UNIVERSIDAD DE EL SALVADOR

Facultad de Ciencias Económicas

Escuela de Contaduría Pública

"MODELO DE PLANEACIÓN DE UNA AUDITORÍA ESTRATÉGICA A LOS SISTEMAS DE INFORMACIÓN COMO UNA RESPUESTA A LA CONFIABILIDAD DE LOS ESTADOS FINANCIEROS PREPARADOS EN UN AMBIENTE INFORMÁTICO"

TRABAJO DE INVESTIGACIÓN PRESENTADO POR:

MANOLO ÁLVARO MÉNDEZ RODRÍGUEZ

PARA OPTAR AL GRADO DE

LICENCIADO EN CONTADURÍA PÚBLICA

ENERO DE 2009

SAN SALVADOR, EL SALVADOR, CENTRO AMÉRICA

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES UNIVERSITARIAS

Rector	:	Master: Rufino Antonio Quezada Sánchez
Secretario	:	Licenciado: Douglas Vladimir Alfaro Chávez
Decano de la Facultad de Ciencias Económicas	:	Licenciado: Roger Armando Arias Alvarado
Secretario de la Facultad de Ciencias Económicas	:	Ingeniero: José Ciriaco Gutiérrez Contreras
Director de Escuela de Contaduría Pública	:	Licenciado.: Juan Vicente Alvarado Rodríguez
Asesor Director		Licenciada: María Margarita de Jesús Martínez Mendoza
Jurado Examinador	:	Licenciada: María Margarita de Jesús Martínez Mendoza
	:	Licenciado: Mario Hernán Cornejo Pérez

ENERO DE 2009

SAN SALVADOR, EL SALVADOR CENTROAMÉRICA

AGRADECIMIENTOS

A DIOS TODOPODEROSO: Por su misericordia y su gran amor, que con su poder me iluminó en todo momento y me fortaleció para culminar mi carrera con éxito.

A MIS PADRES: Mariana de Jesús Rodríguez y Jacinto Méndez, por el sacrificio, amor, apoyo y esfuerzo incondicional que me brindaron para alcanzar la meta planteada.

A MIS HERMANOS Y HERMANAS: Por sus palabras de aliento y apoyo moral que me brindaron durante todo el recorrido de la carrera.

A TODOS LOS CATEDRÁTICOS: Que con su apoyo y enseñanza siempre estuvieron dispuestos a transmitir sus conocimientos.

A TODOS MIS AMIGAS Y AMIGOS: Que con su apoyo moral, contribuyeron a fortalecer y dar ánimo para culminar el trabajo de graduación

Manolo Álvaro Méndez Rodríguez.

INDICE

CAPÍTULO II:

CAPÍTULO III:

CAPÍTULO IV:

RESUMEN EJECUTIVO

Mediante el uso de los sistemas de información, en El Salvador; se ha visto como el recurso humano se ha venido desplazando día a día; asimismo la estrategia y la estructura de las organizaciones ha cambiado conforme las circunstancias lo ameritan.

Para adecuar el funcionamiento interno a las exigencias del entorno, las organizaciones definen su política organizacional de la manera más conveniente, a fin de aprovechar las oportunidades que les brinda el entorno de acuerdo a sus capacidades y recursos, con el propósito de mantener su competitividad (estrategia empresarial)

Para el buen funcionamiento de las empresas, se considera importante mantener una base de control interno y además personal idóneo y competente para vigilar cada uno de esos procesos

Los profesionales de la Contaduría Pública, en El Salvador se ven en la necesidad de mantenerse a la vanguardia de las nuevas tendencias de auditoría basadas principalmente en las tecnologías de la información, para sobrevivir a la competencia

Justamente esto fue lo que motivó a realizar un enfoque de estudio en un área específica y delicada como lo es un modelo de auditoría estratégica a los sistemas de información.
El método utilizado para el desarrollo del trabajo fue el hipotético deductivo, ya que este permitió relacionar la investigación bibliográfica y la de campo. Dicha investigación se realizó con una muestra de sesenta profesionales de la contaduría pública inscritos en el Consejo de Vigilancia de la Profesión de la Contaduría Pública y Auditoría, al treinta y uno de Diciembre de dos mil siete

De acuerdo al análisis de los datos obtenidos y mediante el diagnóstico, se pudo comprobar que la mayoría de Profesionales de la Contaduría Pública que se dedican al área de la auditoría, ejercen su profesión en ramas específicas como la auditoría de Estados Financieros, y Auditoría Fiscal. Sin embargo se comprobó que se ha prestado poca atención a las auditorías de Sistemas Informáticos, específicamente a la Auditoría Estratégica a los Sistemas de Información

Es mediante ésta circunstancia y como aporte social, que se propone un modelo de Planeación de una Auditoría Estratégica a Los Sistemas de Información que contribuya a brindar mayor confiabilidad a los estados financieros que se preparan en ambientes informáticos, de tal manera que minimice los errores, omisiones y fraudes a los que se hace inherente la información que se procesa.

Los profesionales de la contaduría pública que se dedican al campo de la auditoría deben actualizar sus conocimientos en las áreas tecnológicas de manera constante, con relación a los cambios eminentes que éstas experimentan; para enfrentar los retos que demanda el medio

INTRODUCCIÓN

En la actualidad, las Tecnologías de la Información y Comunicación (TIC), se han tornado una necesidad imprescindible para cada uno de los usuarios; los cambios constantes en los sistemas de información transforman el proceso de las entidades, tanto públicas como privadas.

Esto implica inversión para aquellos que consideran las herramientas que proporcionan las TIC, como una parte importante para el desarrollo de la empresa, en tal sentido ven hacia el futuro como una oportunidad para mantenerse en la competencia como un negocio en marcha.

Para un buen funcionamiento de los recursos tecnológicos que se adquieren, es necesario que existan políticas estratégicas de uso y de mantenimiento preventivo que contribuya a minimizar la pérdida de la información que en ellos se procesa.

Las empresas requieren de un personal idóneo para enfrentar dichas circunstancias, los cuales deben de contribuir a lograr los objetivos que se pretenden alcanzar, con base a los requerimientos de un Gobierno Corporativo o mediante la alta administración.

Los profesionales de la contaduría pública deben estar preparados para enfrentar cada día los retos que se le avecinan, tomando en cuenta que para una buena competitividad, se necesita un adiestramiento constante; que contribuya a mejorar sus conocimientos, de tal manera que se mantengan a la vanguardia de los requerimientos del entorno.

Bajo estas circunstancias, se ha elaborado el presente trabajo con la finalidad de ayudar a los profesionales de la Contaduría Publica para que posean un Modelo de Planeación de una Auditoría estratégica a los Sistemas de Información que contribuya como una herramientas más, para garantizar la confiabilidad de la información en las entidades que utilizan Sistemas de información, dicho trabajo ha sido dividido en cuatro capítulos los cuales se detallan a continuación:

Capítulo I: contiene el Marco Teórico que sustenta la investigación a partir de los antecedentes de las Auditorías y de las Tecnologías de la Información y comunicación tanto a nivel mundial como nacional; la conceptualización, las características, su importancia, Clasificación de la Auditoría Estratégica, Fases de

la Auditoría Estratégica, la auditoría estratégica aplicada a los Sistemas de Información, los aspectos legales generales y específicos, mercantiles y fiscales relacionados y la normativa técnica aplicable.

Capítulo II: en él se desarrolla la metodología y diagnóstico de la investigación de campo y bibliográfica; describiendo el tipo de estudio, las unidades de análisis, la población y la muestra; también se muestran los resultados obtenidos en el procesamiento de la información al evaluar cada uno de los datos proporcionados por Profesionales de la Contaduría Pública cuyo orden de presentación atienden a cada una de las áreas que intervienen en la investigación las cuales son Seguridad que los Sistemas de Información proporcionan a las compañías, para la información de sus Estados Financieros, Conocimiento que el Contador Público posee en la Auditoría estratégica a los Sistemas de Información, la cual está directamente relacionada con la Auditoría Financiera, Capacitación que el Contador Público ha recibido frente a las demandas del medio con relación a las Tecnologías de la Información y Comunicación (TIC), Medidas que el auditor implementa al auditar considerando los riesgos de auditoría y aplicación técnica de nuevos conocimientos en el ejercicio profesional de la Contaduría Pública y Auditoria

Capítulo III: se propone un modelo de Planeación de una Auditoría Estratégica a los Sistemas de Información, en el cual se explica el desarrollo de un memorando de planeación comenzando desde el conocimiento de la entidad, investigación preliminar, concluyendo con la propuesta de programas.

Capítulo IV: se plantean las conclusiones a las que se llegaron una vez se realizó la investigación, se dan recomendaciones que diferentes entidades involucradas a la profesión de la Contaduría Pública podrán tomar en cuenta y aplicarlas para un mejor desempeño de la profesión en El Salvador

CAPITULO I

1 MARCO TEORICO

1.1 GENERALIDADES DE LA AUDITORÍA ESTRATÉGICA

Partiendo de las necesidades con que cuenta cada entidad, se consideran como principales, aquellos que constituyen posibles amenazas a la entidad de tal manera que se crean herramientas estratégicas a implementar, para el logro de sus objetivos planteados

La actividad cotidiana sumerge a muchos directivos en una continua sucesión de acontecimientos que hay que atender y resolver. Lamentablemente, en muchas organizaciones la agenda se antepone a la estrategia y en esos casos, la actuación en el corto plazo es prioritaria sobre la preparación del medio y largo plazo; se trata de las "empresas cortoplacistas" en las que sus directivos viven tan instalados en el "hoy" que no son capaces de preveer cómo tendrán que acometer el "mañana". Ciertamente, piensan que mañana, pase lo que pase a su alrededor, harán lo mismo que hoy y lo mismo que ayer.

En el lado opuesto, se sitúan las "empresas con visión estratégica" cuyos directivos asumen su papel de estrategas y están permanentemente atentos a los movimientos del mercado, interpretándolos adecuadamente y previendo su posible impacto sobre la empresa, anticipando escenarios y proponiendo los cambios necesarios en la organización para seguir creciendo.

Para adecuar su funcionamiento interno a las exigencias del entorno, las organizaciones definen su política organizacional de la manera más conveniente, para aprovechar las oportunidades que les brinda el entorno y de acuerdo con sus capacidades y recursos, mantener su competitividad para lo cual se estructuran y coordinan sus elementos de una determinada forma (estructura organizativa). [1].

Por lo mismo no es funcional la simplicidad de una planeación como elemento que las organizaciones se mantengan bien estructuradas, si no mas bien la planeación debe ser de manera tal que se visualice hacia el futuro, comenzando con el pasado, verificando el presente

---

[1] Oliek González Solán, Jorge de la Vega Yabor. Los Sistemas de Control de Gestión Estratégica para las organizaciones P 13 (trabajo de investigación). Barcelona España

Entendiendo que existe una estrecha relación entre estrategia y estructura, que viene dada por una interdependencia, puesto que si para poner en práctica una buena estrategia con éxito se supone que la estructura deberá adaptarse a ella, entonces toda estructura existente influirá, en gran medida, en la estrategia que se diseñará.

El enfoque meramente de estudio, no es la totalidad de la entidad, si no más bien un punto especifico; como son los Sistemas de Información conocidos en el medio como (SIF).

La auditoría estratégica a los sistemas de información, solo es el punto de partida, para una buena funcionabilidad de la entidad.

El sistema de control debe diseñarse de tal manera que la base del tipo de estrategia al que se orienta la organización sea el adecuado o más bien sea a la medida de la organización.

Por otra parte la planificación financiera debe estar integrada con la estrategia a largo plazo, por lo que los presupuestos anuales serán un reflejo de ella y permitirán orientar tanto la actuación de los centros de responsabilidad como la evaluación del desempeño de los diferentes responsables o directores de la entidad.

En este sentido se debe de tomar en cuenta la definición y claridad de la estructura organizativa para poder diseñar el sistema de control:

En primer lugar, a medida que la incertidumbre y la complejidad de la actividad aumentan, mayor dificultad existe en la formalización mediante procedimientos. 2.

En segundo lugar, cuando mayor sea la descentralización, más costoso y difícil será ejercer el control y más necesario será tener un sistema de control formalizado, adecuado además para poder controlar las variables concretas en las que puede incidir la gestión descentralizada en los responsables.

---

[2] Oliek González Solán, Jorge de la Vega Yabor. Los Sistemas de Control de Gestión Estratégica para las organizaciones P16. (trabajo de investigación). Barcelona España

En tercer lugar, el tipo de estructura organizativa influirá igualmente en el sistema de control según la organización adopte una estructura funcional, divisional o matricial.

Por último, es muy importante definir claramente el poder de decisión que se transfiere a cada responsable en cada centro y además que el sistema de control esté integrado con la estructura organizativa de forma que los indicadores se definan en función de ella y los presupuestos y la evaluación del desempeño de cada centro se realicen en función de sus responsabilidades. 3.

De forma ideal, la implantación de una tecnología específica debe ser parte de una maniobra integral de tecnología informática. Algunas veces denominado plan de sistemas de información estratégica.

Una estrategia de tecnología informática comprende todos los aspectos que requiere la tecnología informática de una entidad. Delinear estas necesidades en términos generales sirve para identificar oportunidades para la obtención de tecnología nueva o mejorada e indica donde se puede lograr economías mediante el uso compartido de recursos o de componentes específicos de la tecnología para varios usos.

1.2 ANTECEDENTES DE LA AUDITORÍA ESTRATÉGICA

Las relaciones de la empresa con su entorno se han venido modificando profundamente desde comienzos de los años ochenta, en efecto en décadas presentes, la evolución futura de las empresas podría estimarse, razonablemente a partir del análisis incremental tanto de la situación inicial como la de las situaciones anteriores. En el contexto actual el entorno de la empresa es mucho más inestable no lineal, por lo que la necesidad de anticipación del futuro es mucho más apremiante que en el pasado. 4.

Así la auditoría inicialmente vinculada a la esfera estrictamente financiera, se va expandiendo hacia otros dominios y es específicamente la auditoría de la estrategia que conceptualmente, presenta un campo de aplicación de mayor alcance.

---

3 Oliek González Solán, Jorge de la Vega Yabor. Los Sistemas de Control de Gestión Estratégica para las organizaciones(trabajo de investigación). Barcelona España

4 José Joaquim Marques de Almeida. Revista Contaduría y Administración N203, octubre-diciembre 2001 /(Schuster, 1996, p.3)

Sin embargo, se cree que los objetivos y dimensiones de la auditoría engloban en el momento presente y cada vez con contornos más nítidos, el análisis de la estrategia de la empresa, frente al hecho de que el auditor tenga que obtener un conocimiento total del negocio del cliente, de la industria y de toda la economía.

Algunos autores consientes de que los errores estratégicos pueden ser "altamente onerosos", para las empresas e inclusivemente, llegar a amenazar su continuidad , proponen de la auditoría anual de la estrategia de la empresa, aunque sea bajo la forma de rolling audit, presente un informe prioritario en el desarrollo del trabajo de los auditores, no limitándose a una crítica sobre las estrategias que han orientado a la empresa en el pasado, sino que de preferencia, aconsejan a la mesa de dirección con la finalidad de determinar la estrategia que mejor conduzca a la organización hacia el futuro[5].

Cabe mencionar que la auditoría estratégica abarca el análisis de los factores estratégicos internos y externos, incluyendo la selección de ésta, su implantación, evaluación y control.

Por lo que tal auditoría representará una visión integradora de la estrategia empresarial en acción, materializándose en decisiones operacionales importantes y administrativas[6]

Ahora bien, las decisiones estratégicas, en un entorno de complejidad no lineal, en el que el todo ya no es igual a la suma de las partes, por el efecto de sinergias, apelan para que la información por utilizar en la contabilidad de gestión sea también no lineal[7].

Es de advertir que las decisiones estratégicas no son exclusivas de los auditores y en efecto, muchos administradores apuntan que este tipo de auditorías interfieren llegando a señalar incluso, una falta de competencia técnica del auditor para entender el proceso de decisión estratégica.

La contribución de los auditores independientes en la evaluación de la estrategia se debe fundamentalmente al nacimiento de los comités de auditoría a su papel de creciente importancia en la

---

[5] (Rappaport, 1980. P. 71) (Lausenstein, 1994. P.87). (Wheelen, 1997.p.6)

[6] José Joaquim Marques de Almeida. Revista Contaduría y Administración N203, octubre-diciembre 2001.

[7] (Sawer, 1996.p.89)

organización de la integridad del informe financiero de las empresas y su desempeño en el nombramiento auditores independientes que asesoran a la administración de la misma.

La auditoría de la estrategia abarca ocho puntos convenientemente relacionados que son: [8]

- Evaluación de la performance corriente de la organización en términos de ganancia,
- Recuperación de las inversiones, misión, objetivos, estrategia y políticas.
- Examen y evaluación de la dirección estratégica de la organización.
- Análisis del entorno externo con el objetivo de localizar las oportunidades y amenazas que se colocan en la organización.
- Análisis del entorno interno
- Análisis de los factores utilizando la matriz FODA,
- Implantación de la estrategia con programas presupuestos y procedimientos adecuados.
- Evaluación de la implantación de las estrategias

Para que el auditor pueda evaluar debe obtener las evidencias necesarias y valorar críticamente la empresa como un todo, lo que presupone la existencia de un plan estratégico. [9].

De ahí la necesidad de comprender la posición del cliente dentro de la cadena de valor y su capacidad para sustentar las ventajas competitivas con el entorno. Según Bell (1997,p.31), la comprensión del negocio del cliente abarca[10]

- La comprensión de la ventaja estratégica del cliente.
- La comprensión de los riesgos que amenazan la consecución de los objetivos de la empresa.
- Medir y comparar la performance obtenida con los competidores más eficientes
- Comprender a través de un modelo, el negocio del cliente y su habilidad para crear y generar ganancia.
- Usar la comprensión del negocio para desarrollar previsiones acerca de los factores claves subyacentes a los estados financieros.
- Comparar las previsiones con las realizaciones y diseñar tests de auditoría que aborden los desvíos entre las realizaciones y las previsiones.

[8] Wheelen y Hunger (1978, p.56)/ (Rappaport 1990 p.75)
[9] 9José Joaquim Marques de Almeida. Revista Contaduría y Administración N203, octubre-diciembre 2001.
[10] 10 Idem

- El enfoque en el riesgo del negocio se traduce en una orientación global, holística y sistemática de la auditoría.

Este tipo de auditoría constituye la respuesta más eficaz para garantizar el principio de la empresa en marcha, ya que establece la actividad mediante la utilización de determinadas técnicas especializadas de revisión tiene por objeto la emisión de un informe acerca de la fiabilidad de los documentos previsionales auditados[11].

Se trata pues de un nuevo campo de investigación, hasta el momento poco desarrollado, que impone al auditor una actitud proactiva en la evaluación de los aspectos relacionados con la gestión, la eficiencia, la eficacia y la posición competitiva de la empresa, en la convicción de que además de la información financiera, existen aspectos operacionales de gestión estratégica que deben ser sometidos a revisión y evaluación por parte de un profesional independiente.[12]

1.2.1 CONCEPTO DE AUDITORÍA ESTRATÉGICA

La auditoria estratégica es una investigación promovida desde la Dirección General que tiene como objetivo realizar un diagnóstico de la posición estratégica de la empresa y emitir un pronóstico acerca de las consecuencias de mantener el rumbo actual (*Francisco J. Manso Coronado* Publicado en la revista ***Estrategia Financiera*** nº 97, 1994)

1.2.2 CARACTERÍSTICAS DE LA AUDITORÍA ESTRATÉGICA

La auditoría estratégica es una auditoría de dirección que abarca una perspectiva corporativa y que comprende una valoración de la situación estratégica empresarial y en la medida que la administración tiene conciencia de la expansión de sus responsabilidades y obligaciones, recurrirán a un mayor uso de éstas herramientas; permitiendo entender donde se interrelacionan las diferentes áreas funcionales, así como la forma en que contribuyen al logro de los objetivos de la empresa. [13]

A diferencia con la auditoría de gestión, esta es de dirección y abarca una perspectiva corporativa y amplia.

---

[11] (Mailo Rodriguez, 1998, p. 767).
[12] José Joaquim Marques de Almeida. Revista Contaduría y Administración N203, octubre-diciembre 2001. / (Prado Lorenzo. 1998.p.875)
[13] *Francisco J. Manso Coronado,* Publicado en la revista ***Estrategia Financiera*** nº 97, 1994

Del análisis de la empresa, del conocimiento de todo su entorno y de los agentes que componen su sector de actividad, se obtienen unas conclusiones que permiten diagnosticar en qué situación se encuentra la organización objeto de estudio.

1.2.3 IMPORTANCIA DE LA AUDITORÍA ESTRATÉGICA

La importancia se centra en el método empleado, el cual es un proceso ordenado y riguroso para investigar y conocer con detalle la realidad de la empresa.

Asimismo se considera una herramienta que facilita información acerca de las características y las tendencias principales del entorno y del mercado en el que opera una empresa, obtener un perfil de sus principales competidores y profundizar en sus capacidades y ventajas competitivas y que como resultado, se obtienen unas conclusiones que resaltan sus debilidades y fortalezas, así como las amenazas a las que se enfrenta y por ende las oportunidades que deben aprovecharse; las cuales son la base del diagnóstico de la empresa. [14]

Tomando como referencia las ventajas competitivas de la empresa, también ésta define las opciones estratégicas recomendables y los puntos críticos de actuación que debe aportar a la Administración una clara propuesta de hacia dónde debería dirigirse la organización que representa, o en su defecto, si los objetivos elegidos por dicha organización son alcanzables en base a la situación en la que se encuentra.

En definitiva, esta auditoría permite conocer dónde está la empresa y dónde debería estar en el futuro, para, realizar los planes necesarios en base a los objetivos que se definen en el plan estratégico.
Cabe mencionar que esta auditoría cumple tres funciones fundamentales:
a) Clarificar y revisar conceptos importantes de cada una de las áreas elegidas.

b) Proporcionar un marco de referencia sistemático para el análisis en situaciones complejas.

c) Mejorar la calidad del análisis estratégico, ahorrando mucho tiempo y dinero, sobretodo porque reduce el riesgo de definir falsos problemas estratégicos.

---

14 Francisco J. Manso Coronado, *Publicado en la revista* Estrategia Financiera *nº 97, 1994*

Se toma en cuenta con factores internos como externos, comprendiendo la selección de alternativas, su ejecución, su evaluación y control, su orientación es desde un análisis formal en el presente para orientar la acción del futuro; por tanto, abarca los aspectos clave del proceso de dirección, situándolos en un cuadro apropiado de toma de decisiones.

1.2.4 CLASIFICACIÓN DE LA AUDITORÍA ESTRATÉGICA

La realización del estudio puede ser de carácter interno o externo, ya que un auditor externo puede hacer una "fotografía de la empresa" en un determinado momento; por el contrario, el auditor interno tiene un acceso permanente a la evolución de la empresa, como si se tratase del "rodaje de una película", pero tiene el inconveniente de que su análisis está condicionado por sus percepciones y experiencias directas. [15].

Al margen de que la Administración prefiera acudir a un consultor o delegar esta función en personal propio, siempre debe existir dentro de la empresa un coordinador que se encargue de vigilar la correcta ejecución de la estrategia y del seguimiento de los principales indicadores de la actividad. Por lo que la del Director de Estrategia; en las empresas se denomina administrador o simplemente director quien está a cargo del correcto funcionamiento de la misma.

En la elaboración de la auditoría intervienen todos los departamentos de la empresa, desde la administración se desciende en cascada por cada una de las áreas funcionales por lo que es imprescindible, identificar a aquellos puestos claves en el desarrollo de la actividad diaria de la empresa y solicitar su colaboración.

1.2.5 FASES DE LA AUDITORÍA ESTRATÉGICA

En la auditoría estratégica debe existir una Planeación la cual debe basarse en una metodología propia, adaptada a los negocios, que permita alinear las estrategias de éste.

---

[15] Oliek González Solán, Jorge de la Vega Yabor. Los Sistemas de Control de Gestión Estratégica para las organizaciones (Idea tomada del trabajo de investigación). Barcelona España

Las fases o etapas de este tipo de auditoría no es particular a los métodos tradicionales ya utilizados por la auditoría de sistemas puesto que se parte de una circunstancia existente.

El método se basa en una combinación de técnicas cuantitativas y cualitativas, entre las que destacan la observación (directa y documental) y la entrevista en profundidad.

