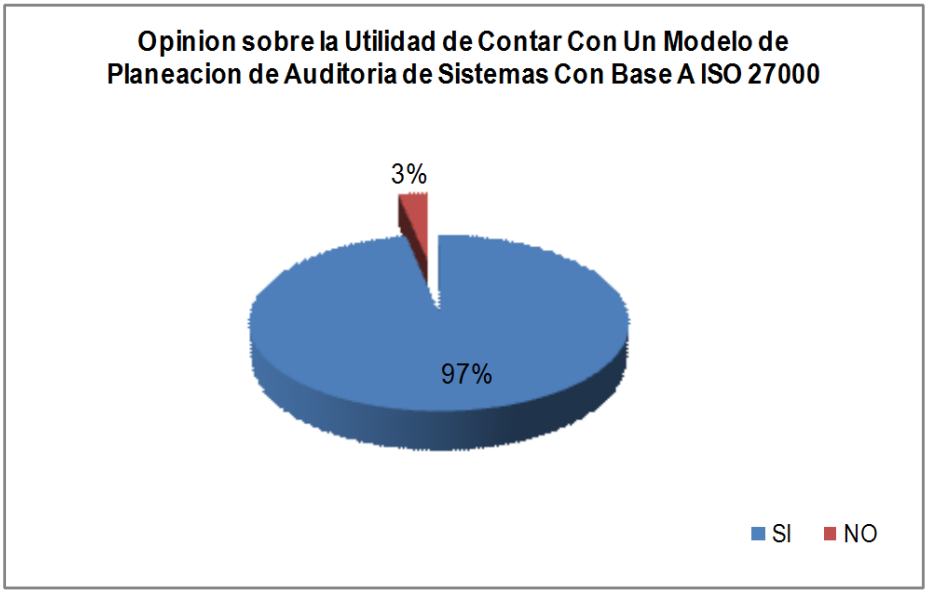


En el cuadro anterior se observa que el 100% de los encuestados opinaron que seria un beneficio para los profesionales en contaduría pública implementar un modelo de planeación de auditoria de sistemas con enfoque ISO 27000 en el desarrollo de sus funciones ya que les permitiría incursionar en este campo de aplicación.

Cuadro 19: ¿Cree usted, que la elaboración de un documento diseñado como un modelo de planeación para la auditoria de sistemas con base a normas ISO 27000, seria útil para agregar valor a los servicios que ofrece?

Objetivo: Conocer la opinión de los encuestados en cuanto que si seria útil para agregar valor a los servicios que ofrece, el contar con un documento diseñado como un modelo de planeación para auditoria de sistemas con base a normas ISO 27000.

ALTERNATIVA	FRECUENCIA	
	ABSOLUTA	RELATIVA
SI	32	96.97%
NO	1	3.03%
TOTALES	**33**	**100.00%**

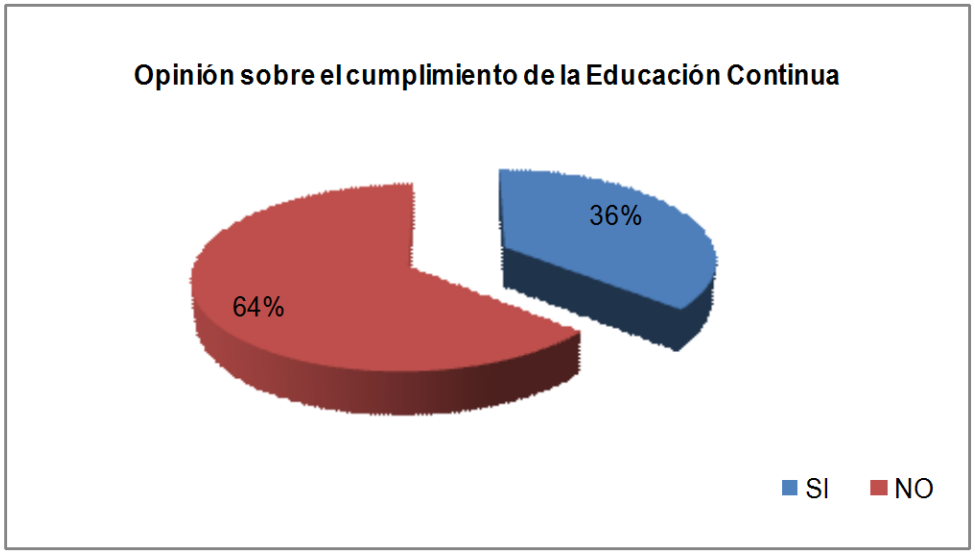


En el cuadro anterior se observa que el 97% de los profesionales en contaduría pública encuestados manifestaron que seria útil contar con un modelo de planeación de auditoria de sistemas con base a las normas ISO 27000 en el desarrollo de sus actividades, ya que les permitiría agregar valor a los servicios que ofrecen.

Cuadro 20: ¿Considera que los profesionales en Contaduría Pública le están dando cumplimiento a la norma de educación continúa (40 horas)?