El análisis de la información generada por la propia actividad de la empresa es la parte esencial de este método. Por lo tanto un buen diagnóstico depende principalmente de la correcta interpretación de los datos internos de la empresa.
Por lo que para alcanzar ciertos objetivos de la investigación, se pueden utilizar las siguientes técnicas de apoyo:

- Grupo de discusión (Focus Group).
- Mistery shopping.
- Estudios de satisfacción del cliente externo.
- Estudios de clima laboral - Satisfacción del Cliente Interno.
- Estudios de Calidad de Servicio.
- Análisis de Canales de Distribución, entre otros..

Para hacer una adecuada planeación de la auditoría estratégica a los sistemas de información, es importante seguir una serie de pasos previos que permitirán dimensionar el tamaño y características del área dentro del organismo a auditar, sus sistemas, organización y equipo. El desarrollo de la planeación de la auditoría estratégica a los sistemas de información deben estar en línea con el plan estratégico de la empresa. Adicionalmente crea un marco de trabajo que permite el enfoque integrado del desarrollo de aplicaciones y bases de datos. [16]
En este caso la planeación es fundamental, pues habrá que hacerla desde el punto de vista de los dos objetivos:

[16], Aspectos generales de la auditoría de gestión (Idea tomada del trabajo exaula de María del Carmen Ramírez)

- Evaluación de los sistemas y procedimientos.
- Evaluación de los equipos de cómputo.

Para hacer una planeación de una auditoría estratégica a los sistemas de información eficaz, lo primero que se requiere es obtener información general sobre la organización y sobre la función de informática a evaluar.

Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas a profundidad sobre los planes estratégicos que esta posee, conocer la estrategia del negocio y las prioridades entendiendo las oportunidades y limitaciones, conocer los portafolios de proyectos y servicios, conocer los planes estratégicos de tecnología informática si los posee; con base en esto planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

1.2.5.1 GOBIERNO CORPORATIVO

Lo que se pretende es entender los requerimientos del gobierno corporativo. Como ya es conocido, éste se encarga de representar un delicado balance entre la transparencia, la equidad corporativa y el cumplimiento de responsabilidades al interior de una empresa por lo que le interesa identificar de forma estratégica cuales son las prioridades a corto y largo plazo. Puesto que:

- *La tecnología no sólo crea nuevos riesgos, sino que también desempeña un papel importante en la mitigación de riesgo.*
- *En este sentido, los ejecutivos de TI deben trabajar en estrecha colaboración con la unidad de negocios líderes y ejecutivos*
- *Los directores de adoptar un conjunto de formalizarse reproducible y escalable de riesgos y el cumplimiento tecnologías de gestión y técnicas.*

Las siete áreas claves de riesgo que los CIO`s necesitan debatir en la estrategia y el presupuesto para incluir son las siguientes

a. Planificación de Continuidad de Negocio
b. Planificación de Recuperación ante Desastres

c. La seguridad de la información y la integridad de los datos Relacionadas con la seguridad
d. Sourcing y la externalización
e. Medición del desempeño
f. Estrategia de TI y gastos
g. Infraestructura de gestión de TI

En tal sentido se procede a realizar el trabajo encomendado buscando los parámetros solicitados y previendo las situaciones pasadas, presentes y futuras.

En función de lo anterior se definen claramente las siguientes etapas de la auditoría estratégica.

a) INVESTIGACIÓN PRELIMINAR

Se deberá observar el estado general del área a evaluar, su situación dentro de la organización, si existe la información solicitada, si es o no necesaria y la fecha de su última actualización, verificar los programas estratégicos de la empresa (presupuestos, proyectos a corto y a largo plazo), verificar la viabilidad de los presupuestos o programas que posee la empresa, verificar cuales son sus necesidades prioritarias, a corto y a largo plazo.

Se debe hacer la investigación preliminar solicitando y revisando la información de cada una de las áreas basándose en los siguientes puntos:

1)-ADMINISTRACIÓN

Se recopila la información para obtener una visión general del departamento administrativo por medio de observaciones, entrevistas preliminares de forma profunda sobre el tema (TI) y solicitud de documentos para poder definir el objetivo y alcances del departamento; para analizar y dimensionar la estructura por auditar se debe solicitar: a nivel del área de informática objetivos a corto y largo plazo, dimensionando cuales son las prioridades que se han tenido, verificando además los planes estratégicos que se han implementado recientemente

2)-RECURSOS MATERIALES Y TECNICOS

Solicitar documentos sobre los equipos, número de ellos, localización y características.

- Estudios de viabilidad.
- Estudio de prioridades de equipos

- Número de equipos, localización y las características (de los equipos instalados y por instalar y programados)
- Fechas de instalación de los equipos y planes de instalación.
- Contratos vigentes de compra, renta y servicio de mantenimiento.
- Contratos de seguros.
- Convenios que se tienen con otras instalaciones(si existen)
- Configuración de los equipos y capacidades actuales y máximas
- Planes de expansión[17]
- Ubicación general de los equipos.
- Políticas estratégicas de operación.
- Políticas estratégicas de uso de los equipos.
- Políticas estratégicas del recurso humano encargado de los equipos
- Políticas estratégicas sobre la exactitud de la arquitectura de la información

3)-SISTEMAS

Descripción general de los sistemas instalados y de los que estén por instalarse que contengan volúmenes de información.

- Manual de formas.
- Manual de procedimientos de los sistemas.
- Descripción genérica.
- Diagramas de captura, archivos, salida.
- Salidas de equipos (si se venden, donan, o desechan)
- Fecha de instalación de nuevos equipos
- Fechas de instalaciones de los Software.
- Proyecto de instalación de nuevos equipos
- Proyectos de Instalación de nuevos software
- Planes estratégicos y tácticos de nuevas tecnologías adoptadas o por adoptarse (si existen).

[17] J Oscar Toro, MANUAL DE AUDITORÍA DE SISTEMAS,otoroc@cmet.net Centro de Formación Técnica DIEGO PORTALES, Concepción CHILE

En el momento de hacer la planeación de la auditoría estratégica a los sistemas de información o bien su realización, debemos evaluar que pueden presentarse las siguientes situaciones.

Se solicita la información y se ve que:

- No tiene y se necesita.
- No se tiene y no se necesita.

Se tiene la información pero:

- No se usa.
- Es incompleta. [18]
- No esta actualizada.
- No es la adecuada.
- Se usa, está actualizada, es la adecuada y está completa.

En el caso de No se tiene y no se necesita, se debe evaluar la causa por la que no es necesaria. En el caso de No se tiene pero es necesaria, se debe recomendar que se elabore de acuerdo con las necesidades y con el uso que se le va a dar. En el caso de que se tenga la información pero no se utilice, se debe analizar por que no se usa. En caso de que se tenga la información, se debe analizar si se usa, si está actualizada, si es la adecuada y si está completa.

El éxito del análisis crítico depende de las consideraciones siguientes:

- Estudiar hechos y no opiniones (mas bien no se toman en cuenta los rumores ni la información sin fundamento).
- Investigar las causas, no los efectos; es decir lo que se está haciendo, no lo que se pretendía hacer.
- Atender razones, no excusas.
- No confiar en la memoria, preguntar constantemente.
- Criticar objetivamente y a fondo todos los informes y los datos recabados de manera estratégica
- Identificar los proyectos a futuros.
- Verificar los proyectos a futuros si se les está dando continuidad.
- Dimensionar cuales han sido la causa por la que no se han dado seguimiento a los proyectos.
- Destacar los objetivos que se pretenden lograr con el proyecto en marcha.

[18] J Oscar Toro, MANUAL DE AUDITORÍA DE SISTEMAS,otoroc@cmet.net Centro de Formación Técnica DIEGO PORTALES, Concepción CHILE

- Considerar si es prioritario o no el proyecto.
- Verificar si se están atendiendo las políticas estratégicas.
- Proponer un plan a corto plazo de políticas estratégicas si no existen.
- Explicar al gobierno corporativo la necesidad del plan estratégico. [19]

4)-RECURSO HUMANO PARTICIPANTE

Una de las partes más importantes dentro de la planeación de la auditoría estratégica a los sistemas de información es el personal que deberá participar y sus características.

Uno de los esquemas generalmente aceptados para tener un adecuado control es que el personal que intervengan esté debidamente capacitado, con alto sentido de moralidad, al cual se le exija la optimización de recursos (eficiencia) y se le retribuya o compense justamente por su trabajo.

Con estas bases se debe considerar las características de conocimientos, práctica profesional y capacitación que debe tener el personal que intervendrá en la auditoría. En primer lugar se debe pensar que hay personal asignado por la organización, con el suficiente nivel para poder coordinar el desarrollo de la auditoría, proporcionar toda la información que se solicite y programar las reuniones y entrevistas requeridas.

Éste es un punto muy importante ya que, de no tener el apoyo de la alta dirección, ni contar con un grupo multidisciplinario en el cual estén presentes una o varias personas del área a auditar, sería casi imposible obtener información en el momento y con las características deseadas.

También se debe contar con personas asignadas por los usuarios para que en el momento que se solicite información o bien se efectúe alguna entrevista de comprobación de hipótesis, proporcionen aquello que se esta solicitando, y complementen el grupo multidisciplinario, ya que se debe analizar no sólo el punto de vista de la dirección de informática, sino también el del usuario del sistema.

[19] J Oscar Toro, MANUAL DE AUDITORÍA DE SISTEMAS,otoroc@cmet.net Centro de Formación Técnica DIEGO PORTALES, Concepción CHILE

Para completar el grupo, como colaboradores directos en la realización de la auditoría se deben tener personas con las siguientes características:

- ✓ Conocimiento básico de la auditoría estratégica (conceptual y Técnica)
- ✓ Profesional de Informática (en caso de no poseer conocimientos sobre ésta área).
- ✓ Experiencia en el área de informática del profesional que realizará la investigación.
- ✓ Experiencia en operación y análisis de sistemas.
- ✓ Conocimientos de los sistemas más importantes.

En caso de sistemas complejos se deberá contar con personal con conocimientos y experiencia en áreas específicas como base de datos, redes, etc. Lo anterior no significa que una sola persona tenga los conocimientos y experiencias señaladas, pero si deben intervenir una o varias personas con las características apuntadas lo importante es dar cumplimiento al plan de auditoría estratégica planteado.

Una vez que se ha hecho la planeación, se puede utilizar, las fases y subfases que comprenden la descripción de la actividad, el número de personas participantes, las fechas estimadas de inicio y terminación, el número de días hábiles y el número de días hombre estimado, los recursos estimados y en el tiempo señalado en la planeación.
El hecho de contar con la información del avance permite revisar el trabajo elaborado por cualquiera de los asistentes.

b) PLANEACIÓN

- Definición de los objetivos de la investigación
- Determinar necesidades de información
- Seleccionar las fuentes de información (internas y externas)

c) EJECUCIÓN

- Recopilar la información
- Tratamiento de los datos
- Análisis de la información

- d) ELABORACIÓN DE INFORMES
- Elaboración del informe de conclusiones y diagnóstico
- Propuesta de recomendaciones estratégicas
- Identificar los puntos críticos de actuación
- Definir el timing de seguimiento

Esta auditoría ayuda a la empresa a conocer su situación, es decir por qué ha llegado a dicha circunstancias y hacia dónde se dirige, entonces está en condiciones de replantear sus objetivos, concretar cuál es el mejor modo de alcanzarlos y qué factores debe vigilar para saber si los está consiguiendo.

La capacidad de una organización de realizar una reflexión profunda y abierta para conocerse a fondo el entorno en el que la empresa se mueve constituye una importante ventaja competitiva, que le sitúa en una mejor posición para asumir nuevos retos y dirigir la actividad de la misma hacia nuevos horizontes.

1.3 AUDITORÍA ESTRATÉGICA APLICADA A LOS SISTEMAS DE INFORMACIÓN (SI)

Al final de los años ochenta, las teorías de la Calidad Total y la de Reingeniería a principios de los noventa, el tema de la Planeación Estratégica, había tomado un sitio en el asiento de atrás. Pero a finales de los noventa, se vuelve a retomar con mayor fuerza la necesidad de efectuar Planeación de Auditoría Estratégica a las Tecnología de la Información Y Comunicación (TIC).

La tecnología informática no es ajena a esta necesidad de planeación de auditoría, por lo que actualmente aun se encuentran atrasos en la utilización de la tecnología para implementar las tendencias administrativas. Para reducción de costos se utilizó el modelo Cliente/Servidor y el esquema de soluciones departamentales y dentro del Proceso de Reingeniería, quedaron muchos equipos, programas y procedimientos que nunca se pusieron en práctica. [20]

Se debe entonces efectuar una actividad que permita definir los objetivos de La Tecnología Informática dentro de las empresas, concretando cómo se apoyarán las estrategias del negocio para la obtención

[20] José Camilo Daccach T Boletín Planeación Estratégica de Tecnología Informática (Artículo

de nuevos mercados, y en últimas circunstancias, cuál será el efecto que la inversión en tecnología tendrá en el último renglón del estado de resultados.

En la revista Director de Información (CIO Magazine) publicada en Enero 15 de 1998 se dedicó un informe especial al tema de la Planeación Estratégica de la Tecnología Informática y en este informe se revela una encuesta sobre cómo y por qué los planes estratégicos se han convertido en algo vital para la organización de Sistemas y la compañía; curiosamente estudios recientes también muestran resultados con las mismas tendencias. [21]

El 70.00% de los trescientos uno ejecutivos que contestaron la encuesta informaron que sus empresas han desarrollado un Plan Estratégico de Tecnología Informática (Plan de Auditoría estratégica a los Sistemas de Información).

- La razón principal para crear una estrategia formal para la Tecnología Informática es la necesidad del entendimiento global de la estrategia del negocio.
- El 57%, manifestó que el proceso de planeación se cubría en seis meses o menos.
- El 30% de las empresas no conducen un proceso formal de planeación estratégica de tecnología informática,

Las prácticas más efectivas para la planeación estratégica incluyen las entrevistas ejecutivas (57%), reuniones enfocadas en el cliente (52%) y reuniones fuera de la oficina (50%). [22]

1.3.1 IMPORTANCIA DE LA AUDITORÍA ESTRATÉGICA A LOS SISTEMAS DE INFORMACIÓN

La necesidad que tienen las empresas de ajustarse rápidamente a los cambios drásticos en el ambiente económico hacen necesario que la administración ejecutiva tenga información disponible y actualizada, de tal manera que un adecuado uso de ésta, puede tomar las decisiones efectivamente con la gran

[21] José Camilo Daccach T Boletín Planeación Estratégica de Tecnología Informática
[22] Idem

disponibilidad de información a través de toda la empresa, las estrategias se pueden mejorar, las decisiones se pueden tomar con mejor base y las operaciones ejecutadas más eficiente.

El plan de auditoría estratégica a los Sistemas de Información, debe determinar qué se debe de hacer, cómo lo va hacer, y cómo puede darse cuenta si cumple o no con sus objetivos. Luego puede definir la dirección en la cual se está moviendo el departamento de TI, por tanto sino se establece una dirección clara es muy poco probable que se logre algo de importancia relevante. Además, sino se tiene retroalimentación la dirección del departamento de TI no puede evolucionar efectivamente a medida de que el tiempo y las necesidades cambian.

También sino existe un plan de auditoría estratégica a los sistemas de información, no hay una dirección adecuada. [23]

La decisión de desarrollar y usar un plan de auditoría estratégica a los Sistemas de Información debe ser considerada a la luz de cultura y el estudio de cada empresa en particular. Si una empresa no utiliza planeación estratégica en ninguna parte, es muy probable que un Plan de Auditoría Estratégica de Tecnología Informática (PAETI) se vea con escepticismo y burla.
Cuando se analiza la planeación de auditoría estratégica de tecnología informática es de vital importancia tener una guía que provea una metodología y una estructura general para el proceso de planeación.

1.3.2 OBJETIVOS DE LOS PLANES DE AUDITORÍA ESTRATÉGICA DE SISTEMAS DE INFORMACIÓN (SI)

Con una adecuada planeación de auditoría estratégica a los sistemas de información y control, el usuario de un método de planeación estratégica de tecnología informática debe poder obtener los objetivos que se describen a continuación. [24]

1. Establecer el proceso de planeación de auditoría estratégica de tecnología informática.

[23] www.deltaasesores.com/2004 J:C Daccach T.
[24] Idem

2. Proveer un método formal y objetivo para que la administración establezca, sin sesgos, las prioridades hacia la tecnología informática. que contribuya a que los sistemas desarrollados sean duraderos, protegiendo la inversión en tecnología.

3. Permitir que los recursos de tecnología se administren de la mejor manera para que eficiente y efectivamente soporten los objetivos del negocio, aumentando la confianza en la posibilidad del uso de información oportuna y veraz para la toma de decisiones.

4. Mejorar las relaciones entre el departamento de sistemas de información y los usuarios mediante el diseño e implementación de sistemas que respondan a las necesidades y a las prioridades de los usuarios, de tal manera que pueda ser usado efectivamente por todos los que la necesitan.

1.3.3 ÁREAS CRÍTICAS A CONSIDERAR EN EL PLAN DE UNA AUDITORÍA ESTRATÉGICA A LOS SISTEMAS DE INFORMACIÓN

Entre las áreas críticas que pueden ser consideradas en una Planeación de Auditoría estrategia a los Sistemas de Información figuran las siguientes:

- Estructura Administrativa: La estructura de toda empresa se obtendrá de acuerdo a la óptima clasificación que requiera, que se pueden agrupar generalmente en cuatro grandes áreas funcionales como son: Producción, Administración, Finanzas, y Recursos Humanos.

- Sistemas de Administración Automatizados; estos hacen referencia a las prioridades de la compañía, donde se contempla la transformación continua de las sucursales; tal es el caso de las sucursales virtuales de una compañía determinada, donde realiza comercio electrónico (e-commerce).

- Adquisición de Equipos de cómputo y Adquisición de Programas (software): El equipo que se adquiere como parte de los sistemas de información, es uno de los elementos fundamentales para que éstos funcionen en forma apropiada y eficiente, es por esa razón que todo equipo que se adquiera deberá contar con los requisitos mínimos del software a utilizar en la compañía.

- Mantenimiento de Equipos: Gran parte de los problemas que se presentan en los SI se pueden evitar o prevenir si se realiza un mantenimiento periódico de cada uno de sus componentes, es decir el mantenimiento debe ser preventivo. El mantenimiento de Sistemas (Software): Con el paso de los años se ha ido produciendo un volumen muy grande de software. Y actualmente, la mayor parte de

éste software está formado por código antiguo "heredado"; en muchas ocasiones, la situación se complica porque el código heredado fue objeto de múltiples actividades de mantenimiento; por consiguiente es importante un mantenimiento preventivo en los software.

- Sistemas para la Automatización de las Oficinas de Trabajo (procesadores de palabra, programas para edición y presentación) la ofimática debe estar al servicio de la gestión empresarial pues representa la aplicación de la informática a las tareas menos estructuradas que se desarrollan en una organización.

- Sistemas Especializados[25] en Actividades Específicas: Este tipo de sistema contribuye a que determinadas actividades que para el ser humano se vuelven tediosas sean realizadas en poco tiempo y con menor esfuerzo entre ellos encontramos; el lector del código de barra, Lectores tipo pluma o lápiz, lectores de ranura o slot, lectores tipo rastrillo o CCD, lectores láser de proximidad los cuales sirven por ejemplo para controles de inventario, registro de electores, votación y conteo electrónico, sistemas generales de finanzas o personal.

- Administración de la Información: Se debe contar con los controles adecuados para el manejo de la información tanto magnética como física, la cual debe ser manejada de forma cautelosa.

- Integración y Compatibilidad de Sistemas: en la integración de los Sistemas se debe contar con los manuales adecuados y las bases de datos, de tal manera que al realizar algún tipo de integración con otro sistema debe ser compatible para evitar posible pérdida de información. Además es importante la verificación y Prueba de Sistemas: antes de utilizar un software, tanto estándar o a la medida realizando las correspondientes pruebas pilotos para conocer las características básicas de este.

- Administración de Servidores: los servidores deben ser administrados de tal manera que existan las políticas necesarias para el resguardo de la información que ahí se procesa. Además es importante la administración de Redes tanto redes físicas y redes no físicas donde fluye la información por lo tanto es importante una buena administración de la misma.

---

[25] "Management of Advanced Technology in Elections", Harry Neufeld, Management Consultant, Canada. (Del boletín Desarrollo de una Estrategia Integral de Tecnología Informática)

- Administración de Comunicaciones: tanto la comunicación física, como la comunicación vía teléfono u otro medio, debe fluir en el momento apropiado.

- Archivos y Respaldos de Datos: El problema más significativo en el manejo de información informática lo constituye su respaldo. A pesar de todos los avances de los sistemas operativos que en alguna medida impiden que se pierda información al producirse una falla del software, los problemas de pérdidas de la integridad de la información continúan siendo frecuentes; la solución consiste en realizar respaldos periódicos de los archivos o documentos relevantes.

- Capacitación del Personal:[26] para el buen funcionamiento de los equipos y el sistema, el personal que se contrate para el manejo de éstos deben de poseer los entrenamientos sobre las funciones mínimas del software y del equipo en general, ya que del procesamiento de los datos que el personal realice se obtendrá la información final.

- Suministros para Equipos de Computo: los suministros para el equipo debe ser el adecuado y compatible con el mismo, debido a que se trata del cuidado y manejo adecuado de éstos para la obtención de buenos resultados. La administración de Suministros e Inventarios, controles de almacén y distribución: como punto principal de la entidad, son la parte medular por lo cual debe existir políticas de suministros adecuadas para mantener coherencia tanto en lo físico como en los que se posee en los sistemas; es importante que se identifique el trato al inventario esto implica el almacenaje y la distribución

- Administración obsoleta (Basura Digital): La imposición de altas multas financieras severas a las empresas, ayudarán a solucionar el problema de la contaminación por esa causa, y de los basureros ilegales; algunas computadoras se reciclan y se venden como equipos de segunda mano a naciones con menos posibilidades económicas, y, por ejemplo, algunas empresas direccionan programas gracias a los cuales sus clientes pueden botar sus ordenadores viejos sin costo alguno. Este plan incluye a compañías socias y contempla una amplia red organizada para cumplir todo un ciclo de tratamiento de desechos.

---

[26] " Management of Advanced Technology in Elections", Harry Neufeld, Management Consultant, Canada. (Del boletín Desarrollo de una Estrategia Integral de Tecnología Informática).

- Ambiente Físico: donde estén colocados los servidores, cableado y demás accesorios debe ser el adecuado de tal manera que garanticen le fluidez de la información.

- Seguridad, Encriptamiento, Protección contra virus y control de calidad para garantizar la confiabilidad de la información: incluye las tres clases de controles fundamentales implantados en el software del sistema, integridad del sistema, confidencialidad (control de acceso) y disponibilidad. Asegurar la Disponibilidad de la Información: se trata de los planes estratégicos que debe mantener la entidad sobre el aseguramiento de la información que se procesa, mediante políticas y procedimientos, sobre el manejo de ésta.

- Sistemas de Contingencia Manuales: en los sistemas de contingencia implica las soluciones inmediatas a tomar, si falla el sistema principal.

- Seguros: tanto al software como al hardware[27], puesto que ambos se combinan para el propósito de la entidad,

- Medidas para el acceso público, Política de información pública y estándares privados: Las actuales circunstancias obligan a las entidades a tomar actitudes y criterios técnicos para el tratamiento de la información contenida en los documentos informáticos, con especial interés, principalmente por la vulnerabilidad del sistema, y no sólo por el soporte de los mismos sino principalmente por la implicancia que tiene la accesibilidad a determinados documentos que por sus características no deben ser de acceso a todos; por lo que se deben crear políticas que delimiten que clase de información debe ser de acceso público y cuales serán las medidas sobre ese acceso.

- Redes: se debe tomar en cuenta que los controles sobre la actividad de los centros de datos y otras funciones de apoyo al sistema, incluyen tanto las redes, cableados, por donde debe fluir la información.

- Presupuestos: Son importantes para tomar en cuenta los proyectos como punto de partida para algún tipo de decisión sobre el rumbo de la entidad, conociendo de esta manera sus propósitos.

---

[27] " Management of Advanced Technology in Elections", Harry Neufeld, Management Consultant, Canada. (Del boletín Desarrollo de una Estrategia Integral de Tecnología Informática).

- Control de Gastos: se debe considerar cada uno de los egresos como gastos que posee la empres para tomar en cuenta los presupuestos y proyectos a considerar.

- Reportes Financieros[28]: partiendo de los reportes financieros, se comienza a investigar, si los procedimientos para obtenerlos, han sido los adecuados, o si ha existido algún tipo de negligencia o errores en el procesamiento de los datos. Con relación a los procedimientos de Auditoría Financiera: se debe conocer los procedimientos empleados en el desarrollo de las auditorías financiera, con el propósito de considerar si éstos han tomado el rumbo necesario en la entidad.