Objetivo: Indagar la opinión de los encuestados respecto a que si los profesionales en contaduría pública están cumpliendo con la norma de educación continua.

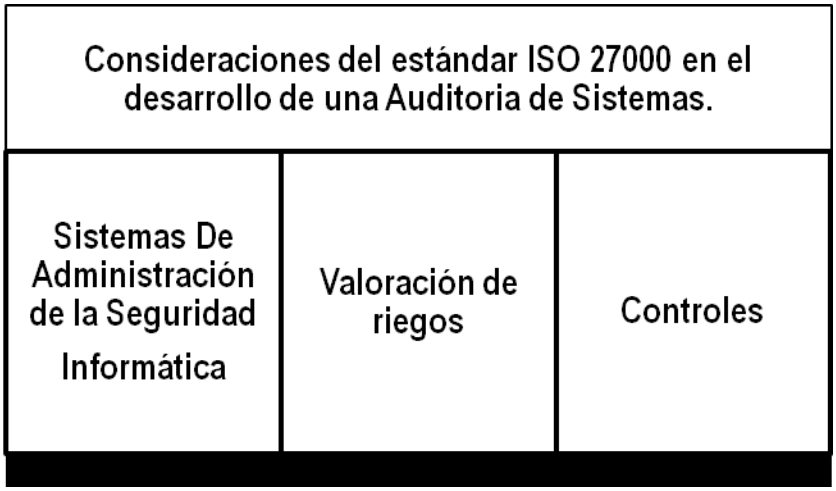
ALTERNATIVA	FRECUENCIA	
	ABSOLUTA	RELATIVA
SI	12	36.36%
NO	21	63.64%
TOTALES	**33**	**100.00%**



En el grafico anterior se presentan los resultados obtenidos de las encuestas, en las cual el 64% de los encuestados manifestaron que los profesionales en contaduría publica no están dándole cumplimiento a las norma de educaron continua.

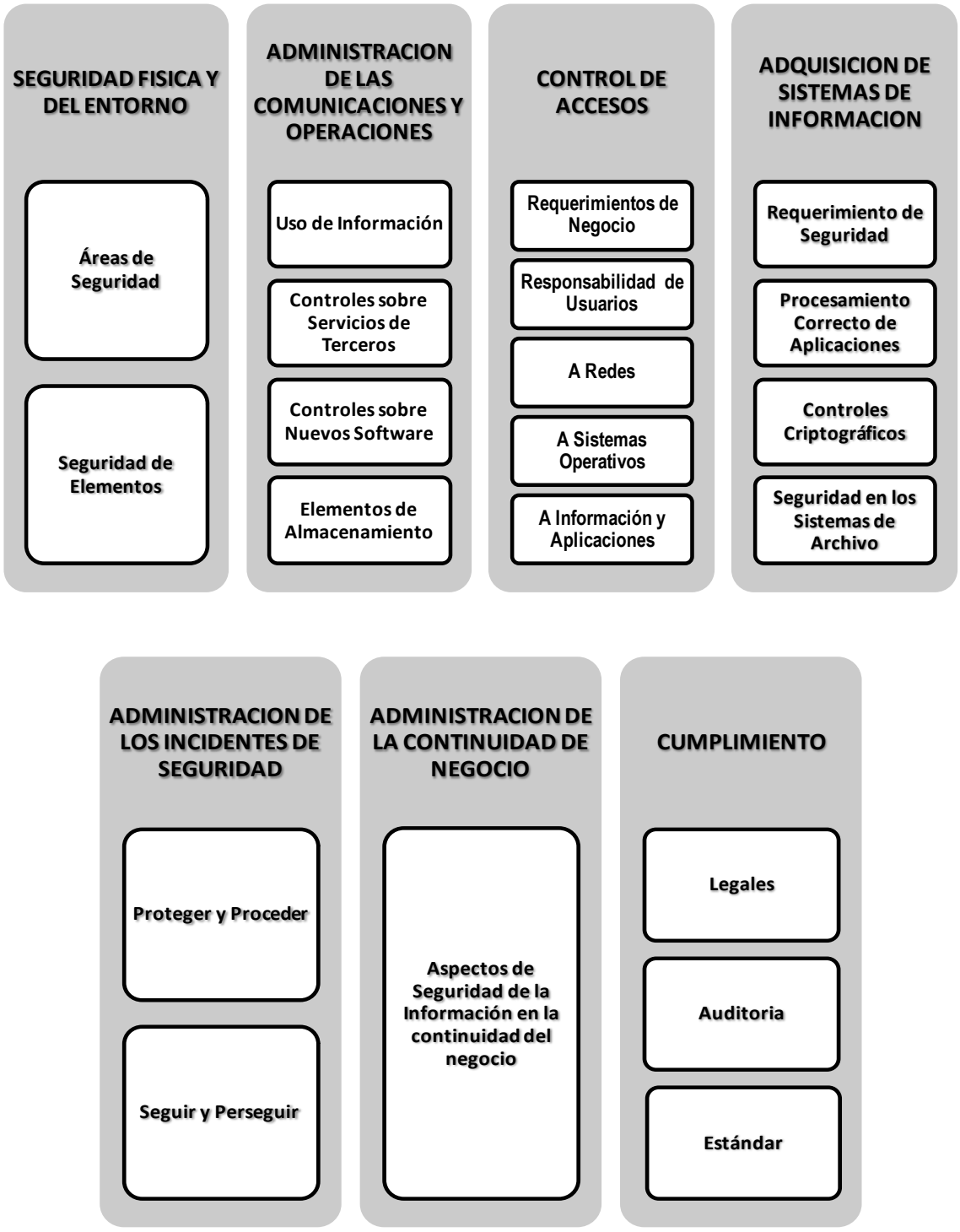
Por el contario un 36% de los encuestados consideran que si se le esta dando cumplimiento a dicha norma.

ANEXO 3 RESUMEN ISO 27000



CONTROLES

CONTROLES


SEGURIDAD FISICA Y DEL ENTORNO
Áreas de Seguridad
Seguridad de Elementos
ADMINISTRACION DE LAS COMUNICACIONES Y OPERACIONES
Uso de Información
Controles sobre Servicios de Terceros
Controles sobre Nuevos Software
Elementos de Almacenamiento
CONTROL DE ACCESOS
Requerimientos de Negocio
Responsabilidad de Usuarios
A Redes
A Sistemas Operativos
A Información y Aplicaciones
ADQUISICION DE SISTEMAS DE INFORMACION
Requerimiento de Seguridad
Procesamiento Correcto de Aplicaciones
Controles Criptográficos
Seguridad en los Sistemas de Archivo
ADMINISTRACION DE LOS INCIDENTES DE SEGURIDAD
Proteger y Proceder
Seguir y Perseguir
ADMINISTRACION DE LA CONTINUIDAD DE NEGOCIO
Aspectos de Seguridad de la Información en la continuidad del negocio
CUMPLIMIENTO
Legales
Auditoria
Estándar

ANEXO 4 GLOSARIO

- Sistemas: Es un conjunto de elementos, entidades o componentes que se caracterizan por ciertos atributos identificables que tienen relación entre sí, y que funcionan para lograr un objetivo común.[9]

- Sistemas de Información: Es un conjunto de elementos que utiliza una entidad con el fin de procesar su información y por lo general esta identificado por componentes que interrelacionados entre si cumplen un objetivo en especifico pero de forma independiente son capaces de generar información.

- Sistemas Contables: Es una estructura organizada mediante la cual se recogen las informaciones de una empresa como resultado de sus operaciones valiéndose de recursos como formularios, reportes, libros, etc., y que presentados a la gerencia le permitirán a la misma tomar decisiones financieras.

- Análisis de Sistemas: Toda aquella actividad que se realiza para descomponer y explicar un sistema de información en cada uno de sus elementos.[10]

CONCEPTOS RELACIONADOS CON AUDITORÍA DE SISTEMAS

- Auditoría de Sistemas: Es el examen y la verificación de los controles y procedimientos utilizados en las áreas de informática, con el propósito de lograr efectivamente los objetivos de continuidad del servicio a los usuarios confidencialidad, seguridad, integridad y coherencia de la información, evitando que los riesgos se materialicen o bien se disminuyan adecuadamente.[11]

- El hardware: se refiere a todos los componentes físicos (que se pueden tocar), en el caso de una computadora personal serían los discos, unidades de disco, monitor, teclado, la placa base, el microprocesador, etc. [12]

---

[9] Fernando Catacora Carpio, Sistemas y Procedimientos Contables, Pág. 25
[10] ídem
[11] Erick L. Kohler "Diccionario para Contadores" Editorial Hispanoamericana, S.A de C.V
[12] http://es.wikipedia.org/wiki/Hardware

- El software: es intangible, existe como información, ideas, conceptos, símbolos, pero no ocupa un espacio físico, se podría decir que no tiene sustancia.

- PED: se refiere al proceso electrónico de datos, que forman parte de la organización de una empresa y que solamente proporcionan servicio a otras divisiones, áreas o departamentos de la misma empresa.[13]

- La seguridad: consiste en asegurar que los recursos del sistema de información (material informático o programas) de una entidad sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

- La seguridad, consiste en asegurar que los recursos del sistema de información (material informático o programas) de una entidad sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

CONCEPTOS RELACIONADOS CON ISO 27000

- International Organization for Standardization (ISO): es una federación internacional con sede en Ginebra (Suiza) de los institutos de normalización de 157 naciones.

- Entidad de certificación: Organismos de evaluación de la conformidad de la aplicación de las normas y estándares de calidad.

- ISO/IEC 27000: es un conjunto de estándares desarrollados o en fase de desarrollo por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission).

- SGSI: es un Sistema de Gestión de la Seguridad de la Información. Esta debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

---

[13] http://www.geocities.com/gehg48/Aef27.html