1.3.4 BENEFICIOS POTENCIALES DE UN PLAN DE AUDITORÍA ESTRATÉGICA DE TECNOLOGÍA INFORMÁTICA

El desarrollo de un plan de auditoría estratégica de Tecnología Informática ofrece muchos beneficios potenciales a tres áreas que son: [29]

a) DEPARTAMENTO DE SISTEMAS

- Comunicación y concientización de la alta gerencia
- Una mejor base para planeación a largo plazo de los presupuestos del área.
- Personal mejor entrenado y más experto para responder a las necesidades del negoció.
- Usuarios involucrados en la fijación de prioridades en sistemas de información.

b) EJECUTIVOS

- Evaluación de la efectividad de los sistemas de información actuales.
- Una aproximación lógica y definida para ayudar en la solución de problemas de control administrativo desde la óptica del negocio.
- Una evaluación de las necesidades futuras de sistemas y tecnología informática basadas en impacto que tiene su implementación en el negocio y sus prioridades.
- Una aproximación planeada que permita un rápido retorno en la inversión que tiene la empresa en los sistemas de información.

---

[28] " Management of Advanced Technology in Elections", Harry Neufeld, Management Consultant, Canada. (Del boletín Desarrollo de una Estrategia Integral de Tecnología Informática).

[29] www.deltaasesores.com/2004 J:C Daccach T.

- Sistemas de información relativamente independiente de la estructura organizacional.
- Confianza en la dirección dada al sistema de información y su adecuada administración que exista para implementar los sistemas propuestos.

c) GERENCIA OPERATIVA Y FUNCIONAL

- Una metodología definida y lógica para ayudar en la solución de problemas de control administrativo y operativo.
- Consistencia en la información que utilizarán todos los usuarios.
- Involucra a la Alta Gerencia en el establecimiento de objetivos y direcciones organizacionales así como en la definición de prioridades
- Sistemas que son orientados más al usuario administrativo que al usuario técnico.

1.4. ASPECTOS LEGALES RELATIVOS A LOS SISTEMAS DE INFORMACIÓN.

1.4.1 CÓDIGO DE COMERCIO:

De acuerdo a lo que se establece en el Código de Comercio, es permitido que los comerciantes hagan uso de la tecnología informática de tal manera que puedan mantener backup de la información necesaria para la contabilidad, sin embargo no se establece aun los parámetros para llevar una contabilidad digitalizada. (Art. 455 COM).

"Art. 258.- La Junta Directiva miembros y tomará sus resoluciones por mayoría de votos celebrará sesión válida con la asistencia de la mayoría de los presentes.
No obstante lo anterior, las sesiones de Junta Directiva podrán celebrarse a través de video conferencias, cuando alguno o algunos de sus miembros o la mayoría de ellos se encontraren en lugares distintos, dentro o fuera del territorio de la República.

Para los efectos del inciso anterior, será responsabilidad del director secretario grabar por cualquier medio que la tecnología permita, la video conferencia y hacer una transcripción literal de los acuerdos tomados, que asentará en el libro de actas correspondiente, debiendo firmar el acta respectiva y remitir una copia de la misma, por cualquier sistema de transmisión, a todos los miembros de la junta directiva, quienes

además podrán requerir una copia de la grabación respectiva." De lo anterior se denota que ya existe una pequeña brecha en El Salvador, con relación al uso de las tecnologías de la información

1.4.2 **CÓDIGO TRIBUTARIO**

Para la emisión de documentos, en El Salvador se permite que éstos puedan emitirse de forma mecanizada (haciendo uso de sistemas de información), siempre que el emisor cumpla con ciertas mediadas de seguridad. "La Administración Tributaria podrá disponer o autorizar, el reemplazo de los documentos señalados en esta Sección a cambio de otro tipo de control de las operaciones, especialmente a contribuyentes que empleen sistemas especiales o computarizados de contabilidad, siempre que se resguarde la seguridad, cumplimiento y exactitud de los impuestos causados.

La Administración Tributaria podrá autorizar el uso electrónico de los antedichos documentos, siempre que los sistemas computacionales del contribuyente aseguren el cumplimiento y veracidad de los impuestos que se causen," (Artículo 113 Código Tributario)

1.4.3 ACUERDO EJECUTIVO NO 339

Con la nueva era de las TIC`s, El Salvador no ha querido quedarse atrás es así como; Según acuerdo Ejecutivo No 399, de fecha 28 de Mayo de 2004, el cual entró en vigencia el 1 de Junio de 2004, en el ramo de Hacienda se establecen una serie de elementos que contribuyen a una "Estrategia de Gobierno Electrónico", todo ello con el objetivo de aprovechar las nuevas Tecnologías de la Información y Comunicación (TIC).
Este acuerdo facilita a las entidades a declarar de forma más eficiente los impuestos relativos al ramo de Hacienda y al uso de las Tecnologías de la Información y Comunicación

1.4.4 LEY DE FOMENTO Y PROTECCIÓN A LA PROPIEDAD INTELECTUAL

Con relación a la propiedad intelectual se emiten ciertas prohibiciones con el propósito de salvaguardar los Sistemas de Información de las cuales se detallan en el artículo 89-B. de la ley de Propiedad Intelectual - "Se prohíben las siguientes actividades:

a) La fabricación, ensamble, modificación, importación, exportación, venta, arrendamiento o distribución por medio, de un dispositivo o sistema tangible o intangible, sabiendo o teniendo razones para saber que el dispositivo o sistema sirve primordialmente para decodificar una señal de satélite codificada portadora de programas, sin la autorización del distribuidor autorizado de dicha señal; y (2)

b) La recepción y subsiguiente distribución de una señal portadora de programas que haya originada como señal de satélite codificada, teniendo conocimiento que ha sido decodificada sin la autorización del distribuidor legítimo de la señal.

En el articulo 90, de la mencionada ley se estable también el derecho de reclamo por daños o perjuicios ante los tribunales. por la violación de algunos de los derechos conferidos en la ley de Propiedad Intelectual

1.4.5 CÓDIGO PENAL.

En el Código Penal se establecen las sanciones, por violación a los Sistemas de información, específicamente a los sistemas receptores de señales.
Art. 227-C.- Será sancionado con prisión de dos a cuatro años, el que:
a) Fabricare, ensamblare, modificare, importare, exportare, vendiere, arrendare o distribuyere por cualquier medio, un dispositivo o sistema tangible o intangible, sabiendo o teniendo razones para saber que el dispositivo o sistema sirve primordialmente para decodificar una señal de satélite codificada portadora de programas, sin la autorización del distribuidor legítimo de dicha señal; o
b) Recibiere y subsiguientemente distribuyere una señal portadora de programas que se haya originado como una señal de satélite codificada, teniendo conocimiento que ha sido descodificada sin la autorización del distribuidor legítimo de dicha señal

1.4.6 LEY DE IMPUESTO SOBRE LA RENTA (LISR):

La amortización de los Software, se establece en la Ley de Impuesto Sobre la Renta como la deducibilidad de los gastos de la empresa, los software pueden derivarse de la producción o la adquisición, el porcentaje máximo a deducir el 25% el cual será fijo y constante, (es decir 4 años). Según lo establece el artículo 30A LISR.

1.4.7 LEY REGULADORA DEL EJERCICIO DE LA CONTADURÍA.

Es importante hacer notar que el profesional de la Contaduría Pública posee atribuciones que le confiere el consejo las cuales se detallan en el artículo 17 de la Ley Reguladora del Ejercicio de la Contaduría, para cumplir dichas atribuciones el profesional debe estar preparado en el área contable y poseer los conocimientos de diferentes procedimientos incluyendo los de Sistemas de información. Aunque en este artículo no los menciona directamente, hoy en día las entidades para realizar sus operaciones hacen uso de Sistemas de Información.

En la Norma de Educación Continuada se establece como área de educación a cubrirse, "Auditoría, contabilidad, impuestos, INFORMATICA, y cualquier otra materia afín". De tal manera que es de vital importancia el conocimiento básico de Sistemas de Información.

1.5 NORMATIVA TÉCNICA APLICADA A LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN:

1.5.1 NORMA DE AUDITORÍA DE SI PLANEACIÓN (DOCUMENTO N° S5)

Tanto para la planeación de un evento, cualesquiera que sean; se necesitan parámetros y/o lineamientos que contribuyan a mejorar lo que se plantea; es de esta forma que en la auditoría de sistemas existe el documento Nº S5 (Planeación) emitido por la Asociación de Auditoría y Control de los Sistemas de Información (ISACA) por si siglas en ingles; el cual contribuye a planear de manera estratégica este tipo de auditoría; como parte importante a continuación se detallan dichos parámetros:

"**Introducción**

01 Los Estándares de Auditoría de SI de ISACA contienen los principios básicos y procedimientos esenciales, identificados en letras en negrita, los cuales son obligatorios, junto con la documentación relacionada.

02 El propósito de esta Norma de Auditoría de SI es establecer normas y brindar asesoría sobre la planeación de una auditoría.

Estándar

03 El auditor de SI debe planear la cobertura de la auditoría de sistemas de información para cubrir los objetivos de la auditoría y cumplir con las leyes aplicables y las normas profesionales de auditoría.

04 El auditor de SI debe desarrollar y documentar un enfoque de auditoría basado en riesgos.

05 El auditor de SI debe desarrollar y documentar un plan de auditoría que detalle la naturaleza y los objetivos de la auditoría, los plazos y alcance, así como los recursos requeridos.

06 El auditor de SI debe desarrollar un programa y/o plan de auditoría detallando la naturaleza, los plazos y el alcance de los procedimientos requeridos para completar la auditoría.

Comentario

07 Para una función de auditoría interna, debe desarrollarse/actualizarse un plan, al menos una vez al año, para las actividades permanentes. El plan debe servir como marco de referencia para las actividades de auditoría y servir para abordar las responsabilidades establecidas por el estatuto de auditoría. El nuevo/actualizado plan debe ser aprobado por el comité de auditoría, en caso de que éste haya sido establecido.

08 Para el caso de una auditoría externa de SI, normalmente debe prepararse un plan para cada una de las tareas, sean o no de auditoría. El plan debe documentar los objetivos de la auditoría.

09 El auditor de SI debe obtener un entendimiento de la actividad que está siendo auditada. El grado del conocimiento requerido debe ser determinado por la naturaleza de la organización, su entorno y riesgos, y por los objetivos de la auditoría.

10 El auditor de SI debe realizar una evaluación de riesgos para brindar una garantía razonable de que todos los elementos materiales serán cubiertos adecuadamente durante la auditoría. En este momento, es posible establecer las estrategias de auditoría, los niveles de materialidad y los recursos necesarios.

11 El programa y/o plan de auditoría puede requerir ajustes durante el desarrollo de la auditoría para abordar las situaciones que surjan (nuevos riesgos, suposiciones incorrectas o hallazgos en los procedimientos ya realizados) durante la auditoría.

12 Debe consultarse la siguiente documentación para obtener más información sobre la preparación de un plan de auditoría.

Guía de Auditoría de SI G6, Conceptos de materialidad para la auditoría de SI

Guía de Auditoría de SI G15, Planeación

Guía de Auditoría de SI G13, Uso de la evaluación de riesgos en la planeación de la auditoría

Guía de Auditoría de SI G16, Efecto de terceros en los controles de TI de una organización

Marco Referencial de COBIT, Objetivos de control

1.5.2 GUIA DE AUDITORÍA DE SISTEMAS

PLANIFICACIÓN

(DOCUMENTO G15)

La presente guía da los lineamientos que se describen en el documento S5 (Norma de Auditoría de Sistema Planeación), de tal manera que es complementaria:

"1.2 Necesidad de la Orientación

El propósito de esta guía es definir los componentes del proceso de planificación como se indica en el estándar de la S5 IS de Normas de Auditoría.

Esta guía también ofrece para la planificación en el proceso de auditoría para cumplir los objetivos fijados por COBIT

El auditor de SI debe desarrollar un plan de auditoría que toma en consideración los objetivos de la auditoría de interés para el área de auditoría y de su infraestructura de tecnología. En su caso, el auditor se debe también que la zona en estudio y su relación con la organización (estratégico, financiero y / o efectiva), y obtener información sobre el plan estratégico, incluida la SE plan estratégico.

2.2.1 Antes del comienzo de un proyecto de auditoría, la labor del auditor de SI debe planificarse de una forma apropiada para el cumplimiento de los objetivos de auditoría. Como parte del proceso de planificación los auditores de SI deben obtener una comprensión de la organización y sus procesos. Además de dar el auditor una comprensión de la organización de las operaciones de los SI y de sus necesidades, esto es ayudar al auditor en la determinación de la importancia de los recursos se está revisando en lo que se refiere a los objetivos de la organización. Los auditores de SI también deben

establecer el alcance del trabajo de auditoría y realizar una evaluación preliminar del control interno sobre la función que está siendo revisado.

Auditoría de los proyectos deben incluir la consideración de los controles internos, ya sea directamente como parte de la auditoría de los objetivos del proyecto o como una base para la confianza en la información que se reunieron como parte de la auditoría del proyecto. Cuando el objetivo es la evaluación de los controles internos el auditor deberá considerar la medida en que será necesario revisar esos controles. Cuando el objetivo es evaluar la eficacia de los controles durante un período de tiempo el plan de auditoría debe incluir procedimientos adecuados para el cumplimiento de los objetivos de auditoría, y esos procedimientos deben incluir las pruebas de los controles. Cuando el objetivo no es evaluar la eficacia de los controles durante un período de tiempo, sino más bien para identificar los procedimientos de control en un punto en el tiempo, las pruebas de los controles pueden ser excluidos"

1.5.3 GUÍA DE AUDITORÍA DE SI G6, CONCEPTOS DE MATERIALIDAD PARA LA AUDITORÍA DE SI

Este documento al igual que el G15, es complementario a la S5, como parte importante para el desarrollo de un plan de auditoría estratégica a los sistemas de información

Norma de Planificación S5 estados, "El auditor debe planificar los sistemas de información para la cobertura de la auditoría abordar los objetivos de auditoría, para cumplir con las leyes y normas profesionales de auditoría

La evaluación de lo que es material es una cuestión de criterio profesional e incluye el examen de los efectos y / o el efecto potencial sobre la capacidad de la organización para cumplir sus objetivos de negocio en caso de errores, omisiones, irregularidades y actos ilegales que puedan surgir como resultado del control debilidades en el área objeto de la auditoría.

El auditor debe evaluar un control general de TI de la deficiencia en relación a su efecto sobre la aplicación los controles y cuando se suman a otras deficiencias de control Por ejemplo, una gestión decisión de no corregir una deficiencia de control general de TI y su reflexión sobre el control "

1.5.4 GUÍA DE AUDITORÍA DE SI G13, USO DE LA EVALUACIÓN DE RIESGOS EN LA PLANEACIÓN DE LA AUDITORÍA

Como parte importante en la evaluación de los riesgos en una auditoría una auditoría estratégica a los sistemas de información la G13, contribuye a dar algunos lineamientos importantes siendo además complementaria a la S5

"El auditor debe planificar la cobertura de la auditoría para hacer frente a la auditoría objetivos y cumplir con las leyes y normas profesionales de auditoría"

Esta guía ofrece orientación en la aplicación de Normas de Auditoría SI. El auditor debe considerar que para determinar la forma de lograr la aplicación de las normas de S5 y S6, utilice su juicio profesional en su aplicación, y estar dispuestos a justificar cualquier desviación

Todas las metodologías de evaluación de riesgos se basan en apreciaciones subjetivas, en algún momento en el proceso (por ejemplo, para la asignación de ponderaciones a los distintos parámetros). El auditor debe determinar la subjetividad decisiones necesarias para utilizar una determinada metodología y examinar si estas sentencias pueden ser realizadas y validadas a un nivel adecuado de precisión

Cuanto más alta sea la evaluación de los riesgos inherentes y de control más pruebas de auditoría se deben tomar normalmente a partir de obtener el cumplimiento de los procedimientos sustantivos de auditoría.

1.5.5 GUÍA DE AUDITORÍA DE SI G16, EFECTO DE TERCEROS EN LOS CONTROLES DE TI DE UNA ORGANIZACIÓN

La guía de auditoría G16, contribuye a enriquecer los lineamientos sobre la planeación en una auditoría estratégica a los sistemas de información, considerándose además como complementaria a la S5 (Planeación) descrita en éste capítulo; así:

Como parte del proceso de planificación, el auditor se debe obtener un documento y la comprensión de la relación entre los servicios prestados por el tercero y la organización del entorno de control. El auditor se debe considerar la posibilidad de revisar tales cosas como el contrato, acuerdo de nivel de servicio, políticas y procedimientos entre el tercero y la organización.

El auditor debe identificar cada control, su ubicación en el conjunto de control (interno o externo), el tipo de de control, su función (preventivas, correctivas o de detectives) y la organización que realiza la función (interna o externa).

El auditor debe evaluar el riesgo de los servicios prestados por el tercero para la organización, sus controles y el control objetivos y determinar la importancia de los controles de terceros a la capacidad de la organización para cumplir sus objetivos de control.

1.5.6 OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y LAS TECNOLOGÍAS RELACIONADAS (COBIT)

Emitido por el Comité Directivo de COBIT y el IT Governance Institute y la Information Systems Audit and Control Association (ISACA)

La misión principal de COBIT es: investigar, desarrollar y promover un conjunto de objetivos de control en tecnologías de información con autoridad, actualizados de carácter internacional y aceptado generalmente para el uso cotidiano de gerentes de instituciones y auditores

Algunos indicadores que propone COBIT, para evaluar las TIC son los indicadores claves de desempeño:

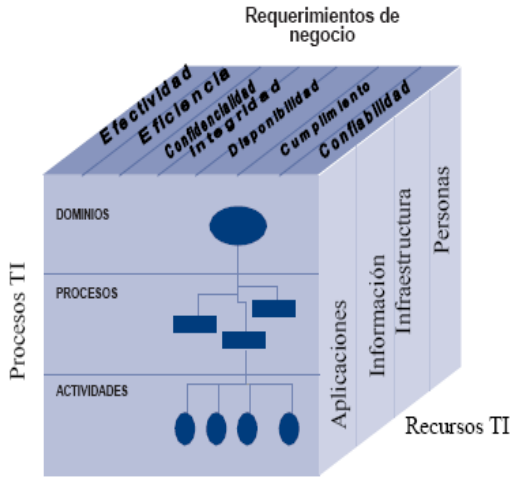
- Mejorar los procesos de costo-eficiencia de TI.
- Incrementar el número de planes de acción de TI para las iniciativas de mejoramiento de procesos,
- Incrementar la utilización de la infraestructura de TI
- Incrementar la satisfacción de los socios y accionistas (encuestas y numero de reclamaciones)
- Incrementar la productividad de los funcionarios de TI
- Incrementar la disponibilidad de los conocimientos e información para administrar la empresa.

- Incrementar las relaciones entre el gobierno de la empresa y el gobierno de TI.
- Incrementar el desempeño mediante mediciones utilizando tarjetas de medición

La necesidad del aseguramiento del valor de TI, la administración de los riesgos asociados a TI, así como el incremento de requerimientos para controlar la información, se entienden ahora como elementos clave del gobierno de la empresa. El valor, el riesgo y el control constituyen la esencia del gobierno de TI.

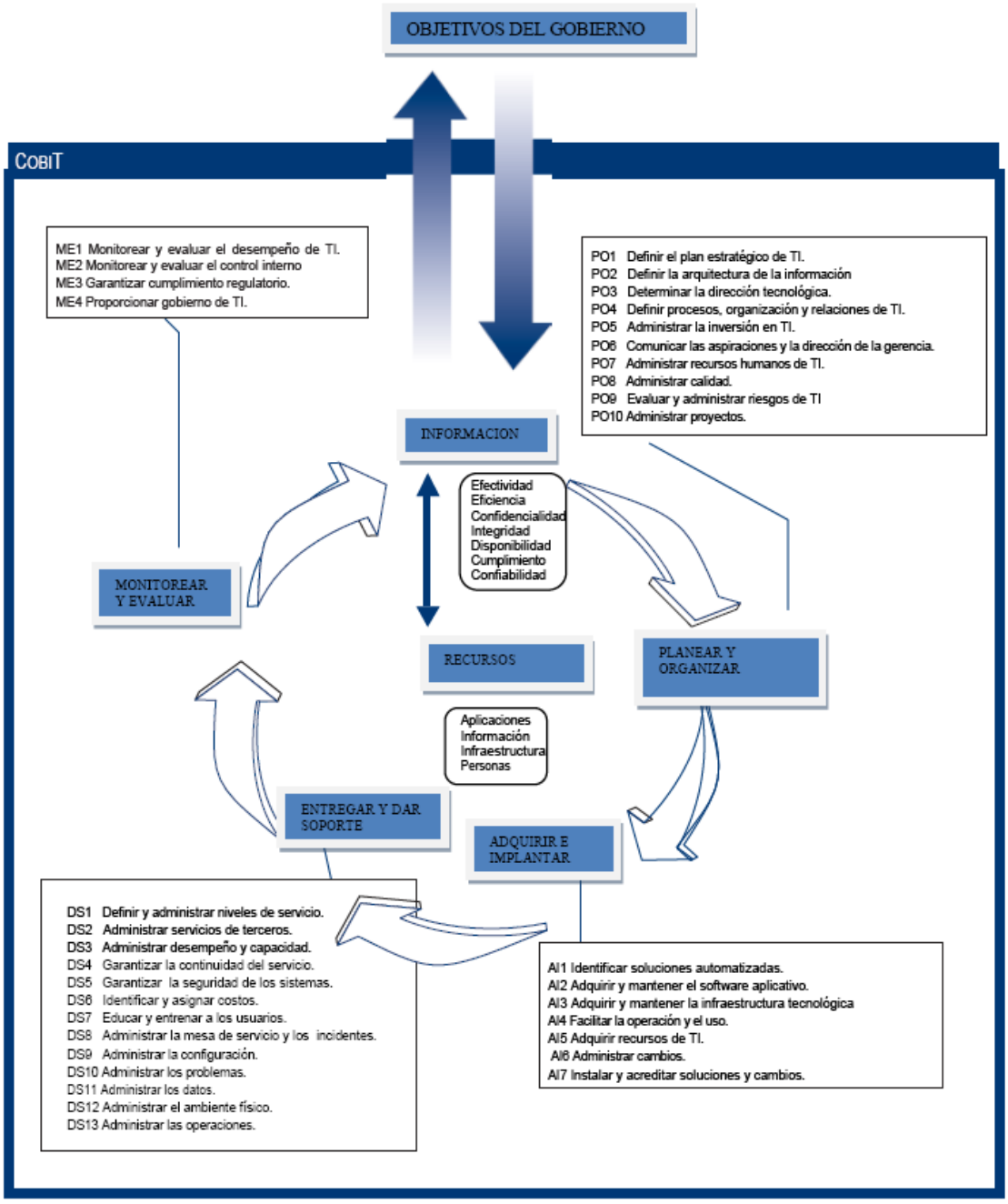
El gobierno de TI es responsabilidad de los ejecutivos, del consejo de directores y consta de liderazgo, estructuras y procesos organizacionales que garantizan que la TI de la empresa sostiene y extiende las estrategias y objetivos organizacionales. [30]

El cubo COBIT



Areas Focales del Gobierno de TI

[30] IT Governance Institute 3701Algonquin Road Suite 1010 Rolling Meadows ISBN 1-933284-37-4 COBIT 4.0



31

[31] IT Governance Institute 3701Algonquin Road Suite 1010 Rolling Meadows ISBN 1-933284-37-4 COBIT 4.0

1.5.7 COMMITTEE OF SPONSOING ORGANIZATIONS (COSO).

Por las siglas en Inglés del comité que patrocinó los estudios que lo produjeron. Emitido además por la Comisión; Treadway (EUA).

El objetivo principal de este informe es la estandarización de conceptos de control interno que ayuden a evaluar de mejor manera sus sistemas de control y gestión y tomar decisiones de cómo mejorar estos sistemas.

1.5.8 CRITERIOS DE CONTROL (COCO)

Por sus siglas en ingles de una parte medular de sus aportes, emitido por el Instituto Canadiense de Contadores Certificados (CICA) o Jurados de Cuenta.

Este informe es muy similar al COSO, no obstante se diferencia por el establecimiento de criterios de aplicación y un enfoque más humanístico, es decir el éxito de su aplicabilidad recae en todas las personas y no en unas cuantas como lo establece el COSO:

1.5.9 CADBURY.

Este informe hace honor al realizador Sr Walter Cadbury, Emitido en el reino Unido por el Consejo de Información Financiera, la Bolsa de Londres entre otros.

Algunas normas que se consideran:

- Responsabilidad que les compete a los directores y administradores para revisar e informar a los accionistas y otras partes interesadas.
- Composición, rol y desempeños de los comités de auditoría
- Responsabilidad de directores y administradores en el control, alcance y el valor de la auditoría.
- Establece los puntos de contacto entre accionistas, directores y auditores.

1.5.10 NORMAS INTERNACIONALES DE AUDITORÍA. (NIA)

Las Normas internacionales de auditoría, son el parámetro para realizar cualquier tipo de auditoría; en tal sentido se parte de que debe existir una planeación sobre el trabajo que se ha de realizar

1.5.10.1 OBJETIVO Y PRINCIPIOS GENERALES QUE GOBIERNAN UNA AUDITORÍA DE ESTADOS FINANCIEROS. (NIA 200)

Es de aclarar que el objetivo principal de esta norma se basa en los principios generales de una auditoría de Estados financieros, no obstante es necesario conocer las necesidades que conllevan a la realización de una auditoría de ese tipo y si la entidad utiliza sistemas de información para el procesamiento de los datos, la cual no exime de posibles errores de importancia relativa en ese evento por tanto aunque "el propósito de esta Norma Internacional de Auditoría (NIA) es establecer normas y dar lineamientos sobre el objetivo y los principios generales que gobiernan una auditoría de estados financieros".

También describe la responsabilidad de la administración por la preparación y presentación de los estados, financieros y por la identificación del marco de referencia de información financiera que se ha de usar para preparar los estados financieros, al cual se refiere la NIA como el "marco de referencia de información financiera aplicable", así mismo es responsabilidad de la entidad un buen procedimiento para el proceso de sus datos.

1.5.10.2 RESPONSABILIDAD DEL AUDITOR DE CONSIDERAR EL FRAUDE EN UNA AUDITORÍA DE ESTADOS FINANCIEROS. (NIA 240)

Tanto en una Auditoría de Estados financieros, como en la auditoría Estratégica a los sistemas de información el auditor posee un grado de responsabilidad sobre su trabajo realizado, según sus aseveraciones hechas puesto que esto implica dar un punto de vista de la entidad en tal momento.

Así "el propósito de esta Norma Internacional de Auditoría (NIA) es establecer normas y proporcionar lineamiento sobre la responsabilidad del auditor de considerar el fraude en una auditoría de estados

financieros y abundar en cómo deben aplicarse las normas los lineamientos de la NIA 315, Entendimiento de la entidad y su entorno y evaluación de los riesgos de representación errónea de importancia relativa y de la NIA 330. Procedimiento del auditor en respuesta a los riesgos evaluados en relación con los riesgos de representación errónea de importancia relativa debida a fraude. Las normas y lineamientos de esta NIA son con la intención de integrarse en el proceso global de auditoría". Esto implica que el profesional debe estar preparado básicamente sobre el trabajo que se propone a desempeñar y sobre los requerimientos que las entidades exigen.

1.5.10.3 ENTENDIMIENTO DE LA ENTIDAD Y SU ENTORNO Y EVALUACIÓN DE LOS RIESGOS DE REPRESENTACIÓNERRÓNEA DE IMPORTANCIA RELATIVA. (NIA 315)

Esta norma se basa en el establecimiento de lineamientos para entender el negocio y considerar sus riesgos existentes, de tal manera que se pueda dilucidar los planes a seguir para la elaboración de una auditoría. Es así como "El propósito de esta Norma Internacional de Auditoría (NIA) es establecer normas y proporcionar guías para obtener un entendimiento de la entidad y su entorno, incluyendo su control interno, y para evaluar los riesgos de representación errónea de importancia relativa en una auditoría de estados financieros", la cual debe ser considerada en una auditoría estratégica los sistemas de información

"El auditor usa el juicio profesional para determinar el grado requerido de entendimiento de la entidad y su entorno, incluyendo su control interno. La principal consideración del auditor es si el entendimiento que se ha obtenido es suficiente para evaluar los riesgos de representación errónea de importancia relativa de los estados financieros y para diseñar y desempeñar procedimientos adicionales de auditoría. La profundidad del entendimiento general que requiere el auditor al desempeñar la auditoría es menor que la que posee la administración para manejar la entidad"

"Planear una auditoría implica establecer la estrategia general de auditor para el trabajo y desarrollar un plan de auditoría, para reducir el riesgo a un nivel aceptablemente bajo. La planeación involucra al socio del trabajo y a otros miembros claves del equipo para ganar de su experiencia y clara percepción y para enriquecer la efectividad y eficiencia del proceso de planeación." NIA 300

Dada la necesidad de establecer parámetros en los diferentes trabajos de auditoría, existen diferentes guías y/o procedimientos que establecidos por diferentes normas una de ellas es la NIA, 402, la cual se refiere a

"Consideraciones de auditoría relativas a entidades que utilizan organizaciones de servicio"

"Al obtener un entendimiento de la entidad y su entorno, el auditor deberá determinar la importancia de las actividades de la organización de servicio para la entidad y la relevancia para la auditoría. Al hacerlo así, el auditor obtiene un entendimiento de lo siguiente, según sea apropiado:

Información disponible sobre los controles relevantes a los sistemas de información de la organización de servicio, como controles generales de TI (Tecnología de la Información) y controles de aplicación."

1.5.10.4 EVIDENCIA DE AUDITORÍA. (NIA 500)

"El propósito de esta Norma Internacional de Auditoría (NIA) es establecer normas y proporcionar guías sobre lo que constituye evidencia de auditoría en una auditoría de estados financieros, la cantidad y calidad de la evidencia de auditoría que se debe obtener, y los procedimientos de auditoría, que usan los auditores para obtener dicha evidencia; .el auditor deberá obtener evidencia suficiente apropiada de auditoría para poder llegar a conclusiones razonables en las cuales basar la opinión de auditoría"

Bajo el lineamiento que el auditor debe basar su opinión sobre la evidencia obtenida, esto implica poseer los criterios apropiados y necesarios para que dicha opinión sea coherente con la evidencia, la cual en muchas ocasiones, depende de los registros lo cuales implican ser procesados en algún tipo de sistema que posee la entidad.

1.5.10.5 EVIDENCIA DE AUDITORÍA-CONSIDERACIONES ADICIONALES PARA PARTIDAS ESPECÍFICAS (NIA 501)

"El propósito de esta Norma Internacional de Auditoría (NIA) es establecer normas y proporcionar lineamientos adicionalmente a lo contenido en NIA 500,

Evidencia de auditoría, con respecto a ciertos saldos de cuenta específicos de los estados financieros y a otras revelaciones"

Partiendo del hecho que para demostrar que a existido algún tipo de fraude o error en algún procedimiento tiene que ser demostrado mediante la evidencia, la cual en muchas ocasiones solamente se posee de forma magnética, (automatizada), de tal manera que debe poseer el grado de fiabilidad sobre las aseveraciones que el auditor realiza.

1.5.10.6 MUESTREO DE LA AUDITORÍA Y OTROS MEDIOS DE PRUEBAS.(NIA 530)

Bajo el criterio que la auditoría no es sobre un 100% de los registros, existen medios de pruebas, sobre los que se debe basar éste trabajo, esto implica conocer básicamente las necesidades de la entidad y los posibles riesgos inherentes que se mantiene la entidad, en tal sentido "el propósito de esta Norma Internacional de Auditoría (NIA) es establecer normas y proporcionar lineamientos, sobre el uso de procedimientos de muestreo en la auditoría y otros medios de selección de partidas para reunir evidencia en la auditoría". la muestra contribuye directamente al trabajo que se está realizando ya sea una auditoría de estados financieros u otro tipo de auditoría.

1.5.10.7 USO DEL TRABAJO DE UN EXPERTO. (NIA 620)

El uso del trabajo de un experto implica conocer las necesidades que tiene la entidad sobre algún tipo de auditoría especializada.

"El propósito de esta Norma Internacional de Auditoria (NIA) es establecer normas y proporcionar lineamientos sobre el uso del trabajo de un experto como evidencia de auditoría; cuando use el trabajo desempeñado por un experto, el auditor deberá obtener suficiente evidencia apropiada de auditoría de que dicho trabajo es adecuado para los fines de la auditoría", se trata de mantener la coherencia con lo revisado versus la evidencia, la cual se obtendrá mediante el trabajo de un experto cuando el auditor no posea los conocimientos necesarios y suficientes para cumplir dicho propósito.

Se debe tomar muy en cuenta, que para la realización del trabajo del auditor existen también lineamientos de Éticas como los emitidos por el IFAC "Código de ética para Contadores profesionales".

También se relaciona la Norma Internacional de Control de Calidad (NICC) ISQC No 1

". El propósito de esta Norma Internacional en el Control de Calidad (NICC) es establecer normas y dar lineamientos respecto de las responsabilidades de una firma sobre su sistema del control de calidad para auditorías y revisiones de información financiera histórica, y para otros trabajos para atestiguar y sus servicios relacionados. Esta NICC debe leerse en forma conjunta con las partes A y B del Código de Ética para Contadores Profesionales de IFAC (el código de IFAC)"

CAPÍTULO II

2. METODOLOGÍA Y DIAGNÓSTICO DE LA INVESTIGACIÓN.

2.1. METODOLOGÍA DE LA INVESTIGACIÓN.

2.1.1. TIPO DE ESTUDIO.

El tipo de estudio que se realizó en la investigación, tuvo un enfoque hipotético deductivo, el cual es un instrumento para el desarrollo de investigaciones llamado también cuantitativo, debido a que permite descubrir y explicar determinadas situaciones a través de proposiciones hipotéticas generales, es decir, trata de estudiar la realidad a partir de información estadística.

En tal sentido, se llevó a cabo este tipo de estudio en los profesionales inscritos como personas naturales en el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoria al 31 de Diciembre de 2007. Con el propósito de determinar el grado de conocimiento del Contador Público en lo que corresponde a efectuar una Planeación de Auditoría Estratégica a los Sistemas de Información que permita asegurar la confiabilidad de los Estados Financieros

2.1.2. UNIDADES DE ANÁLISIS.

Las unidades de análisis en las que se enfocó la investigación fueron todos los profesionales inscritos como personas naturales en el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría al 31 de Diciembre de 2007

2.1.3. POBLACIÓN Y MUESTRA.

a) Población.

De acuerdo a criterios estadísticos, la población que se estudió fue finita y para determinar la muestra se utilizó el muestreo aleatorio simple, debido a que la probabilidad que cada unidad muestral sea elegida es la misma, ya que hay probabilidad equitativa.

b) Muestra.

El tamaño de la muestra, en este caso, se determinó por la siguiente fórmula que corresponde a universos finitos

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

Donde:

n= Tamaño de la muestra

Z= Nivel de confianza de la muestra = 1.96

P= Proporción de la población que cumple con el atributo investigado, debido a no contar con un parámetro previo se utilizara el criterio conservador (P=0.80), con tales valores se esta asumiendo la máxima variabilidad.

Q= proporción de la población que no cumple el atributo investigado, obtenido por diferencia. (Q=1-P). Q=0.20

$e =$ Precisión de la muestra, este valor es determinado por el juicio del investigador e implica el grado de error en la estimación a realizar, para efectos de la investigación se utilizó un error de 15%.

APLICACIÓN DE LA FÓRMULA.

DATOS:

N=3312	Z=1.96	e=0.10
Q=0.20	P=0.80	n=?

Sustituyendo en la fórmula se obtiene el siguiente resultado:

$$n = \frac{(1.96)^2.(0.80).(0.20)(3312)}{(3312-\ )\ (0.10)^2 + 1.96)^2.(0.80)(0.20)}$$

$$n = \frac{2,035.74}{33.72}$$

$n = 60.36 \approx 60$ Profesionales de la Contaduría Pública

2.1.4. MÉTODOS E INSTRUMENTOS DE RECOLECCIÓN DE LA INFORMACIÓN.

a) Investigación Bibliográfica.

Para el desarrollo de este trabajo se utilizaron libros, tesis, revistas, sitios web, leyes generales y específicas, normativa técnica y otra información relacionada a la Auditoría Estratégica a los Sistemas de Información.

b) Investigación de Campo.

Para efectuar el diagnóstico de la investigación se utilizó el cuestionario como instrumento de recolección de información, el cual incluyó preguntas breves y comprensibles a fin de comprobar la información obtenida, éste se dirigió a los profesionales inscritos como personas naturales en el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría al 31 de Diciembre de 2007

2.1.5. TABULACIÓN Y ANÁLISIS DE LA INFORMACIÓN.

Toda la información obtenida a través de los cuestionarios, fue tabulada y procesada en cuadros estadísticos generados en Microsoft Office Excel, el cual facilitó el procesamiento de datos cuantitativos, por medio de la distribución de frecuencias absolutas y relativas de cada pregunta del cuestionario, la cual se presentó en gráficos estadísticos de pastel para efecto de interpretar y analizar los resultados.

Se analizó individualmente cada pregunta del cuestionario, observándose si se logró el objetivo trazado para cada una de ellas y posteriormente se interpretaron los resultados obtenidos en el procesamiento de la información.

2.2. DIAGNÓSTICO DE LA INVESTIGACIÓN.

Considerando los resultados obtenidos en la investigación de campo, el diagnóstico se dividió, para efecto de un mejor análisis, en cuatro áreas de interés con el fin de dar solución al sistema de hipótesis diseñado, las cuales se definen a continuación:

a) Seguridad que los Sistemas de Información proporcionan a las compañías, para la información de sus Estados Financieros.(Ver cuadro Nº 1).

b) Conocimiento que el Contador Público posee en la Auditoría estratégica a los Sistemas de Información, la cual está directamente relacionada con la Auditoría Financiera.(Ver cuadro Nº 2).

c) Capacitación que el Contador Público ha recibido frente a las demandas del medio con relación a las Tecnologías de la Información y Comunicación (TIC).(Ver cuadro Nº 3).

d) Medidas que el auditor implementa al auditar considerando los riesgos de auditoría y aplicación técnica de nuevos conocimientos en el ejercicio profesional de la Contaduría Pública y Auditoria.(Ver cuadro Nº 4).

2.2.1 SEGURIDAD QUE LOS SISTEMAS DE INFORMACIÓN PROPORCIONAN A LAS COMPAÑÍAS, PARA LA INFORMACIÓN DE SUS ESTADOS FINANCIEROS

De acuerdo al cuadro número uno se presenta el grado de experiencia, que el contador público tiene en el ejercicio de las áreas de su competencia de la profesión; por lo que en la mayoría de los casos, esta experiencia se desarrolla en las áreas de: Contabilidad, auditoría externa y auditoría interna; sin embargo en la auditoría de sistemas de información, es evidente analizar el poco tiempo del ejercicio de su profesión en ésta área ya que el 83.33% manifiestan no haber efectuado ningún tipo de esta auditoría.

Consecuentemente al criterio anterior los contadores públicos que consideran que los lineamientos para asegurar la confiabilidad de los estados financieros no son suficientes representa el 56.67%, lo cual indica que el profesional está consiente que es necesario un tipo de auditoría que prevenga de forma estratégica de forma inherente al riesgo informático y a la información financiera, según la pregunta cinco del cuadro número uno las razones por las cuales las empresas tienen la necesidad para realizar una auditoría a los sistemas de información son:

a) Por la seguridad de los programas (20.00% de la muestra).

b) Garantizar las bases de datos (63.33% de la muestra).

c) Prevención de fraudes (10.00%).

Sin embargo los contadores públicos consideran que los seguros al software y al hardware no son suficientes, para el resguardo de la información, lo cual indica un riesgo latente e inherente a los sistemas de información y que en opinión de los encuestados representa el 73.33%.

Los planes estratégicos de seguridad que se deben aplicar a los sistemas de información en caso de desastres según los encuestados tienen que ser en función de los planes de contingencia de las empresas y significativamente ésta le corresponde el 56.67%, de los encuestados, sin embargo los profesionales encuestados manifiestan que otra medida emergente para la focalización de las áreas prioritarias es decir aquellas que le indican mayor riesgo la cual representa para la empresa áreas críticas de pérdida de información y de acuerdo a la investigación ésta representa un 30.00% de la muestra.

Según la pregunta 10 del cuadro número uno se puede analizar que entre las medidas de seguridad, más importantes para el resguardo de la información que el contador público considera está enfocada al control interno de las siguientes áreas: Hardware, software, operación, seguridad de datos, implementación de sistemas y administrativos que conllevan a la protección física y lógica del activo informático de datos.

CUADRO No.1
SEGURIDAD QUE LOS SISTEMAS DE INFORMACIÓN PROPORCIONAN A LAS COMPAÑÍAS, PARA LA INFORMACIÓN DE SUS ESTADOS FINANCIEROS

No. PREG.	CRITERIOS	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
1	Experiencia que Posee el contador Público en las áreas de:		
	➢ Contabilidad	(14)16-20A	23.33%
	➢ Auditoria Interna	(32)cero A	53.33%
	➢ Auditoria Externa	(28)1-10 A	46.66%
	➢ Auditoría de Sistemas Informáticos	(50)cero A	83.33%

CUADRO No.1
SEGURIDAD QUE LOS SISTEMAS DE INFORMACIÓN PROPORCIONAN A LAS COMPAÑÍAS, PARA LA INFORMACIÓN DE SUS ESTADOS FINANCIEROS

4	Criterio que posee el Contador Público encuestado que no hay lineamientos sufrientes para asegurar la confiabilidad de los Estados Financieros de las entidades que utilizan sistemas de información	34	56.67%
5	Razón por la cual las empresas se ven en la necesidad de realizar algún tipo de auditoría a los Sistemas de Información		
	➢ Seguridad de los Programas	12.	20.00%
	➢ Garantizar las bases de datos	38	63.33%
	➢ Evitar fraudes	6	10.00%
8	Contador Público encuestado que consideran que los seguros al software y al hardware para el resguardo de la información financiera en caso de desastres no son sufrientes	44	73.33%
9	Planes estratégicos de seguridad que se deben aplicar a los Sistemas de Información en caso de desastres Según la opinión del Contador Público encuestado:		
	➢ Planes de Contingencia que contemplen simulacros de desastres	34	56.67%
	➢ Focalizar áreas prioritarias	18	30.00%

CUADRO No.1
SEGURIDAD QUE LOS SISTEMAS DE INFORMACIÓN PROPORCIONAN A LAS COMPAÑÍAS, PARA LA INFORMACIÓN DE SUS ESTADOS FINANCIEROS

10	Medidas de seguridad que considera el Contador Público importantes para el resguardo de la información financiera de los Sistemas de Información		
	Controles al hardware Controles al Software Controles de operación Controles de seguridad de datos Controles de Implementación Controles Administrativos Todos los anteriores	42	70.00%

2.2.2 CONOCIMIENTO QUE EL CONTADOR PÚBLICO POSEE EN LA AUDITORÍA ESTRATÉGICA A LOS SISTEMASDE INFORMACIÓN, LA CUAL ESTÁ DIRECTAMENTE RELACIONADA CON LA AUDITORÍA FINANCIERA

Con respecto al conocimiento que el contador público tiene en la auditoría estratégica a los sistemas de información; en el cuadro número dos se puede analizar los siguientes aspectos.

De acuerdo a la investigación de campo se puede determinar que las área de aplicación de la auditoría que tienen mayor énfasis son: el área financiera con un 96.67% de los encuestados, auditoría interna con un 83.33%, fiscal con un 80.00%, gubernamental y administrativa con un 63.33%. sin embargo es evidente que el ejercicio profesional de la auditoría estratégica aplicado, es limitado, ya que solamente representa el 6.67% de la muestra.

Según la pregunta tres del cuadro numero dos se analiza que el contador público que posee conocimientos acerca de cómo realizar una auditoría de sistemas es muy reducido ya que esta representa EL 26.67% es decir 16 encuestados de una muestra de 60.

Consecuentemente con la aseveración anterior, en la pregunta número once del cuadro Nº 2 se muestra la razón del sentido de la investigación de campo acerca de la auditoría estratégica donde se puede indagar el conocimiento que el profesional de la contaduría pública tiene en esta área de aplicación es mínimo pues solo representa el 26.67% es decir 16 de 60 encuestados.

Sin embargo en la pregunta número 6 del cuadro Nº 2 de acuerdo a los resultados de la investigación el 70.00% de la muestra posen conocimiento acerca de la seguridad informática, sin embargo no sabe como enfrentar éstos retos mediante la técnica de la auditoría estratégica.

En la pregunta Nº 13 se muestra el grado de adiestramiento que el contador público posee en el ejercicio de la auditoría de los sistemas de información, el cual de forma muy limitada representa el 30% de los encuestados, es decir 18 unidades muestrales han efectuado algún tipo de auditoría de esta magnitud.

En lo relativo a las consideraciones que el contador público tiene acerca de la utilidad de la auditoría estratégica a los sistemas de información 50 unidades muestrales que representa el 83.33% de la muestra manifiestan que éste tipo de auditoría es necesaria debido a que las compañías deben tener un plan estratégico a los sistemas de información que les permita salvaguardar sus activos tecnológicos (pregunta 17 cuadro Nº 2).

Con relación a lo anterior los contadores públicos encuestados en un 91.67% manifiestan que es necesario la creación de un modelo de planeación de auditoría estratégica a los sistemas de información, el cual les puede servir como guía o parámetro para implementarlo en las compañías de acuerdo a sus necesidades y requerimientos de la información de los usuarios del software y del hardware y muy esencialmente del Procesamiento Electrónico de Datos (PED).

CUADRO No.2
CONOCIMIENTO QUE EL CONTADOR PÚBLICO POSEE EN LA AUDITORÍA ESTRATÉGICA A LOS SISTEMAS DE INFORMACIÓN, LA CUAL ESTÁ DIRECTAMENTE RELACIONADA CON LA AUDITORÍA FINANCIERA

No. PREG.	CRITERIOS	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
2	Clases de Auditoría que conoce el Contador Público encuestado		
	➢ Financiera	58	96.67%
	➢ Interna	50	83.33%
	➢ De Sistemas	28	46.67%
	➢ Fiscal	48	80.00%
	➢ Administrativas	38	63.33%
	➢ Gubernamental	38	63.33%
	➢ Ambiental	16	26.67%
	➢ Forense	22	36.67%
	➢ De gestión	34	56.67%
	➢ Estratégica	4	6.67%
3	Conocimiento que posee el contador Público encuestado sobre lineamientos para realizar una auditoría a los Sistemas de Información	16	26.67%
6	Conocimiento que posee el contador Público encuestado acerca de la Seguridad Informática	42	70.00%
11	Conocimiento que posee el Contador Público encuestado para desarrollar un plan de auditoría estratégica a los sistemas de información:	16	26.67%
13	Adiestramiento que posee al contador Público Sobre la Auditoría a los Sistemas de Información	18	30.00%

CUADRO No.2
CONOCIMIENTO QUE EL CONTADOR PÚBLICO POSEE EN LA AUDITORÍA ESTRATÉGICA A LOS SISTEMAS DE INFORMACIÓN, LA CUAL ESTÁ DIRECTAMENTE RELACIONADA CON LA AUDITORÍA FINANCIERA

17	Consideración del Contador Público encuestado sobre la utilidad de implementar una auditoría estratégica a las empresas.	50	83.33%
21	Contadores Públicos que consideran necesario la creación de un Modelo de planeación de una auditoría Estratégica a los Sistemas de Información que sirva de parámetro para implementarlo en las empresas	55	91.67%

2.2.3 CAPACITACIÓN QUE EL CONTADOR PÚBLICO HA RECIBIDO FRENTE A LAS DEMANDAS DEL MEDIO CON RELACIÓN A LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC)

Con respecto a la capacitación que el profesional ha adquirido en ésta área es muy limitada ya que, no representa ni siquiera el 50.00% de la muestra, sin embargo, las unidades muestrales manifiestan que la forma que han adquirido los conocimientos en ésta área ha sido a través de su ejercicio profesional 40.00%; cabe mencionar que debido a los costos y al tiempo incurrido en los procesos de capacitación los contadores públicos que han recibido adiestramiento en los últimos seis meses solamente son el 10.00% de la muestra es decir seis contadores públicos de 60 encuestados.

Por otra parte, un contador público manifiesta que los conocimientos en el área de su profesión son necesarios debido a la constante demanda que el medio globalizado le impone; de igual forma el constante cambio que la tecnología de la información requiere de éste (96.67% de la muestra).

Por otra parte los profesionales de la contaduría pública manifiestan que los gremios profesionales deben comprometerse a realizar capacitaciones y especializaciones de acuerdo a la demanda del conocimiento y servicio que el contador público debe ofrecer en el ejercicio de su profesión.

CUADRO No.3
CAPACITACIÓN QUE EL CONTADOR PÚBLICO HA RECIBIDO FRENTE A LAS DEMANDAS DEL MEDIO CON RELACIÓN A LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC)

No. PREG.	CRITERIOS	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
12	Medios por los que el Contador público encuestado ha adquirido conocimientos sobre un plan de auditoría estratégica a los Sistemas de información:		
	Capacitaciones	26	43.33%
	En el Ejercicio Profesional	24	40.00%
15	Capacitaciones recientes que haya recibido el contador público encuestado relacionadas con las TIC, que contribuya a ampliar los conocimientos para realizar un plan de auditoría estratégica a los Sistemas de Información	6	10.00%
16	Consideración del contador Público encuestado sobre la actualización de los conocimientos constantes de acuerdo a las demandas del medio y los avances de las TIC	58	96.67%
20	Difusión que consideran los profesionales de la contaduría Pública que realizan los gremios de profesionales sobre nuevos conocimientos de la profesión.	42	70.00%

2.2.4 MEDIDAS QUE EL AUDITOR IMPLEMENTA AL AUDITAR CONSIDERANDO LOS RIESGOS DE AUDITORÍA Y APLICACIÓN TÉCNICA DE NUEVOS CONOCIMIENTOS EN EL EJERCICIO PROFESIONAL DE LA CONTADURÍA PÚBLICA Y AUDITORIA

El profesional de la contaduría pública considera que es necesario implementar auditorías que consideren los riesgos inherentes a la tecnología de la información; por ende es necesario definir, ejecutar y supervisar controles preventivos que permitan asegurarse que la información presentada en los estados financieros posean mínimo de errores importantes, en lo relativo a la seguridad lógica de los sistemas de información, criterio que es sustentado por 38 contadores públicos de una muestra de 60.

En función de lo anterior los contadores públicos entrevistados manifestaron que es necesario implementar medidas estratégicas de control a la información generada partiendo de la premisa que la mayoría de compañías poseen un sistema de información estándar o a la medida para controlar sus operaciones básicas criterio que es sustentado por 70.00% de la muestra.

En conclusión los cambios constantes de la tecnología de la información, la creciente demanda por los servicios especializados, el posicionamiento de las empresas, así como la internacionalización y creciente aumento de servicios contables, entre otros relacionados; condicionan al contador público a especializarse en áreas afines y conexas a las finanzas; de tal manera que le permita incrementar su portafolio de servicios, por ende su cartera de clientes

Asimismo las compañías que utilicen sistemas de información son consientes de los constantes cambios que estos sufren a diario debido a la misma demanda del mercado existente; por lo tanto es determinante que sus operaciones sean resguardadas de forma efectiva a través de los procedimientos de la auditoría estratégica a los sistemas de información con apoyo directo de las tecnologías de la información.

CUADRO No.4
MEDIDAS QUE EL AUDITOR IMPLEMENTA AL AUDITAR CONSIDERANDO LOS RIESGOS DE AUDITORÍA Y APLICACIÓN TÉCNICA DE NUEVOS CONOCIMIENTOS EN EL EJERCICIO PROFESIONAL DE LA CONTADURÍA PÚBLICA Y AUDITORIA

No. PREG.	CRITERIOS	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
18	Tipos de medidas que el Contador Público implementa al realizar una auditoría considerando los riesgos existentes en el uso de Tecnologías de Información y Comunicación Controles Preventivos	38	63.33%
19	Contadores Públicos encuestado que consideran que las medidas implementadas actualmente son suficientes para el desarrollo de las auditorías; partiendo del hecho que la mayoría de entidades utilizan Sistemas de Información para el proceso de la información	18	30.00%

CAPITULO III

3. MODELO DE PLANEACIÓN DE UNA AUDITORÍA ESTRATÉGICA A LOS SISTEMAS DE INFORMACIÓN COMO UNA RESPUESTA A LA CONFIABILIDAD DE LOS ESTADOS FINANCIEROS PREPARADOS EN UN AMBIENTE INFORMÁTICO.

En este Capítulo se propone al gremio de Contadores Públicos inscritos en el Consejo de Vigilancia de la Profesión de la Contaduría Publica y Auditoría un modelo de planeación de una auditoría estratégica basada en los sistemas de información

3.1. SITUACIÓN ACTUAL DE LOS PROFESIONALES DE CONTADURÍA PÚBLICA.

3.1.1. PLANEACIÓN DE AUDITORÍA ESTRATÉGICA A LOS SISTEMAS DE INFORMACIÓN

Los profesionales de la Contaduría Pública que ejercen su trabajo en el área de la auditoría en El Salvador, han centrado mayor atención a la auditoría de Estados Financieros y auditoría Fiscal, prestando poca atención a las auditorías especializadas, cabe mencionar que no se a prestado importancia a la planeación de una auditoría estratégica a los sistemas de información;

3.1.2. CONOCIMIENTO DE LA AUDITORÍA ESTRATÉGICA.

Para realizar adecuadamente el trabajo que se encomienda a los profesionales de la contaduría pública, en el área de auditoría, es imprescindible poseer los conocimientos básicos en las ramas especializadas. Considerando que la mayoría de profesionales no posee una especialización sobre áreas específicas como es el caso de la planeación de una auditoría estratégica a los sistemas de información y que es importante estar a la vanguardia de los conocimientos mínimos tanto de las nuevas tendencias de auditoría, así como de los avances tecnológicos; en tal sentido se considera importante la creación de un modelo de auditoría estratégica a los sistemas de información que contribuya a ampliar los conocimientos de los profesionales de la Contaduría Pública.

3.2 MODELO DE PLANEACIÓN DE UNA AUDITORÍA ESTRATÉGICA A LOS SISTEMAS DE INFORMACIÓN

Con la finalidad de que todo profesional sea competente para satisfacer las demandas del medio, se hace necesaria la creación de un modelo de planeación de una auditoría estratégica a los sistemas de información que contribuya a ampliar los conocimientos de éste

A continuación se presenta el desarrollo de planeación de una auditoría estratégica a los sistemas de información.

3.2.1 MEMORANDUM DE PLANEACIÓN (NIA 300,315; NAS S5, Guía de Auditoría de SI G15)

COMPONENTES DEL MEMORANDUM:

1. COMPROMISOS COMO FIRMA

1.1 OBJETIVO GENERAL (NAS S5 P'3)

Realizar una revisión y evaluación estratégica de: los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia, eficacia y seguridad, del Gobierno Corporativo (GC), de la estructura organizativa que participan en el procesamiento de la información, Recursos Humanos, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

1.2 OBJETIVOS ESPECÍFICOS

- Confirmar que el Gobierno Corporativo funciona de forma adecuada, conforme a los lineamientos y políticas estratégicas de dicho comité
- Verificar que la estructura administrativa ha determinado los proyectos de forma estratégica de tal manera que se determine su viabilidad
- Evaluar la estrategia del Procesamiento Electrónico de Datos (PED)
- Evaluar las políticas estratégicas al Ciclo de Vida de los Sistemas (CDVDS)
- Evaluar de forma estratégica, el diseño y prueba de los sistemas del área de Informática.

- Evaluar de forma estratégica la utilización del sistema de acuerdo a las especificaciones establecidas de los usuarios.
- Determinar de forma estratégica la veracidad de la información del área de Informática.
- Evaluar los procedimientos estratégicos de control de operación, analizar su estandarización y evaluar el cumplimiento de los mismos.
- Evaluar la forma estratégica como se administran los dispositivos de almacenamiento básico del área de Informática.
- Evaluar de manera estratégica el control que se tiene sobre el mantenimiento y las fallas de los equipos de Cómputo
- Verificar de manera estratégica las disposiciones y reglamentos que coadyuven al mantenimiento del orden dentro del departamento de cómputo

1.3 ALCANCE (NIA 300 P 8,9; NAS S5 P 6)

Se hará un estudio y evaluación estratégico a los sistemas de información de la empresa (Nombre de la empresa) para determinar los proyectos que se poseen en ésta área además se verificarán los sistemas de información existentes para determinar si el funcionamiento del mismo es adecuado y cubre las necesidades o requerimientos de los usuario primario y secundarios; para el período (anotar el periodo), con base a las pruebas que se determinen necesarias para establecer el adecuado funcionamiento y emitir una opinión sobre el mismo.

El alcance comprende:

1. Evaluación de la Dirección de Informática en lo que corresponde a:
   - Capacitación estratégicas
   - Planes Estratégicos de de trabajo
   - Controles
   - Estándares
2. Evaluación estratégica de los Sistemas
   a. Evaluación de los diferentes sistemas en operación (flujo de información, procedimientos, documentación, redundancia, organización de archivos, estándares de programación, controles, utilización de los sistemas)
   b. Evaluación del avance de los sistemas en desarrollo y congruencia con el diseño general
   c. Evaluación de prioridades y recursos asignados (humanos y equipos de cómputo)

d. Seguridad física y lógica de los sistemas, su confidencialidad y respaldos

3. Evaluación de los equipos

- Capacidades
- Utilización
- Nuevos Proyectos
- Seguridad física y lógica
- Evaluación física y lógica

4. Metodología

La metodología de investigación a utilizar en el proyecto se presenta a continuación:

a. Para la evaluación de la Dirección de Informática se llevarán a cabo las siguientes actividades:

- Solicitud de los estándares utilizados y programa de trabajo
- Aplicación del cuestionario al personal
- Análisis y evaluación de la información
- Elaboración del informe

b. Para la evaluación de los sistemas tanto en operación como en desarrollo se llevarán a cabo las siguientes actividades:

- Solicitud del análisis y diseño de los sistemas en desarrollo y en operación
- Solicitud de la documentación de los sistemas en operación (manuales técnicos, de operación del usuario, diseño de archivos y programas)
- Recopilación y análisis de los procedimientos administrativos de cada sistema (flujo de información, formatos, reportes y consultas)
- Análisis de llaves, redundancia, control, seguridad, confidencial y respaldos
- Análisis del avance de los proyectos en desarrollo, prioridades y personal asignado
- Entrevista con los usuarios de los sistemas
- Evaluación Estratégica directa de la información obtenida contra las necesidades y requerimientos del usuario
- Análisis objetivo de la estructuración y flujo de los programas
- Análisis y evaluación de la información recopilada
- Elaboración del informe

c. Para la evaluación estratégica de los equipos se llevarán a cabo las siguientes actividades:

- Solicitud de los estudios de viabilidad y características de los equipos actuales, proyectos sobre ampliación de equipo, su actualización
- Solicitud de contratos de compra y mantenimientos de equipo y sistemas
- Solicitud de contratos y convenios de respaldo
- Solicitud de contratos de Seguros
- Elaboración de un cuestionario sobre la utilización de equipos, memoria, archivos, unidades de entrada/salida, equipos periféricos y su seguridad
- Visita técnica de comprobación de seguridad física y lógica de la instalaciones de la Dirección de Informática
- Evaluación técnica del sistema electrónico y ambiental de los equipos y del local utilizado
- Evaluación de la información recopilada, obtención de gráficas, porcentaje de utilización de los equipos y su justificación

d. Elaboración y presentación del informe final (conclusiones y recomendaciones)

2. CONOCIMIENTO DE LA ENTIDAD (NIA 315)

2.1 NATURALEZA (NIA 315 P. 25)

Anotar el nombre de la empresa, la naturaleza, a que se dedica, donde ejerce la actividad comercial, entre otros relacionados.

2.2 ESTRUCTURA LEGAL (NIA 315 P 25-27)

Accionistas y su porcentaje de participación.

En este apartado se anotará la estructura organizativa comenzando desde la alta gerencia hasta el último nivel jerárquico (de los accionistas)

2.3 FECHA DE FUNDACION

Anotar la fecha de fundación de la entidad

2.4 ACTIVIDAD ECONOMICA PRINCIPAL (NIA 315 P 25)

Anotar la actividad económica principal

2.5 OTRAS ACTIVIDADES PRODUCTIVAS

Anotar las actividades secundarias a las que se dedica la entidad o las que proyecta dedicarse en el corto plazo.

2.6 MONTO DEL CAPITAL SOCIAL (NIA 315 P 26)

Anotar el monto del capital social, (especificar si todo está totalmente pagado o existe parte adeudada por parte de los accionistas), anotar además las participaciones de cada uno de los accionistas:

3. INFORMACION DEL AREA DE SISTEMAS

3.1 ESTRUCTURA ORGANIZATIVA (NIA 315

Solicitar el organigrama de la estructura organizativa de la empresa y anotarlo en este apartado, comenzando desde la alta gerencia hasta el último nivel orgánico.(toda la organización)

3.2 FUNCIONES Y UBICACION GEOGRÁFICA

Anotar las funciones y dependencias de cada uno de los miembros de la estructura organizativa, detallando la ubicación geográfica de estos de forma específica.
En este apartado nos interesa conocer de qué departamento depende el área de informática (o de sistema)

3.3 CANTIDAD DE EMPLEADOS

Anotar la cantidad de empleados con que cuenta el área de sistemas, anotando cada uno de los nombres y especificando su función principal.

3.4 SERVICIOS PRESTADOS

Anotar cada uno de los servicios que prestan los encargados del área de sistemas, especificando los principales reportes que éstos emiten

3.5 DEPENDENCIAS RELACIONADAS

3.5.1 RELACIÓN EL DEPARTAMENTO DE INFORMÁTICA CON GERENCIA

Anotar la relación que existe del departamento de informática con la gerencia

3.5.2 RELACIÓN DEL DEPARTAMENTO DE INFORMÁTICA CON EL DEPARTAMENTO DE AUDITORÍA INTERNA.

Anotar la relación que existe con el departamento de auditoría interna.

3.5.3 RELACIÓN DEL DEPARTAMENTO DE INFORMÁTICA CON AUDITORÍA DE SISTEMAS

Anotar la relación que existe con el departamento de auditoría informática (si la entidad cuenta con dicho departamento)

4. INVESTIGACIÓN PRELIMINAR (NIA 300 P6-7; NIA 315 P 20 y 21; NAS S5 P 3)

- ENTREVISTAS

Anotar cada una de las entrevistas realizadas

- NARRATIVAS

Anotar cada una de las narrativas empleadas

- CUESTIONARIOS

Anotar los cuestionarios que se diseñen para la evaluación preliminar

ENTRE OTRAS.

4.1 INVESTIGACIÓN PRELIMINAR

La primera etapa a evaluar en una auditoría Estratégica a los Sistemas de Información son los planes estratégicos que posee la compañía con relación a los sistemas de información

El plan estratégico deberá establecer los proyectos que se presentarán en un futuro tomando en cuenta la estrategia de desarrollo la cual deberá establecer las nuevas aplicaciones, recursos y la arquitectura en que estarán fundamentados; la consulta de los usuarios, el plan estratégico debe definir los requerimientos de información de la dependencia; por último, el plan estratégico determina la planeación de los recursos. Contestando preguntas como las siguientes:

EVALUACIÓN DE SISTEMAS

REF	PREGUNTA	SI	NO
	PLAN ESTRATÉGICO		
	¿Cuáles Proyectos se implementarán?		
	¿Cuándo se pondrán a disposición de los usuarios? ¿Qué características tendrán?		
	¿Cuántos recursos se requerirán para implantarlos?		
	¿Qué tipo de proyectos serán desarrolladas y cuando?		
	¿Qué tipo de recursos se utilizarán para éste fin y cuando?		
	¿Cómo serán utilizados estos recursos y Cuando?		
	¿Afectarán los recursos actuales del hardware y software?		
	¿Qué tipo de tecnología será utilizada y cuando se implementará?		
	¿Cuántos recursos se requerirán aproximadamente? ¿Cuál es aproximadamente el monto de la inversión en hardware y software que se tiene previsto invertir?		
	¿Contempla el plan estratégico las ventajas de los nuevos proyectos en tecnología?		
	Consulta a los usuarios		
	¿Qué estudios van a ser realizados al respecto?		
	¿Qué metodología se utilizará para dichos estudios?		
	¿Quién administrará y realizará dichos estudios?		
	¿Cuál es la inversión requerida en servicios, desarrollo y consulta a los usuarios?		

EVALUACIÓN DEL DISEÑO LÓGICO DEL SISTEMA

En esta etapa se deberán analizar las especificaciones del sistema considerando las situaciones estratégicas que lo afectan:

Los puntos a evaluar son:

- Entradas (captura).
- Salidas.
- Procesos.
- Especificaciones de datos.
- Especificaciones de proceso.
- Métodos de acceso.
- Operaciones.
- Manipulación de datos (antes, durante y después del proceso electrónico de datos).
- Proceso lógico necesario para producir informes.
- Identificación de archivos, tamaño de los campos y registros.
- Proceso en línea o lote y su justificación.
- Frecuencia y volúmenes de operación.
- Sistemas de seguridad.
- Sistemas de control.
- Responsables.
- Número de usuarios.

Dentro del estudio de los sistemas en uso se deberá solicitar:

- Manual del usuario.
- Descripción de flujo de información y/o procesos.

Descripción y distribución de información. [32]

- Manual de formas
- Manual de reportes.
- Lista de archivos y especificaciones

[32] "Management of Advanced Technology in Elections", Harry Neufeld, Management Consultant, Canada. (Del boletín Desarrollo de una Estrategia I**ntegral de Tecnología Informátic**a)

EVALUACIÓN DEL DISEÑO LÓGICO DE LOS SISTEMAS

REF.	PREGUNTA	SI	NO
	Lo que se debe determinar en el sistema: En el procedimiento: • ¿Quién hace, cuando y como? • ¿Qué formas estratégicas se utilizan en el sistema? • ¿Son necesarias, se usan, están duplicadas? • ¿El número de copias es el adecuado? • ¿Existen puntos estratégicos de control o faltan? En la gráfica de flujo de información: • ¿Es fácil de usar? • ¿Es lógica? • ¿Se encontraron vacíos que afecten los planes estratégicos? • ¿Hay faltas de control Estratégico? En el diseño: • ¿Cómo se usarán la herramienta de diseño si existe? • ¿Qué también se ajusta la herramienta al procedimiento?		

[33]

EVALUANDO DEL DISEÑO LÓGICO DE OPERACION

En esta etapa del sistema se deberán auditar de manera estratégica los programas, su diseño, el leguaje utilizado, interconexión entre los programas y características del hardware empleado (total o parcial) para el desarrollo del sistema.

[33] "Management of Advanced Technology in Elections", Harry Neufeld, Management Consultant, Canada. (Del boletín Desarrollo de una Estrategia I**ntegral de Tecnología Informátic**a)

EVALUANDO DEL DISEÑO LÓGICO DE OPERACIÓN

REF	PREGUNTA	SI	NO
	¿Se posee un diagrama de flujo por cada programa? ¿Existe un diagrama particular de entrada/salida? ¿Cuenta el sistema con mensajes y su explicación? ¿Están bien definidos los parámetros y su explicación? ¿Se posee diseño de impresión de resultados? ¿Se pueden administrar cifras de control? ¿El sistema cuenta con fórmulas de verificación? ¿Los programadores tienen acceso a los programas en operación? ¿Cuentan con instrucciones en caso de error? ¿Se preveen los errores de manera estratégica, de tal manera que se solucionen al instante que ocurren? ¿Se cuenta con un calendario de proceso y resultados?		

34

[34] "Management of Advanced Technology in Elections", Harry Neufeld, Management Consultant, Canada. (Del boletín Desarrollo de una Estrategia I**ntegral de Tecnología Informátic**a)

CONTROL DE PROYECTOS ESTRATÉGICOS DE TECNOLOGÍA INFORMATICA

El control de proyectos estratégicos de tecnología informática, va encaminado a verificar irregularidades que se puedan dar sobre aquellos proyectos que se pretenden implementar.

Para un adecuado control de proyectos es importante que se utilice la técnica de administración por cada uno de los proyectos, se considera lo siguiente:

CONTROL DE PROYECTOS ESTRATÉGICOS DE TECNOLOGÍA INFORMATICA

REF	PREGUNTA	SI	NO
	1. ¿Existe una lista de proyectos estratégicos de sistemas informáticos y de procedimiento de información y fechas programadas de implantación que puedan ser considerados como plan estratégico? 2. ¿Está relacionado el plan estratégico con un plan general de desarrollo de la dependencia? 3. ¿Ofrece el plan estratégico la atención de solicitudes urgentes de los usuarios? 4. ¿Asigna el plan estratégico un porcentaje del tiempo total de producción al reproceso o fallas de equipo? 5. Escribir la lista de proyectos a corto plazo y largo plazo 6. Escribir una lista de sistemas en proceso periodicidad y usuarios 7 .¿Quién autoriza los proyectos? 8. ¿Cómo se asignan los recursos? 9. ¿Cómo se estiman los tiempos de duración? 10. ¿Quién interviene en la planeación de los proyectos? 11. ¿Cómo se calcula el presupuesto del proyecto? 12. ¿Qué técnicas se usan en el control de los proyectos? 13. ¿Quién asigna las prioridades? 14. ¿Cómo se asignan las prioridades? **Pasa**		

CONTROL DE PROYECTOS ESTRATÉGICOS DE TECNOLOGÍA INFORMATICA

REF	PREGUNTA	SI	NO
	Viene 15 ¿Cómo se controla el avance del proyecto? 16. ¿Con qué periodicidad se controla el reporte del avance del proyecto? 17. ¿Cómo se estima el rendimiento del personal? 18. ¿Con qué frecuencia se estiman los costos del proyecto para compararlo con lo presupuestado? 19. ¿Qué acciones correctivas se toman en caso de desviaciones? 20. ¿Qué pasos y técnicas siguen en la planeación y control de proyectos enumérelos secuencialmente?: ( ) Documentación de la investigación ( ) Evaluación de la factibilidad de los sistema ( ) Análisis y valuación de propuestas ( ) Selección de equipos 21. ¿Se llevan a cabo revisiones periódicas de los sistemas para determinar si aún cumplen con los objetivos estratégicos para los cuales fueron diseñados? De análisis SÍ ( ) NO ( ) De programación SÍ ( ) NO ( ) Observaciones 22. Incluir el plazo estimado de acuerdo con los proyectos estratégicos que se tienen en que el departamento de informática podría satisfacer las necesidades de la dependencia, según la situación actual.		

35

[35] "Management of Advanced Technology in Elections", Harry Neufeld, Management Consultant, Canada. (Del boletín Desarrollo de una Estrategia I**ntegral de Tecnología Informátic**a)

CONTROL DE DISEÑO ETRATÉGICO DE SISTEMAS Y PROGRAMACIÓN

El objetivo es asegurarse de que el sistema funcione conforme a las especificaciones proyectadas, de tal manera que el usuario tenga la suficiente información para su manejo, operación y aceptación. Las revisiones se efectúan en forma paralela desde el análisis hasta la programación

DISEÑO DE SISTEMAS Y PROGRAMACION

REF.	PREGUNTA	SI	NO
	¿Quiénes intervienen al diseñar un sistema? ▪ Analista. ▪ Programadores. ▪ Operadores. ▪ Gerente de departamento. ▪ Auditores internos. ▪ Auditores externos ▪ Asesores. ▪ Otros ¿Se posee un plan estratégico para el diseño de los Sistemas Informáticos? ¿Qué tipo de planes estratégicos se posee? A corto plazo ( ) A largo Plazo ( ) ¿En qué tiempo se tiene programado ese tipo de plan? ¿Los analistas son también programadores? ¿Qué lenguaje o lenguajes conocen los analistas? ¿Cuántos analistas hay y qué experiencia tienen? ¿Qué lenguaje conocen los programadores? ¿Cómo se controla el trabajo de los analistas? ¿Cómo se controla el trabajo de los programadores? **Pasa**		

DISEÑO DE SISTEMAS Y PROGRAMACION

REF.	PREGUNTA	SI	NO
	Indique qué pasos siguen los programadores en el desarrollo de los proyectos programados: Estudio de la definición ( ) Discusión con el analista ( ) Diagrama de bloques ( ) Tabla de decisiones ( ) Prueba de escritorio ( ) Codificación ( ) ¿Es enviado a captura? ( ) ¿Los programadores capturan? ( ) ¿Quién los captura? Compilación ( ) Elaborar datos de prueba ( ) Solicitan datos al analista ( ) Correr programas con datos ( ) Revisión de resultados ( ) • Corrección del programa ( ) • Documentar el programa ( ) • Someter resultados de prueba ( ) • Entrega del programa ( ) ¿Qué documentación acompaña al programa cuando se entrega?		

EVALUACIÓN DEL ANÁLISIS ADMINISTRATIVO

En esta etapa se evaluarán si se cumple con los proyectos estratégicos requeridos por la administración; además se evalúa si se cumplen con las desmandas del los Sistemas de Información, las políticas, procedimientos y normas que se tienen para llevar a cabo el análisis.

La situación de una aplicación en dicho inventario puede ser alguna de las siguientes:

Planeada para ser desarrollada en el futuro.

En desarrollo.

En proceso, pero con modificaciones en desarrollo.

En proceso con problemas detectados.

En proceso sin problemas.

En proceso esporádicamente.

EVALUACIÓN DEL ANÁLISIS ADMINISTRATIVO

REF	PREGUNTA	SI	NO
	¿Se está ejecutando en forma correcta y eficiente el proceso de los proyectos estratégicos a los Sistemas de información? ¿Se han realizado algún tipo de estudio para la implementación de esos de proyectos? ¿Qué tipos de estudio se han realizado? ¿Son viables ese tipo de proyectos de acuerdo a los estudios? ¿Qué tan viables son esos proyectos? ¿Qué beneficios potenciales se esperan de cumplirse esos proyectos? ¿Son acordes a los programas de la administración? ¿Se ha considerado si cumplen con los requerimientos a los sistemas de información según la empresa? ¿Son acorde a los avances tecnológicos ese tipo de proyectos? ¿En qué tiempo pretende la empresa implementarlo? O ¿no pretende implementarlo? Si no pretende implementarlo. ¿se han considerado otros tipos de proyectos; de tal manera que se satisfagan las necesidades de la compañía y se mantenga de manera competitiva? ¿Se tiene propuesto un adecuado control y seguridad sobre los proyectos de sistema? ¿Está en el análisis la documentación adecuada?		

4.2 MATRICES Y ANÁLISIS DE LOS RIESGOS IDENTIFICADOS

En el siguiente cuadro se anotaran los resultados obtenidos de los métodos utilizados en la evaluación preliminar.

ÁREAS	R. INHERENTE	R. DE CONTROL	R. DE DETECCIÓN
CICLO DE VIDA DE LOS SISTEMAS (CDVS)	ALTO MEDIO BAJO LO MAS BAJO	ALTO MEDIO BAJO LO MAS BAJO	ALTO MEDIO BAJO LO MAS BAJO
GOBIERNO CORPORATIVO	ALTO MEDIO BAJO LO MAS BAJO	ALTO MEDIO BAJO LO MAS BAJO	ALTO MEDIO BAJO LO MAS BAJO
ESTRUCTURA ADMINISTRATIVA	ALTO MEDIO BAJO LO MAS BAJO	ALTO MEDIO BAJO LO MAS BAJO	ALTO MEDIO BAJO LO MAS BAJO
PED	ALTO MEDIO BAJO LO MAS BAJO	ALTO MEDIO BAJO LO MAS BAJO	ALTO MEDIO BAJO LO MAS BAJO
SEGURIDAD FISICA Y LOGICA	ALTO MEDIO BAJO LO MAS BAJO	ALTO MEDIO BAJO LO MAS BAJO	ALTO MEDIO BAJO LO MAS BAJO
SOFTWARE	ALTO MEDIO BAJO LO MAS BAJO	ALTO MEDIO BAJO LO MAS BAJO	ALTO MEDIO BAJO LO MAS BAJO
HARDWARE	ALTO MEDIO BAJO LO MAS BAJO	ALTO MEDIO BAJO LO MAS BAJO	ALTO MEDIO BAJO LO MAS BAJO

4.3 PRINCIPALES POLÍTICAS

4.3.1 POLÍTICAS ADMINISTRATIVAS

A. Controles Administrativos.

Anotar cada uno de los controles estratégicos que posee la administración, con todos los detalles que se especifican en las políticas

B. Evaluación del personal.

Anotar el tipo de evaluación que se realiza al personal y además anotar la frecuencia con que se realiza

4.3.2 POLÍTICAS ESTRATÉGICAS CONTABLES

- **Componentes de los estados financieros**

Un conjunto completo de estados financieros comprende los siguientes componentes:

- Balance General
- Estado de Resultados
- Estado de Cambios en el Patrimonio
- Estado de Flujos de Efectivo
- Políticas contables utilizadas y demás notas explicativas.

Anotar cada una de las políticas estratégicas que se aplica a los elementos de los estados financieros y que aplica la entidad

4.3.3 POLÍTICAS ESTRATÉGICAS APLICABLES AL SISTEMA INFORMÁTICO

4.3.3.1 POLITICAS ESTRATÉGICAS GENERALES

- Anotar cada una de las políticas estratégicas generales aplicadas a los sistemas de información por parte de la entidad

4.3.3.2 MANTENIMIENTO DE LA INFORMACIÓN

- .Anotar cada uno de los métodos aplicados para la protección de la información por parte de la entidad

4.3.3.3 APLICACIONES ESTRATÉGICAS

- Anotar el manejo estratégico de la información, detallando cual es plan estratégico aplicación que se sigue mediante los requerimientos por parte de las autoridades competentes

4.3.3.4 NIVELES DE ACCESO:(315 P 60)

- Anotar cada una de las políticas estratégicas de acceso por parte de la entidad para los niveles de acceso tanto al software como al hardware

4.3.3.5 CONTROLES DE ACCESO: (NIA 315 P 60)

- Anotar las políticas de control sobre los accesos a los equipos y al software. tomando en cuenta que se estén poniendo en práctica

4.3.3.6 PERFILES DE LOS USUARIOS:

- Anotar los perfiles de cada uno de los usuarios detallando detallándolo por cada nivel jerárquico

4.3.3.7 SITUACIONES ESTRATÉGICAS DE EMERGENCIA:

- Anotar cada políticas estratégica de emergencia que posee la entidad (sugerir en el caso de no poseerla) de tal manera que se de cumplimiento a la salvaguarda de los activos de la entidad

5 IDENTIFICACIÓN DE LAS LEYES Y REGLAMENTOS APLICABLES (NIA 250)

5.1 LEYESA PLICABLES A LA EMPRESA

5.1.1 LEYES MERCANTILES

- Anotar cada una de las leyes mercantiles que le son aplicables a la empresa

5.1.2 LEYES TRIBUTARIAS

- anotar cada una de las leyes tributarias que les son aplicables a la empresa

5.1.3 OTRAS LEYES APLICABLES

- anotar otro tipo de leyes y reglamentos que le son aplicables (pueden incluirse leyes internacionales)

5.2 LEYES ESPECÍFICAS Y NORMATIVAS APLICABLES AL SISTEMA

5.2.1 LEYES ESPECÍFICAS

- Anotar cada una de las leyes específicas a los sistemas de información con los detalles de artículos

5.2.2 NORMATIVA LEGAL PROPIA DEL SISTEMA

- anotar la normativa técnica aplicable a la entidad (tanto local como internacional)

5.2.2 MANUALES DEL SISTEMA

VERIFICAR CADA UNO DE LOS SIGUIENTES MANUALES

- Manual del usuario
- Manual de Operación
- Manual del software
- Manual del hardware

5.2.3 NIVELES DE SEGURIDAD DEL SISTEMA

Anotar cada una de las estrategias para salvaguardar la información y los activos de la empresa, en virtud de la seguridad empleada

6 ADMINISTRACIÓN DEL TRABAJO

Anotar de forma breve y descriptiva el trabajo que realizará cada una de las personas asignadas para la ejecución del trabajo encomendado en la auditoría

7 PRESUPUESTO DE RECURSOS (NIA 300 P 10)

7.1. PRESUPUESTO DE RECURSOS

Anotar los tipos de recursos a utilizar en el desarrollo del trabajo

1. Recursos Humanos

2. Recursos Financieros

3. Recursos Materiales

Entre otros. Detallando el presupuesto a utilizar de cada uno de ellos

8. CRONOGRAMA DE ACTIVIDADES (NAS S5 P 6)

PRESUPUESTO DE TIEMPO

								ACTIVIDADES											
								PLANEACIÓN (hrs)					DESARROLLO (hrs)			DICTAMEN(INFORME) (hrs)		
Presupuesto / Fecha	Aplicación	Sub Total	HT (1)	RF (2)	MM (3)	RU (4)	EV (5)	Conocimiento del negocio (IVESTIGACIÓN PRELIMINAR)	Cuestionarios	Narrativas	MP	Programas	Desarrollo de Programas	Documentación de Programas	Hallazgos	Borrador de Informe	Preparación de Informe	Opinión
A																		
N																		
O																		
T																		
A																		
R																		
L																		
A																		
S																		
F																		
E																		
C																		
H																		
A																		
S																		
TOTALES																		

PROGRAMAS DE AUDITORÍA ESTRATÉGICA A LOS SISTEMAS DE INFORMACIÓN (NAS S5 P3-6; NIA 300 P8-27; GUIA DE AUDITORÍA DE SISTEMA G15)

FIRMA DE AUDITORÍA
Cliente:

Período:

Ref.:_____
Hecho Por:_____ Fecha:_____
Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Ciclo de Vida de los Sistemas (CDVS)

Empresa:

Fecha de la Auditoria:

OBJETIVO.

- Comprobar que se cumpla con las políticas y procedimientos establecidos en un proyecto estratégico a los sistemas de información como parte del plan de la entidad.

TECNICAS:

- Confirmación
- Revisión
- Verificación
- Comprobación
- Observación

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
1. Verificar la existencia de un marco de trabajo para la administración de proyectos estratégicos relacionados a la inversión de TI.			PO10.1	
2. Verifique que el/los proyecto/s contribuya/n al apoyo de/los programa/s estratégico/s de la entidad			PO10.1	
3. Verifique el marco de trabajo de administración de proyectos estratégicos			PO10.2	
4. Revise que el marco de trabajo para la administración de proyectos define el alcance y límite de/los proyecto/s, así como la metodología empleada en cada proyecto emprendido. **pasa**			PO10.2	

FIRMA DE AUDITORÍA

Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Ciclo de Vida de los Sistemas (CDVS

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene				
5. Confirme que el enfoque de/los proyecto/s estratégico/s corresponda a la complejidad y requerimiento regulatorio de cada uno de éstos			**PO10.3; ME3.1 ME3.3**	
6. Verifique que por cada uno de los proyectos se da una rendición de cuentas a quien los patrocina (oficina de proyectos, gerente de proyecto, entre otros), en cada una de las etapas.			**PO10.3**	
7. Verificar cada uno de los proyectos cuentan con patrocinadores de proyectos de TI con la suficiente capacidad y autoridad para apropiarse del proyecto dentro del programa estratégico de la entidad.			**PO10.3**	
8. Comprobar que existe un compromiso de los interesados en la definición y ejecución del proyecto estratégico dentro del contexto del programa de TI.			**PO10.4**	
9. Compruebe que estén definidos los estatutos sobre el alcance del/os proyecto /s estratégico/s			**PO10.5**	
10. Verifique que se documente la naturaleza y alcance del/os proyecto/s estratégico/s **pasa**			**PO10.5**	

FIRMA DE AUDITORÍA

Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Ciclo de Vida de los Sistemas (CDVS)

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene 11. Compruebe que las etapas de inicio del/os proyecto/s se hayan aprobado de manera formal y se hayan comunicado a todos los interesados (asegurarse mediante la revisión de documentación que respalde dicho proceso)			**PO10.6**	
12. Compruebe que las fases subsiguientes se de continuidad previo a la revisión y aceptación de la fase anterior (asegúrese que en las fases traslapadas exista un punto de aprobación por parte de los patrocinadores)			**PO10.6**	
13. Verifique que exista un plan integrado para el proyecto, que esté aprobado el cual contribuya a guiar la ejecución del proyecto a través del la vida de éste; dicho plan debe de mantenerse en el proyecto y en las modificaciones (si existen) el cual debe de ser aprobado de acuerdo al gobierno del proyecto			**PO10.7**	
14. Compruebe. la coordinación que existe para definir las responsabilidades de los recursos del/os proyecto/s (asegúrese que las obtención de productos y servicios requeridos para cada proyecto se planee y administre de acuerdo al los objetivos planteados)			**PO10.8**	
Pasa			**PO10.9**	

FIRMA DE AUDITORÍA

Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Ciclo de Vida de los Sistemas (CDVS)

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene				
15. Verifique que existe una administración de riesgos de proyectos estratégicos, mediante una sistemática planificación, identificación, análisis, respuesta, monitoreo y control de las áreas o eventos que tengan potencial riesgo.			**PO10.10**	
16. Verificar la existencia de un plan de administración de la calidad en el proyecto estratégico, y si este se encuentra descrito como será implantado. (asegúrese que esté aprobado de manera formal por las partes interesadas).			**PO10.10**	
17. Verifique que exista el establecimiento de un sistema de control de cambios para cada proyecto de tal manera que cada uno de los cambios sean revisados y aprobados de manera apropiada por los interesados; de acuerdo al plan estratégico planteado.			**PO10.11**	
18. Verifique las tareas de aseguramiento requeridas para apoyar las acreditaciones de nuevos sistemas durante la etapa de planeación del proyecto (asegúrese que las tareas proporcionen las seguridad de los controles y que satisfagan los requerimientos requeridos)			**PO10.12**	
Pasa				

FIRMA DE AUDITORÍA
Cliente:

Período:

Ref.:_____
Hecho Por:_____ Fecha:_____
Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Ciclo de Vida de los Sistemas (CDVS)

Empresa:

Fecha de la Auditoria:

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene				
19. compruebe que exista una medición adecuada del desempeño; así como reportes y monitoreo del/os proyecto/s estratégico/s (asegúrese que existan medidas correctivas en caso de fallas de acuerdo al marco de trabajo)			**PO10.13**	
20. Verifique que al finalizar el proyecto, los interesados se cercioren que el proyecto estratégico haya proporcionado tos resultados y beneficios esperados			**PO10.14**	
21. Compruebe que se han identificado y comunicado cualquier actividad sobresaliente requerida para alcanzar los resultados planteados del proyecto estratégico y los beneficios del programa a fin de ser utilizadas en proyectos posteriores.			**PO10.14**	
22. Verifique que el entrenamiento al personal sea el adecuado, de acuerdo al proyecto estratégico de TI,			**AI7.1**	
23. Verifique que el plan de prueba se base en los estándares de toda la organización (cerciórese que el plan incluye pruebas definidas, requerimientos de entrenamiento, instalación o actualización y corrección de errores y aprobación formal).			**AI7.2**	
Pasa				

FIRMA DE AUDITORÍA
Cliente:
Período:

Ref.:_____
Hecho Por:_____ Fecha:_____
Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Ciclo de Vida de los Sistemas (CDVS)

Empresa:

Fecha de la Auditoria:

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene				
24. Verifique que el plan de implantación sea aprobado por las partes relevantes (cerciórese que en dicho plan se han definido las versiones, construcción de paquetes procedimientos de implantación, manejo de incidentes, controles de distribución, almacenamiento del software, revisión de versión y documentación de cambio; como parte del plan estratégico de la entidad			**AI7.3**	
25. Verifique que el ambiente de prueba contempla el plan estratégico (amiente futuro de operaciones), para permitir pruebas acertadas (cerciórese que la documentación de la prueba sea archivada).			**AI7.4**	
26. Verifique que la entidad contempla para todos los proyectos estratégicos, la implantación o modificación de los elementos necesarios tales como: Hardware, software, datos de transacciones, archivos maestros, respaldos, interfaces con otros sistemas, procedimientos, documentación de sistemas entre otros, los cueles deben ser convertidos del sistema anterior al nuevo con base a lo previsto. (cerciórese, que los propietarios del sistema lleven acabo una verificación detalladas del proceso inicial del nuevo sistema			**AI7.5**	
Pasa				

FIRMA DE AUDITORÍA
Cliente:
Período:

Ref.:_____
Hecho Por:_____ Fecha:_____
Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Ciclo de Vida de los Sistemas (CDVS)

Empresa:

Fecha de la Auditoria:

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene				
27. Verifique que la prueba de cambios, garantice que son de acuerdo con el plan de aceptación definido y con base a una evaluación de impacto y recurso que incluye la dimensión del desempeño en un ambiente separado de pruebas por parte de un grupo independiente, antes de comenzar su uso en el ambiente de operación regular (las pruebas en paralelo o piloto se consideran parte del plan, además los controles de seguridad deben ser probados)			**AI7.6**	
28. Compruebe que la prueba final de aceptación garantice que los procedimientos proporcionan, una evaluación formal y la aprobación formal de los resultados de la prueba por parte de la gerencia de los departamentos de usuarios afectados y la función de TI, (cerciórese que la prueba cumpla con todos los componentes del sistema de información y garanticen que los requerimientos de seguridad se satisfagan)			**AI7.7** **AI7.1**	
29. Compruebe que la transferencia a producción del sistema se haga mediante procedimientos formales desde el ambiente de desarrollo al de prueba; de acuerdo con el plan estratégico			**AI7.8**	
Pasa				

FIRMA DE AUDITORÍA
Cliente:
Período:

Ref.:_____
Hecho Por:_____ Fecha:_____
Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Ciclo de Vida de los Sistemas (CDVS)

Empresa:

Fecha de la Auditoria:

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene				
30. Verifique que la liberación del software se realice mediante procedimientos formales que aseguren la autorización, acondicionamiento, prueba de regresión, distribución, transferencia de control rastreo de estatutos, procedimientos de respaldo y notificación de usuario.			**AI7.9**	
31. Compruebe que la distribución del sistema se realiza mediante procedimientos de control oportuna y correcta y la actualización de los componentes aprobados de la configuración, esto incluye: controles de integridad, segregación de funciones, prueba y operación, y adecuadas pistas de auditoría de todas las actividades			**AI7.10**	
32. Compruebe que existen procedimientos de acuerdo a los estándares de desarrollo y de cambios de la empresa que requieran una revisión posterior a la implantación del sistema para evaluar y reportar si el cambio satisface los requerimientos del cliente			**AI7.12**	
Pasa				

Viene

FIRMA DE AUDITORÍA
Cliente:

Período:

Ref.:_____
Hecho Por:_____ Fecha:_____
Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Ciclo de Vida de los Sistemas (CDVS)

ALCANCE:

CONCLUSION:_____
_____

Los objetivos señalados al principio de esta sección del programa de auditoria ¿Han sido alcanzados?
SI_____ NO_____ FIRMA_____
Explicación de porqué no hay conclusión_____

SUPERVISOR: _____ FECHA: _____
AUTORIZO: _____ FECHA: _____
AUDITOR: _____ FECHA: _____

FIRMA DE AUDITORÍA
Cliente:

Período:

Ref.:_____
Hecho Por:_____ Fecha:_____
Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Gobierno Corporativo

Empresa:

Fecha de la Auditoria:

OBJETIVO.

- Determinar la existencia de un gobierno corporativo para un mejor desempeño en el área de informática.

TECNICAS:

- Confirmación
- Revisión
- Verificación
- Comprobación
- Observación

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
33. Verificar la estructura del Gobierno (GC); Corporativo con la finalidad de dar cumplimiento a los planes estratégicos que se pretenden alzar			PO4.2;ME4.1	
34. Verifique las reglas de actuación del Gobierno Corporativo, con la finalidad de determinar los proyectos que se pretenden alcanzar.			PO4.3;ME4.2	
35. Verifique los Códigos de conducta con que se rige el Gobierno Corporativo			PO4.6	
36. Confirmar si se está dando cumplimiento a los Códigos de Conducta por parte del Gobierno Corporativo. pasa				

FIRMA DE AUDITORÍA

Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Gobierno Corporativo

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene				
37. Confirmar si los códigos de conducta del Gobierno Corporativo son acorde con la realidad y si contemplan exigencias externas ante la sociedad.				
38. Verifique la creación de proyectos estratégicos que plantea el GC			**PO4.1;PO4.2**	
39. Verificar si se está dando cumplimiento a la guía estratégica de la compañía, el monitoreo efectivo del equipo de dirección por el consejo de administración y las responsabilidades del Consejo de Administración con sus accionistas			**ME4.2**	
40. Comprobar que el GC, asegura que haya una revelación adecuada y a tiempo de todos los asuntos relevantes de la empresa, incluyendo la situación financiera, su desempeño, la tenencia accionaria y su administración			**ME4.2**	
41. Compruebe que el GC, reconoce los derechos de terceras partes interesadas y promueve una cooperación activa entre ellas y las sociedades en la creación de riqueza, generación de empleos y logro de empresas financieras sustentables de acuerdo a los planes estratégicos implementados			**PO4.6**	
pasa				

FIRMA DE AUDITORÍA

Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Gobierno Corporativo

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene				
42. Compruebe que el GC, promueve el tratamiento equitativo para todos los accionistas, incluyendo a los minoritarios y a los extranjeros				
43. Determine la estructura de gestión del GC con relación al Las Tecnologías de la Información			**PO4.15**	
44. Verifique los planes estratégicos de corto y largo plazo de expansión de la compañía que propone el GC, y las expectativas que se proponen.			**PO4.2**	
45. Compruebe, la comunicación que existe entre el comité del GC, los accionistas, administración, y demás interesados en la entidad, para una buena entrega de información, seguimiento de control para que los planes estratégicos se resuelvan de la mejor manera			**PO4.15**	
46. Determinar la medición del desempeño del Gobierno corporativo, con relación a los planes estratégicos planteados.			**PO4.6**	
Pasa				

Viene

FIRMA DE AUDITORÍA

Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Gobierno Corporativo

ALCANCE:

CONCLUSION:_____
_____

Los objetivos señalados al principio de esta sección del programa de auditoria ¿Han sido alcanzados?
SI_____ NO_____ FIRMA_____
Explicación de porqué no hay conclusión_____

SUPERVISOR: _____ FECHA: _____
AUTORIZO: _____ FECHA: _____
AUDITOR: _____ FECHA: _____

FIRMA DE AUDITORÍA

Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información relativo al Área Estructura Organizativa

Empresa:

Fecha de la Auditoria:

OBJETIVO.

- Verificar la existencia, funcionalidad, segregación de funciones y la adecuada determinación de responsabilidades dentro de la estructura organizativa de la Institución, de forma estratégica

TECNICAS:

- Verificación.
- Observación.
- Revisión.
- Investigación.
- Evaluación

No.	PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
1.	Verificar la misión y las metas de la organización			PO10.1: PO4.1	
2.	Revisar las iniciativas de tecnología de información para soportar la misión y las metas de la organización			PO10.1;PO10.2 PO4.1	
3.	Verificar las oportunidades para las iniciativas de tecnología de información de la organización			PO4.1	
4.	Investigar los estudios de factibilidad de las iniciativas de tecnología de información			PO10.1	
	Pasa				

Viene
FIRMA DE AUDITORÍA
Cliente:

Período:

Ref.:_____
Hecho Por:_____ Fecha:_____
Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Área Estructura Organizativa

Empresa:

Fecha de la Auditoria:

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
5. Verificar la evaluación de los riesgos de las iniciativas de tecnología de información			**PO6.2;PO4.8**	
6. Verificar la inversión óptima de las inversiones en tecnología de información actuales y futuras				
7. Verificar la existencia de un Comité de TI			**PO4.2;PO4.5**	
8. Observar si se han definido e identificado la calidad de miembro, las funciones y las responsabilidades del comité de planeación de los procesos de			**PO4.6**	
9. Verificar si las políticas y los comunicados del Gerente General de de la compañía son para asegurar la independencia y la autoridad de la función de los servicios de información.			**PO4.6**	
10. Verificar si existen políticas que determinen las funciones y responsabilidades para todo el personal dentro de la organización con respecto a sistemas de información, control y seguridad internos.			**PO4.11**	
11. Verificar si existen políticas y procedimientos en TI para controlar las actividades de consultores y demás personal por contrato, asegurando así la protección de los activos de la organización			**PO4.12**	
Pasa				

FIRMA DE AUDITORÍA
Cliente:

Período:

Ref.:_____
Hecho Por:_____ Fecha:_____
Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Área Estructura Organizativa

Empresa:

Fecha de la Auditoria:

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene			**PO4.6**	
12. Evaluar Segregación de Tareas en TI ▣ Existe una segregación de funciones entre los siguientes pares de unidades: ▣ desarrollo y mantenimiento de sistemas ▣ desarrollo y operaciones de sistemas ▣ desarrollo/mantenimiento de sistemas y seguridad de la información. ▣ operaciones y control de datos ▣ operaciones y usuarios ▣ operaciones y seguridad de la información			**PO4.11**	
13. Evaluar Calidad				
14. Revisar si existen políticas y funciones de aseguramiento de la calidad.			**PO4.7**	
15. Revisar si se cuenta con un grupo de aseguramiento de la calidad.			**PO4.7;PO8.2** **PO8.6**	
16. Evaluar Seguridad ▣ Hay un grupo de seguridad de la información ▣ Existen campañas regulares para incrementar la conciencia y disciplina en cuanto al control y la seguridad interna. ▣ El Jefe de la Oficina de Sistemas ha asignado formalmente la responsabilidad a lo largo de toda la organización para la formalización de políticas y procedimientos de control y seguridad internos (tanto lógicos como físicos) a algún funcionario de seguridad de la información			**PO4.2** **DS5.1** **PO4.7**	
Pasa				

FIRMA DE AUDITORÍA
Cliente:

Período:

Ref.:_____
Hecho Por:_____ Fecha:_____
Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Área Estructura Organizativa

Empresa:

Fecha de la Auditoria:

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene				
17. Verificar la reingeniería de las iniciativas de tecnología de información para reflejar los cambios en la misión y las metas de la organización.			**PO6.1**	
18. Verifique la evaluación de las estrategias alternativas para las aplicaciones de datos, tecnología y organización			**PO1.3**	
19. Realizar visitas preliminares al encargado del área para tener mayor conocimiento de la organización y su funcionamiento.			**PO1.3**	
20. Obtener manuales de organización y descripción de puestos del área de informática.				
21. Verificar la adecuada segregación de funciones.			**PO4.11**	
22. Investigar si los puestos de trabajo existentes son adecuados a las necesidades y objetivos que tiene el área para llevar a cabo sus funciones.			**PO4.6**	
23. Verificar que la estructura organizativa de la Institución se ajusta a los reglamentos establecidos internamente.				
24. Analizar si los niveles jerárquicos establecidos son necesarios y suficientes para el desarrollo de las actividades del área.				
Pasa				

FIRMA DE AUDITORÍA
Cliente:

Período:

Ref.:_____
Hecho Por:_____ Fecha:_____
Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Área Estructura Organizativa

Empresa:

Fecha de la Auditoria:

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene				
25. Determinar si las áreas cuentan con sub-áreas y si éstas están delimitadas con claridad sus funciones y responsabilidades.			**PO4.4;PO4.5**	
26. Conocer de que dirección o gerencia depende el área de informática			**PO4.4**	
27. Corroborar que los niveles jerárquicos existentes permiten una comunicación oportuna, ágil y veraz de la información			**PO4.15**	

ALCANCE:

CONCLUSION:_____
_____

Los objetivos señalados al principio de esta sección del programa de auditoria ¿Han sido alcanzados?
SI_____ NO_____ FIRMA_____
Explicación de porqué no hay conclusión_____

SUPERVISOR: _____ FECHA: _____
AUTORIZO: _____ FECHA: _____
AUDITOR: _____ FECHA: _____

FIRMA DE AUDITORÍA
Cliente:
Período:

Ref.:_____
Hecho Por:_____ Fecha:_____
Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Área de Recursos Humanos

Empresa:

Fecha de la Auditoria:

OBJETIVO.

- Determinar la existencia de políticas y procedimientos estratégicos adecuados y su aplicación en el área de recursos humanos.

TECNICAS:

- Confirmación
- Revisión
- Verificación
- Comprobación

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
1. Verificación de los procedimientos de reclutamiento de personal.de Sistemas			PO7.1;PO4.14	
2. Verificación de capacitación constante para el buen funcionamiento del sistema.			PO7.4	
3. Verificar el entrenamiento y desarrollo Profesional de los empleados			PO7.4	
4. Verificar que los programas de entrenamiento sean consistentes con los requerimientos mínimos sobre los planes estratégicos de la empresa; relacionados con la educación, el conocimiento y la conciencia generales que cubren los asuntos de seguridad de la información			PO7.4	

Pasa

FIRMA DE AUDITORÍA
Cliente:
Período:

Ref.:_____
Hecho Por:_____ Fecha:_____
Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Área de Recursos Humanos

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene				
5. Verificar si los empleados son evaluados tomando como base un conjunto estándar de perfiles de competencia para la posición y si se llevan a cabo evaluaciones en forma periódica de tal manera que cubran los requerimientos sobre las políticas estratégicas de la empresa.			**PO7.1** **PO7.2**	
6. Verificación de las herramientas adecuadas para realizar el trabajo., como parte del plan estratégico que se pretende lograr.la empresa			**DS3.4**	
7. Revisión de desempeño por áreas de trabajo.			**PO7.3**	
8. Verificación de procedimientos para el control del personal.				
9. Confirmar si administración está comprometida con el entrenamiento y el desarrollo profesional de sus empleados.			**PO7.4;DS7.2**	
10. Verificar si están bien definidas las responsabilidades y funciones del personal del área de sistema			**PO7.3**	
11. Verificar si está el departamento dotado del personal adecuado y cómo la dirección del mismo influye en la ética de los trabajadores del área **Pasa**			**PO7.2**	

FIRMA DE AUDITORÍA
Cliente:
Período:

Ref.:_____
Hecho Por:_____ Fecha:_____
Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Área de Recursos Humanos

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene				
12. Verificar si es compatible la estructura del departamento de sistemas con los demás departamentos de la entidad.			**PO4.15**	
13. Verificar si existe una buena comunicación entre los trabajadores del área Sistemas con otras áreas de la entidad.			**PO4.15**	
14. Verificar si las condiciones de trabajo son las más adecuadas.				
15. Comprobar si es utilizada al máximo la capacidad de los equipos instalados y de forma eficiente			**DS3.1;DS3.2**	
16. Verificar si se tienen en cuenta los criterios de los empleados subordinados en la elaboración de las estrategias del departamento y de la entidad en general.				
17. Verificar si los procedimientos estratégicos establecen ➢ Las tareas a realizar, ➢ Definen las responsabilidades de los individuos que intervienen, teniendo en cuenta las áreas de responsabilidad, ➢ Contribuyen al flujo de trabajo. ➢ Permiten destacar las excepciones a la actuación planeada.			**PO7.3;PO4.6 PO4.11**	
Pasa				

FIRMA DE AUDITORÍA
Cliente:
Período:

Ref.:_____
Hecho Por:_____ Fecha:_____
Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Área de Recursos Humanos

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene				
18. Verificar si el sistema de estimulación existente permite el desarrollo de las expectativas y necesidades sociales de los trabajadores del área.			**PO7.7**	
19. Verificar si son compatibles las necesidades de recursos humanos con los objetivos y metas trazados en la entidad y en el departamento			**PO7.7**	
20. Verificar si existe un adecuado control de las entradas y salidas del personal que labora en esta área.			**PO7.8**	

ALCANCE:
CONCLUSION:_____
_____
Los objetivos señalados al principio de esta sección del programa de auditoria ¿Han sido alcanzados?
SI_____ NO_____ FIRMA_____
Explicación de porqué no hay conclusión_____

SUPERVISOR: _____ FECHA: _____
AUTORIZO: _____ FECHA: _____
AUDITOR: _____ FECHA: _____

FIRMA DE AUDITORÍA
Cliente:

Período:

Ref.:_____
Hecho Por:_____ Fecha:_____
Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Área de Políticas y Procedimientos

Empresa:

Fecha de la Auditoria:

OBJETIVO.

- Determinar la existencia de políticas y procedimientos estratégicos adecuados y su aplicación en el área de informática.

TECNICAS:

- Confirmación
- Revisión
- Verificación
- Comprobación

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
1. Identificar a la persona encargada de la institución de las políticas y procedimientos.			**PO6.1**	
2. Verificar que las políticas y procedimientos Estratégicos existentes estén debidamente autorizadas por la autoridad competente.			**PO6.3**	
3. Comprobar que los empleados del departamento de informática tiene conocimiento y comprensión de las políticas y procedimientos establecidos.			**PO6.4**	
4. Corroborar que las políticas y procedimientos toman en cuenta los requerimientos de los empleados **Pasa**			**PO6.5**	

FIRMA DE AUDITORÍA
Cliente:

Período:

Ref.:_____
Hecho Por:_____ Fecha:_____
Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Área de Políticas y Procedimientos

Empresa:

Fecha de la Auditoria:

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene				
5. Verificar si las políticas establecidas contribuyen al máximo rendimiento por parte del personal				
6. Comprobar si existen medidas correctivas en caso de que los empleados del área no acaten las políticas y procedimientos establecidos.			**PO6.2**	
7. Asegurarse que las actividades desarrolladas por cada individuo estén claramente determinadas.			**PO7.3**	
8. Verificar que se establecen relaciones con las demás áreas de la institución.				
9. Confirmar que se emiten procedimientos sobre los siguientes puntos:			**PO7.1**	
☛ Selección y contratación de personal ☛ Manejo de la documentación con que se trabaja ☛ Seguridad sobre los activos del área ☛ Mantenimiento del equipo ☛ Reacción del personal en caso de contingencia			**DS5.1** **AI3.3**	
10. Verificar si los procedimientos establecidos en el manual general sirven de guía facilitándola para el desarrollo de las labores de los empleados			**PO6.5**	
Pasa				

Viene

FIRMA DE AUDITORÍA
Cliente:

Período:

Ref.:_____
Hecho Por:_____ Fecha:_____
Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Área de Políticas y Procedimientos

ALCANCE:

CONCLUSION:_____
_____

Los objetivos señalados al principio de esta sección del programa de auditoria ¿Han sido alcanzados?
SI_____ NO_____ FIRMA_____
Explicación de porqué no hay conclusión_____

SUPERVISOR: _____ FECHA: _____
AUTORIZO: _____ FECHA: _____
AUDITOR: _____ FECHA: _____

FIRMA DE AUDITORÍA

Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Procesamiento Electrónico de Datos (PED)

Empresa:

Fecha de la Auditoria:

OBJETIVOS.

- Evaluar : Establecer la existencia de Objetivos y políticas estratégicas con relación al área de procesamien de datos.
- Evaluar : Los Criterios de administración del área de soporte técnico.
- Verificar : Que el personal trabaja en base a manuales de aplicación.
- Comprobar : La competencia del personal responsable del manejo del software.
- Evaluar : El nivel de segregación de funciones para el manejo de los software.

TECNICAS:

- Confirmación.
- Verificación.
- Revisión.
- Evaluación.
- Investigación.

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
1. Verificar el plan estratégico de la organización y todos los métodos coordinados y medidas adaptadas en el PED, para salvaguardar sus activos, la exactitud y confiabilidad de sus datos contables, la eficiencia de las operaciones y el apego a las políticas prescritas. Tales como: a. Un plan estratégico de la organización que proporcione segregación apropiadas de las responsabilidades funcionales. **Pasa**			**PO1.4** **PO07.3**	

FIRMA DE AUDITORÍA

Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Procesamiento Electrónico de Datos (PED)

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene b. Un sistema adecuado de procedimientos de autorización y registro para ejercer un control de contabilidad razonable sobre los activos, pasivos, ingresos y gastos.			**PO4.14**	
c. Practicas consecuentes a seguir en la ejecución de los deberes y las funciones de cada uno de los departamentos de la organización.			**PO7.3**	
d. Un grado de calidad del personal conmensurable con sus responsabilidades.			**PO7.2**	
2. Evaluar si el plan estratégico sobre la segregación de funciones en el PED se está dando cumplimiento para el logro de los siguientes objetivos			**PO1.3**	
☛ Proporcionar una eficaz verificación cruzada de la exactitud y corrección de los cambios introducidos en el sistema			**DS11.6**	
☛ Impedir al personal de operación efectuar revisiones sin previa autorización y plena verificación.			**DS11.6**	
☛ Evitar que el personal ajeno a la operación tenga acceso al equipo			**DS12.3;DS11.6**	
Pasa				

Viene

FIRMA DE AUDITORÍA

Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Procesamiento Electrónico de Datos (PED)

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
☛ Mejorar la eficiencia, puesto que las capacidades, el adiestramiento y las pericias que se requieren para desempeñar tan diversas actividades, difieren notablemente				
3. Verifique que la dirección ha determinado su, control estratégico de sistema que debe comprender como mínimo tres niveles: a) El nivel de datos fuente b) El nivel de procesamiento de datos c) El nivel de reportes			**ME2.5**	
4. Confirmar que los controles de los datos fuente cumpla con la finalidad perseguida tales como: ❖ Determinar que todas las transacciones se hayan registrado correctamente en su punto de origen o fuente ❖ Determinar que todas las transacciones se trasmitan del punto de registro al de procesamiento				
Pasa				

Viene

FIRMA DE AUDITORÍA

Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Procesamiento Electrónico de Datos (PED)

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
5. Confirmar la existencia de verificaciones programadas para determinar la validez de los datos de entrada o fuente tales como: ✓ Verificación de existencia ✓ Verificación de combinación ✓ Verificación de totalidad ✓ Verificación de razonabilidad				
6. Evaluar la exactitud del procesamiento de datos en un sistema PED mediante verificaciones programadas de la siguiente manera Descubrir la perdida de datos o la falta de su procesamiento Determinar que las funciones aritméticas se ejecuten correctamente Determinar que todas las transacciones se asienten en el registro indicado Asegurar que todos los errores descubiertos en el procesamiento de datos se corrijan satisfactoriamente. **Pasa**			**Po4.4**	

FIRMA DE AUDITORÍA

Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Procesamiento Electrónico de Datos (PED)

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene				
7. Verificar la funcionabilidad de los controles de salida determinando que los datos procesados no incluyan ninguna alteración desautorizada por la sección de operación de la computadora, y que los datos sean sustancialmente correctos o razonables.			**DS11.6**	
8. Verificar que existan controles de salida de comparación de los datos procesados con los totales obtenidos independientemente de procesos anteriores o de los datos fuente original.			**DS11.6**	
9. Investigar la existencia de Políticas de revisión a la documentación, para determinar la existencia de un sistema contable, así como para evaluar los controles empleados para fomentar el apego a las políticas de las empresas y para lograr eficiencias de operación			**DS9.3**	
10. Observar las actividades de Procesamiento de datos a fin de verificar el cumplimiento de las políticas implementadas en el PED				
Pasa				

FIRMA DE AUDITORÍA

Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Procesamiento Electrónico de Datos (PED)

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene 11. Verificar claves de acceso de usuario y acceso al software, si las hay capture las pantallas hasta llegar a seleccionar la empresa. 12. Realizar pruebas de registro de documentos. 13. Verificación de la buena digitación para introducir la información 14. Validación de los reportes emitidos por el sistema. 15. Verificación y validación de pruebas aritméticas del sistema. 16. Verificación de políticas establecidas para poder ingresar un documento al sistema. 17. Verificación de los procedimientos a seguir para la eliminación de reportes modificación, fusión, división de reporte? 18. Verificación de la captación de datos que se reciben **Pasa**			**DS5.7** **PO6.5**	

Viene

FIRMA DE AUDITORÍA

Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Procesamiento Electrónico de Datos (PED)

ALCANCE:

CONCLUSION:_____
_____

Los objetivos señalados al principio de esta sección del programa de auditoria ¿Han sido alcanzados?
SI_____ NO_____ FIRMA_____
Explicación de porqué no hay conclusión_____
SUPERVISOR: _____ FECHA: _____
AUTORIZO: _____ FECHA: _____
AUDITOR: _____ FECHA: _____

FIRMA DE AUDITORÍA
Cliente:

Período:

Ref.:_____
Hecho Por:_____ Fecha:_____
Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Área de Seguridad Electrónica

Empresa:

Fecha de la Auditoria:

OBJETIVO.

- Determinar la existencia estratégica de Seguridad Electrónica y su aplicación en el área de informática.

TECNICAS:

- Confirmación
- Revisión
- Verificación
- Comprobación

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
1. Verificar si se cuenta con un plan de seguridad estratégico que proporcione una dirección y control centralizados sobre la seguridad de los sistemas de información, así como requerimientos de seguridad de usuario con propósitos de consistencia.			**DS5.1** **DS5.2**	
2. Comprobar si se cuenta con una organización de seguridad centralizada responsable de asegurar el acceso apropiado a los recursos del sistema			**DS5.3**	
3. Revisar si se cuenta con un esquema de clasificación de datos en operación que indique que todos los recursos del sistema cuentan con un propietario responsable de su seguridad y contenido			**DS5.3**	
4. Revisar si los equipos con bluetooth cuentan con un nivel de acceso estrictamente restringido y con claves de acceso específicas para el usuario			**DS5.7**	

Pasa

FIRMA DE AUDITORÍA
Cliente:

Período:

Ref.:_____
Hecho Por:_____ Fecha:_____
Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Área de Seguridad Electrónica

Empresa:

Fecha de la Auditoria:

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene				
5. Verificar si se cuenta con perfiles de seguridad de usuario que representen "los menos accesos requeridos" y que muestren revisiones regulares a los perfiles por parte de la administración con fines de reacreditación.			**DS5.2** **DS5.5**	
6. Confirmar si el entrenamiento de los empleados incluye un conocimiento y conciencia sobre seguridad, las responsabilidades de los propietarios y los requerimientos de protección contra virus			**DS7.7**	
7. Confirmar si las acciones que posibilitan la transición del sistema de un estado a otro. se registra información sobre las acciones y se examina el estado corriente y la transición propuesta para determinar si el nuevo estado debería no permitirse. sólo el analizar la transición puede no ser suficiente y se puede necesitar el estado inicial. se tiende a utilizar esto cuando las transiciones específicas requieren siempre análisis,			**DS5.5**	
8. Confirmar si al sistema se accesa de forma no autorizado.			**DS5.10**	
Pasa				

FIRMA DE AUDITORÍA
Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Área de Seguridad Electrónica

Empresa:

Fecha de la Auditoria:

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene				
9. Verifique la efectividad de los mecanismos de protección y determinar que mecanismos son apropiados y averiguar además si se. disuade de ataques debido a la presencia de un registro identificar algunos problemas:,			**DS5.10**	
10. Identificar a la persona encargada de la institución de las políticas, procedimientos y si los cambios son divulgados oportunamente			**DS5.2**	
11. Verificar que las políticas y procedimientos Estratégicos existentes estén debidamente autorizadas por la autoridad competente.			**DS5.1** **DS5.2**	
12. Comprobar que los empleados del departamento de informática tiene conocimiento y comprensión de las políticas y procedimientos establecidos.			**DS5.2**	
13. Corroborar que las políticas y procedimientos toman en cuenta los requerimientos de los empleados.			**DS5.2**	
14. Verificar si las políticas establecidas contribuyen al máximo rendimiento por parte del personal			**DS5.2**	
15. Verifique si existe cualquier violación de una política conocida, se trata de preguntarse si el sistema entra o no en un estado no permitido. El enfoque se centra en la política y las acciones diseñadas para violar la política, las acciones específicas pueden no ser conocidas.			**DS5.2**	
Pasa				

FIRMA DE AUDITORÍA
Cliente:

Período:

Ref.:_____
Hecho Por:_____ Fecha:_____
Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Área de Seguridad Electrónica

Empresa:

Fecha de la Auditoria:

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene				
16. Verifique si las acciones conocidas que son parte de un intento de hacer brecha en la seguridad. Se enfoca en acciones específicas que han sido determinadas para indicar ataques; pueden identificarse dos formas en torno a la detección de violaciones de política conocida: se observa el estado actual del sistema, se registra información sobre el estado y se determina si el estado esta permitido.			**DS5.4** **DS5.5**	
17. Verificar si la política de seguridad describe lo que está permitido y el mecanismo de seguridad, la forma de ejecutar la política; es decir verificar si el mecanismo de seguridad cumple con los procedimientos de la política de seguridad de los usuarios.			**DS5.2** **DS5.3**	
18. Comprobar si existen medidas correctivas en caso de que los empleados del área no acaten las políticas y procedimientos establecidos.			**DS5.6**	
19. Asegurarse que las actividades desarrolladas por cada individuo estén claramente determinadas			**DS5.2**	
20. Verificar que se establecen relaciones con las demás áreas de la institución				
Pasa				

FIRMA DE AUDITORÍA
Cliente:

Período:

Ref.:_____
Hecho Por:_____ Fecha:_____
Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Área de Seguridad Electrónica

Empresa:

Fecha de la Auditoria:

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene				
21. Confirmar que se emiten procedimientos sobre los siguientes puntos: - Selección y contratación de personal - Manejo de la documentación con que se trabaja - Seguridad sobre los activos del área - Mantenimiento del equipo - Reacción del personal en caso de contingencia			**PO7.1** **DS5.6** **DS4.4**	
22. Verificar si los procedimientos establecidos en el manual general sirven de guía facilitadora para el desarrollo de las labores de los empleados				

ALCANCE:

CONCLUSION:_____
_____

Los objetivos señalados al principio de esta sección del programa de auditoria ¿Han sido alcanzados?
SI_____ NO_____ FIRMA_____
Explicación de porqué no hay conclusión_____

SUPERVISOR: _____ FECHA: _____
AUTORIZO: _____ FECHA: _____
AUDITOR: _____ FECHA: _____

FIRMA DE AUDITORÍA

Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información para Evaluar el Área de Hardware

OBJETIVOS DEL PROGRAMA:

Los objetivos de este programa son determinar que:

La seguridad del hardware esté adecuadamente diseñada para el logro de los objetivos estratégicos de la Compañía; contribuyendo a la agilización de los procesos administrativos.

Los Responsables de la seguridad del hardware, usuarios operadores de los hardwares cumplan con las medidas estratégicas de seguridad establecidas por la compañía.

Que los equipos físicos (Hardware) estén en lugares adecuados, así como también que cuenten con instalaciones eléctricas adecuadas y medidas de seguridad estratégicas propias de las características de este tipo de equipos.

PROCEDIMIENTOS	REFERENCIA P/T	HECHO POR	REF COBIT	OBSERVACIONES
Seguridad física:				
a) Verifique si hay personas encargadas de la Seguridad y tome nota de:				
1- Como están organizados.			**DS5.1;DS5.5**	
2- Si es compañía particular de seguridad o si son contratados por cuenta de la empresa.			**DS5.5**	
3- Si las personas cuentan con la capacidad necesaria para desempeñar su cargo.			**PO7.2**	
4- Si la persona encargada de la seguridad, del ingreso al centro de cómputo cuenta con listado de las personas autorizadas para ingresar.			**DS5.2;DS5.3**	
5 - Si la seguridad es adecuada y si hay deficiencia en cuanto a los procedimientos de autorización para el ingreso al centro de computo Pasa			**DS12.2;DS12.3**	

FIRMA DE AUDITORÍA

Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información para Evaluar el Área de Hardware

PROCEDIMIENTOS	REFERENCIA P/T	HECHO POR	REF COBIT	OBSERVACIONES
Viene **b)** Verifique las medidas de seguridad aplicadas a los equipos de cómputo y compruebe que: 1- Los manuales de Operación se Cumplen				
2- Si las labores de mantenimiento son las adecuadas			**AI3.3**	
3- Que las instalaciones cumplan con las condiciones necesarias para el resguardo de los equipos, así como para su buen funcionamiento.			**DS12.1;AI3.1**	
4 Que las instalaciones eléctricas cumplan con los estándares de calidad en cuanto a sus materiales así como de su distribución. (Si es necesario auxiliarse de un especialista en instalaciones eléctricas).			**DS12.2**	
5 Comprobar si existen conductos o equipos de aires acondicionados en el centro de cómputo.			**DS12.2;DS12.5**	
6- verificar si existe extintores de fuego (en caso de una emergencia)			**DS12.5**	
7- Investigar si se cuenta con seguridad para desastres provocados por agua.			**DS12.4**	
8- Asegurarse de que cada máquina cuente con UPS, y que sea de la capacidad necesaria			**DS12.5**	
Verifique que el mantenimiento al Hardware sea de forma Preventiva **Pasa**			**DS13.5**	

FIRMA DE AUDITORÍA

Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información para Evaluar el Área de Hardware

PROCEDIMIENTOS	REFERENCIA P/T	HECHO POR	REF COBIT	OBSERVACIONES
Viene **Seguridad Lógica:** a) Si hay una Persona encargada del mantenimiento técnico del equipo o si existe un contrato con una compañía en particular y verifique: • Si cumplen con los requisitos mínimos para desempeñar su función, tales como: - Conocimiento de Equipos de Computo - Utilización de materiales adecuados para la limpieza del equipo. - Otros • Se cumplen con las fechas pactadas para el mantenimiento. b) Verifique las medidas de seguridad que se utilizan para el almacenamiento de la información y compruebe: • Que las unidades que se utilizan para almacenar la información son adecuados y tienen la capacidad necesaria para almacenar volúmenes importantes de información. • Que dichas unidades sean guardadas en un lugar seguro, que garantice su seguridad tanto física como de extravió. • Que procedimientos se siguen para poder obtener la información almacenada en las unidades magnéticas **Pasa**			**AI3.2;AI3.3** **DS12.1** **DS12.2** **DS12.1;DS5.11**	

FIRMA DE AUDITORÍA

Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información para Evaluar el Área de Hardware

PROCEDIMIENTOS	REFERENCIA P/T	HECHO POR	REF COBIT	OBSERVACIONES
Viene				
c) Cerciórese de las adquisiciones de recursos informáticos:			**AI5.1**	
☛ Verificar si existe un proveedor exclusivo para el suministro de equipo o si se requiere de cotizaciones de varios proveedores.			**AI5.2;AI5.3**	
☛ Solicitar los contratos de adquisición de maquinas y licencias de programas.			**AI5.2**	
☛ Verificar si al comprar un equipo cuenta con la garantía establecida en el contrato.			**AI5.2**	
☛ Verificar si al momento de adquirir equipo nuevo se tiene los controles para comprobar su buen estado físico.			**AI5.1**	
☛ Examine las pólizas de seguro y contrato de mantenimiento.			**AI5.1**	
☛ Determine el número de máquinas existentes y el uso para el cual están destinadas.				
Pasa				

Viene

FIRMA DE AUDITORÍA

Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información para Evaluar el Área de Hardware

ALCANCE:

CONCLUSION:_____
_____

Los objetivos señalados al principio de esta sección del programa de auditoria ¿Han sido alcanzados?
SI_____ NO_____ FIRMA_____
Explicación de porqué no hay conclusión_____

SUPERVISOR: _____ FECHA: _____
AUTORIZO: _____ FECHA: _____
AUDITOR: _____ FECHA: _____

FIRMA DE AUDITORÍA

Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información Relativo al Área del Software

Empresa:

Fecha de la Auditoria:

OBJETIVOS.

- Evaluar Establecer la existencia de Objetivos y políticas estratégicas con relación al área de soporte técnico
- Evaluar Los Criterios de administración del área de soporte técnico.
- Verificar Que el personal trabaja en base a manuales de aplicación.
- Comprobar La competencia del personal responsable del manejo del software.
- Evaluar : El nivel de segregación de funciones para el manejo de los software.

TECNICAS:

- Confirmación.
- Verificación.
- Revisión.
- Evaluación.
- Investigación.

No. PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Seguridad Lógica:				
1. Verificar si la empresa posee la licencia del Software. Y Verificar además que tipo de sistema se está utilizando (a la medida, o enlatado)			**AI5.4**	
2. Verificar claves de acceso de usuario y acceso al software, si las hay capture las pantallas hasta llegar a seleccionar la empresa. **Pasa**			**DS5.7**	

FIRMA DE AUDITORÍA

Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información para Evaluar el Área de Software

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene				
3. Comprobar de forma estratégica las claves de acceso al programa.			**DS5.7**	
4. Verificar el nivel de acceso de los usuarios con respecto a su posición y cargo de: a) Gerente General o presidente b) Gerente Administrativo o Gerente de RRHH c) Gerente de Producción u Operación d) Gerente de Ventas e) Gerente Financiero f) Contralor g) Auditoría interna h) Contador General i) Auxiliares j) otros externos relacionados			**DS5.1** **PO4.6** **PO4.10**	
5. Revisar el proceso estratégico de las actividades del usuario de los sistemas informáticos. A través de: -Claves de acceso. -Los Password de cada usuario. -Limitaciones y responsabilidades. -Manual del usuario.			**DS5.4** **DS5.7**	
6. Corroborar que la información generada por los programas sean fiables.			**DS11.1**	
Pasa				

FIRMA DE AUDITORÍA

Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información para Evaluar el Área de Software

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene				
7. Investigar las fechas de procesos de emisión de los comprobantes por el sistema, a través de la obtención y captura de pantallas y además la verificación al imprimir reportes la verificación de partidas, así como datos de reportes impresos.				
8. Corroborar que las cifras de los reportes del sistema sean veraces.				
Seguridad Física:				
9. Comprobar la existencia de un sistema de seguridad para el área de procesamiento de Datos.			**DS5.1**	
10. Evaluar la efectividad del sistema de seguridad física de las bases de datos.			**DS11.6;DS11.1**	
11. Evaluar el grado de organización y asignación de responsabilidades en la preparación de la información.				
12. Verificar, que todos los datos sean procesados con exactitud.			**DS11.1**	
Pasa				

FIRMA DE AUDITORÍA

Cliente:

Período:

Ref.:_____

Hecho Por:_____ Fecha:_____

Revisado Por:_____ Fecha:_____

Programa de Auditoria Estratégica a los Sistemas de Información para Evaluar el Área de Software

PROCEDIMIENTOS	HECHO POR	REF. P/T	REF COBIT	OBSERVACIONES
Viene 13. Verificar si existe la rotación de personal que utiliza los sistemas informáticos, para evitar las acciones Fraudulentas o manipulación de datos.			**DS5.3;PO7.8**	
14. Analizar la eficiencia con que se ejecutan los trabajos dentro del departamento de cómputo, tomando en cuenta equipo y operador, a través de inspección visual, y describa sus observaciones.				
15. Verificar la seguridad del ingreso a los programas o software mediante lo siguiente: • Examine los últimos reportes de uso de las maquinas.			**DS5.5**	

ALCANCE:

CONCLUSION:_____
_____

Los objetivos señalados al principio de esta sección del programa de auditoria ¿Han sido alcanzados?
SI_____ NO_____ FIRMA_____
Explicación de porqué no hay conclusión_____

SUPERVISOR: _____ FECHA: _____
AUTORIZO: _____ FECHA: _____
AUDITOR: _____ FECHA: _____

CAPÍTULO IV

4. CONCLUSIONES Y RECOMENDACIONES.

4.1. CONCLUSIONES.

1. Los profesionales de la contaduría pública, que se dedican al área de la auditoría, han prestado mayor énfasis a la auditoría de estados financieros.

2. La mayoría de profesionales de la contaduría pública poseen poca experiencia en el desarrollo de una auditoría a los sistemas de información, lo cual contribuye al escaso interés en actualizar los conocimientos en el área de Tecnología de Información y Comunicación (TIC).

3. Existe un conocimiento limitado departe del contador público, sobre la auditoría estratégica a los sistemas de información y sobre: lineamientos, importancia y beneficios potenciales entre otros que ésta proporciona

4. La mayoría de los contadores públicos no posee un adiestramiento adecuado en el ejercicio de la auditoría Estratégica a los sistemas de información

5. Los contadores públicos consideran que es importante y necesaria la implementación de un modelo de planeación de una auditoría estratégica a los sistemas de información; debido a que ésta contribuiría a mantener un parámetro para implementarlo en el desarrollo de su ejercicio profesional; de acuerdo a los requerimientos de las compañías
6. Existe poca actualización departe del contador público en las áreas tecnológicas debido a: el tiempo y dinero que debe invertir en las diferentes capacitaciones y al poco interés que demuestran los gremios de profesionales para la divulgación de nuevos conocimientos; tanto en ésta área cono a las nuevas tendencias de la auditoría.

4.2. RECOMENDACIONES.

1. Los profesionales de la contaduría pública dedicados al campo de la auditoría deben actualizar sus conocimientos en las áreas tecnológicas constantemente, con relación a los cambios eminentes que éstas experimentan; para enfrentar los retos que demanda el medio.

2. El Ministerio de Economía, mediante el consejo de vigilancia de la profesión de la contaduría pública y auditoría, debe mantener informado a los gremios de profesionales sobre los cambios en las nuevas tendencias de la auditoría; proporcionándoles los suficientes lineamientos que afectan a la profesión y manteniendo además una constante vigilancia sobre la aplicación de Normas Internacionales que de forma directa o indirectamente señalan el uso de la tecnología de la información como herramienta para el desarrollo del trabajo profesional.

3. Es necesario que los gremios de profesionales de la contaduría pública, presten mayor énfasis a los cambios constantes sobre las nuevas tendencias de la auditoría, y que promuevan capacitaciones para que el profesional se mantenga informado sobre estos cambios que ocurren; además para que se enfrenten al medio que lo demanda

4. Es importante e imprescindible que el profesional de la contaduría pública, ponga mayor esmero sobre los cambios constantes que ocurren en la Tecnología de la Información y Comunicación; los cuales afectan directamente el desarrollo de su trabajo: asimismo es necesario que el profesional de la contaduría pública se adiestre en el desarrollo de la auditoría estratégica a los sistemas de información, puesto que ésta es una herramienta la cual proporciona lineamientos para contribuir a disminuir el grado de riesgo inherente existente.

BIBLIOGRAFÍA

Aguirre Bautista, José de Jesús. Auditoría de las Tecnologías de Información, www.emprendedoresunam.com.mx

ASAMBLEA LEGISLATIVA DE LA REPÚBLICA EL SALVADOR. Decreto Legislativo No 230, Reformas DL 590 al 18 de Abril de 2008, Código Tributario

ASAMBLEA LEGISLATIVA DE LA REPÚBLICA EL SALVADOR. Decreto Legislativo No 130, Reformas DL 504 al 07 de de Diciembre de 2007, Ley de Impuesto Sobre la Renta

ASAMBLEA LEGISLATIVA DE LA REPÚBLICA EL SALVADOR, Decreto Legislativo No 296, Reformas DL 183 del 10 14 de Diciembre de 2006, Ley de Impuesto a la transferencia de Bienes Muebles y a la Prestación de servicios

ASAMBLEA LEGISLATIVA DE LA REPÚBLICA EL SALVADOR, Decreto Legislativo No 671, Reformas DL 641 del 12 de Junio de 2008, Código de Comercio

ASAMBLEA LEGISLATIVA DE LA REPÚBLICA EL SALVADOR, Decreto Legislativo No 1030, del 26 de Abril de 1997, Código Penal

ASAMBLEA LEGISLATIVA DE LA REPÚBLICA EL SALVADOR, Decreto Legislativo No 828, del 26 de Enero de 2000, Ley Reguladora del Ejercicio de la Contaduría.

Cohen ,Daniel, Sistemas de Información para los Negocios, 3º Edición, México

De Mantilla Blanco, Samuel Alberto "Control Interno, Estructura Conceptual Integrada (COSO)" Segunda Edición y Segunda Reimpresión, Colombia, Enero 2002.

De Mantilla Blanco, Samuel Alberto. "Auditoria Aseguramiento de información. Auditoria Estratégica"

De Callao Gastón, Susana. Hernández Ortega, Blanca. Jarne Jarne, José Ignacio. Laínez Gadea, José Antonio. Análisis Internacional de la calidad de la auditoria empresarial. Revista internacional Legis de contabilidad y auditoria No. 17. p 25 – 57

EFFY OZ, Administración de Sistemas de Información 2º Edición, México

Francisco J. Manso Coronado, Publicado en la revista Estrategia Financiera nº 97, 1994

José Joaquim Marques de Almeida. Revista Contaduría y Administración N203, Octubre-Diciembre 2001, México

Jovel Jovel, Roberto Carlos. Guía básica para elaborar trabajos de investigación, 1º Edición San Salvador El Salvador, Editorial e Imprenta Universitaria, 2008

J:C Daccach T. Planeación Estratégica de Tecnología Informática, www.deltaasesores.com/2004 (contacto por e-mail)

Milton José Narváez Sandino ; Proyecciones de las TICs en El Salvador para 2008; El Periódico Nuevo Enfoque, No.26 Segunda Época Primera Quincena de Marzo 2008

Rojas Soriano Raúl "Guía para realizar investigaciones sociales". Trigésima primera Edición, México, 2003.

Oscar Toro, MANUAL DE AUDITORÍA DE SISTEMAS,otoroc@cmet.net Centro de Formación Técnica DIEGO PORTALES, Concepción CHILE

XBRL Reporte financiero digital. Evolución de la contabilidad digital. www.perucontable.com /xbrl/modules/news2/article

INDICE DE ANEXOS

ANEXO 1

CUESTIONARIO

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONOMICAS

ESCUELA DE CONTADURIA PÚBLICA

CUESTIONARIO DE INVESTIGACION PARA TRABAJO DE GRADUACION

El presente cuestionario tiene como objeto recolectar información que permita conocer las necesidades de proporcionar al gremio de profesionales en Contaduría Pública, un Modelo de Planeación de una Auditoría Estratégica a los Sistemas de Información

OBJETIVO: recopilar la información sobre las áreas de conocimiento y especialización del Contador Público en lo relativo a la Auditoría Estratégica a los Sistemas de Información

DIRIGIDO A: a los profesionales en Contaduría inscritos en el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoria al 31 de Diciembre de 2007..

A.) ASPECTOS GENERALES

1. En su ejercicio profesional, ¿cuantos años de experiencia tiene en las áreas de:

   a.) Contabilidad ____Años

   b.) Auditoria Interna ____Años

   c.) Auditoria Externa ____Años

   d.) Auditoría de Sistemas Informáticos ____Años

   Otros.

   Especifique _____

2. ¿Que clases de auditoria conoce?

Financiera,	☐	Gubernamental	☐
Interna,	☐	Ambiental	☐
Sistemas,	☐	Forense	☐
Fiscal,	☐	De Gestión	☐
Administrativa	☐	Estratégica	☐

Otras, Especifique

_____

_____

3. ¿Conoce de algunos lineamientos para realizar la auditoría a los sistemas de información?

   SI ☐ NO ☐

4. ¿Considera que en el país existen suficientes lineamientos para asegurar la confiabilidad de los Estados Financieros de las entidades que utilizan sistemas de información?

   SI ☐ NO ☐

   ¿Porqué?_____

_____

5. ¿Cuál cree que ha sido la razón por la cual las empresas se ven en la necesidad de realizar algún tipo de auditoría a los sistemas de información?

   _____

_____

B.) ASPECTOS TECNICOS

6. ¿Conoce sobre la seguridad informática?

   SI ☐ NO ☐

7. Si su respuesta fue afirmativa, ¿Qué planes preventivos considera, que deben implementarse ante los errores del software para el resguardo de la información financiera?

_____

a) Mantenimiento preventivo periódicamente ☐

b) Backup ☐

c) programas auxiliares de retroalimentación para comparación de errores

d) Todos los anteriores ☐

Otros, Especifique

_____

_____

8. ¿cree usted que los seguros al software y al hardware son suficientes para el resguardo de la información financiera en caso de desastres?

   SI ☐ NO ☐

   ¿Porqué?_____

9. ¿Qué planes estratégicos de seguridad, cree usted que se deben aplicar a los Sistemas de Información en caso de desastres?

   a) Planes de contingencia que contemplen simulacros de desastres . ☐

   b) Focalizar áreas prioritarias ☐

   c) Sitios auxiliares de operación ☐

   Otros, Especifique

   _____

10. ¿Qué mediadas de seguridad cree que son las más importantes para resguardar la información financiera de los sistemas de información?

    a) Controles al Hardware ☐

    b) Controles al Soffware ☐

    d) Controles de Operación de Cómputo ☐

    e) Controles de seguridad de datos ☐

    f) Controles de implementación ☐

    g) Controles administrativos ☐

    h) Todos los anteriores ☐

    Otros, Especifique

    _____

11. ¿Qué tipo de conocimientos posee para desarrollar un plan de auditoría estratégica a los sistemas de información; el cual esta directamente ligado a la auditoría financiera?

    a) Mucho ☐

    b) Medio ☐

    c) Poco ☐

    d) Nada ☐

12. ¿porque medios adquirió estos conocimientos?

    a) Capacitaciones ☐
    b) Seminarios taller ☐
    c) En su ejercicio profesional ☐
    d) Libros ☐
    e) Boletines ☐
    f) Información intergremial ☐

    Otros, Especifique

    _____

13. ¿Ha realizado algún tipo de auditoria a los sistemas de información, en alguna entidad?

    SI ☐ NO ☐

    ¿Porqué?_____

14. ¿Cree usted que este tipo de auditoria le ayudaría a sustentar y garantizar mejor su opinión de los estados financieros?

    SI ☐ NO ☐

    ¿Porqué?_____

15. ¿Ha recibido recientemente algún tipo de capacitación relacionada con el tema de las TIC, que contribuya a mejorar su conocimiento para realizar un plan estratégico de auditoría a los Sistemas de Información?

    SI ☐ NO ☐

    Especifique_____

16. ¿Cree que es necesario que el contador público actualice sus conocimientos constantemente de acuerdo a las demandas del medio y los avances en la Tecnología de la Información y Comunicación (TIC)?

    SI ☐ NO ☐

¿Porqué?_____

17. ¿Considera que implementar un modelo de planeación de Auditoria Estratégica es rentable y útil para la compañía que lo utilice?

    SI ☐ NO ☐

    ¿Porqué?_____

18. ¿Que tipo de medidas de control implementa al realizar una auditoría considerando los riesgos existentes en el uso de TIC?

    Controles Preventivas ☐

    Controles Defectivas ☐

    Controles Correctivos. ☐

    Otros, Especifique

    _____

19. ¿Considera que las medidas implementadas actualmente para el desarrollo de las auditorías son suficientes; partiendo del hecho que la mayoría de entidades utilizan sistemas de información para el proceso y almacenamiento de datos?

    SI ☐ NO ☐

    ¿Porqué?_____

20. ¿Considera usted que los gremios de profesionales toman un papel protagónico en cuanto a la difusión de nuevos conocimientos sobre la profesión contable?

    SI ☐ NO ☐

    ¿Porqué?_____

21. ¿Cree usted que es necesario la creación de un modelo de planeación de auditoria estratégica a los sistemas de información que sirva de parámetro para poder implementarlo en cualquier tipo de empresa?

    SI ☐ NO ☐

    ¿Porqué?_____

ANEXO 2

TABULACIÓN Y ANÁLISIS DE LA INFORMACIÓN

PREGUNTA Nº1

En su ejercicio profesional, ¿cuantos años de experiencia tiene en las áreas de:

e.) Contabilidad _____Años

f.) Auditoria Interna _____Años

g.) Auditoria Externa _____Años

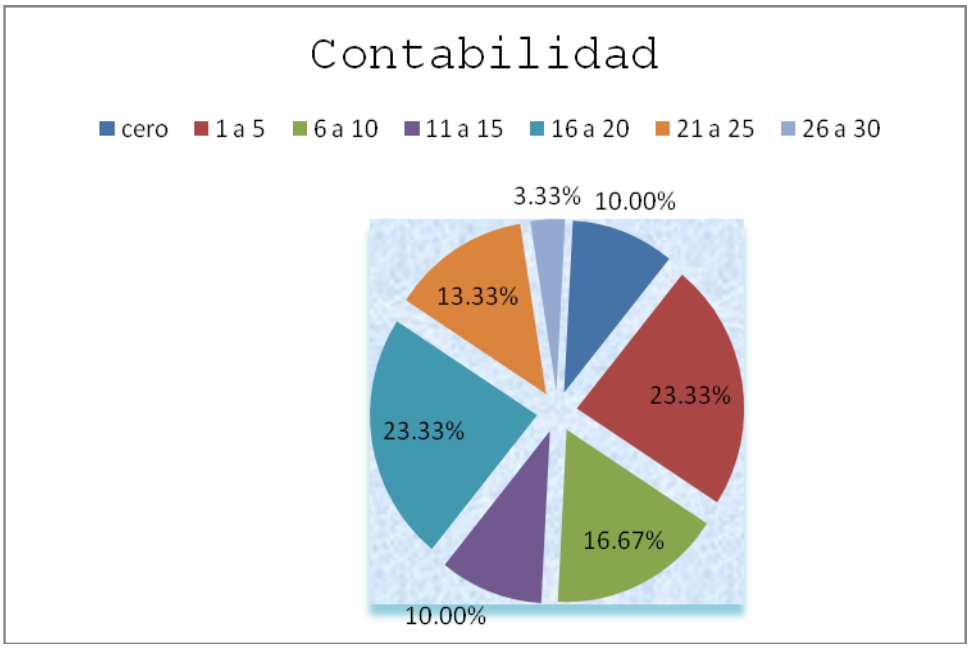
h.) Auditoría de Sistemas Informáticos _____Años

Otros.

Especifique _____

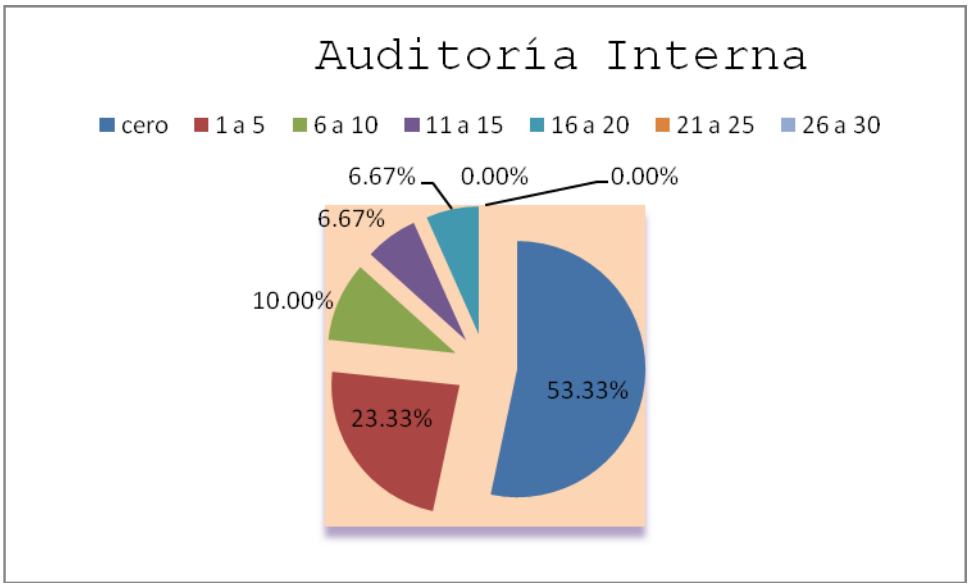
Objetivos: Conocer la experiencia profesional de los contadores públicos

Alternativa	Rango en Años	Frecuencia Absoluta	Frecuencia Relativa
Contabilidad	cero	6	10.00%
	1 a 5	14	23.33%
	6 a 10	10	16.67%
	11 a 15	6	10.00%
	16 a 20	14	23.33%
	21 a 25	8	13.33%
	26 a 30	2	3.33%
Total		60	100.00%



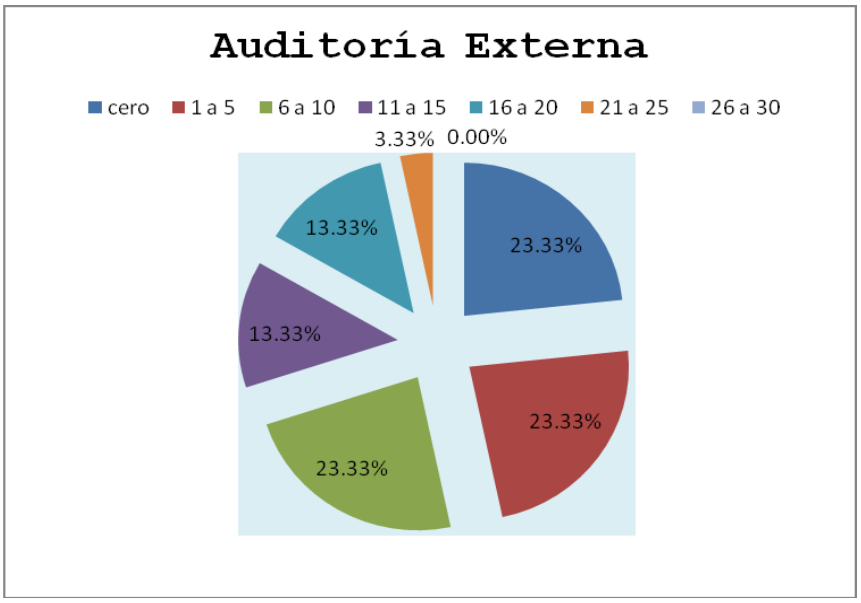
ANÁLISIS. Como se observa en la tabla anterior, de los encuestados el 23.33% poseen experiencia en el área contable entre 1 a 5 y entre 16- y 20 años, y tan solo dos tienen experiencia entre 26 a 30 años, lo que representa un 3.33% de la muestra.

Alternativa	Rango en Años	Frecuencia Absoluta	Frecuencia Relativa
Auditoría Interna	cero	32	53.33%
	1 a 5	14	23.33%
	6 a 10	6	10.00%
	11 a 15	4	6.67%
	16 a 20	4	6.67%
	21 a 25	0	0.00%
	26 a 30	0	0.00%
Total		60	100.00%



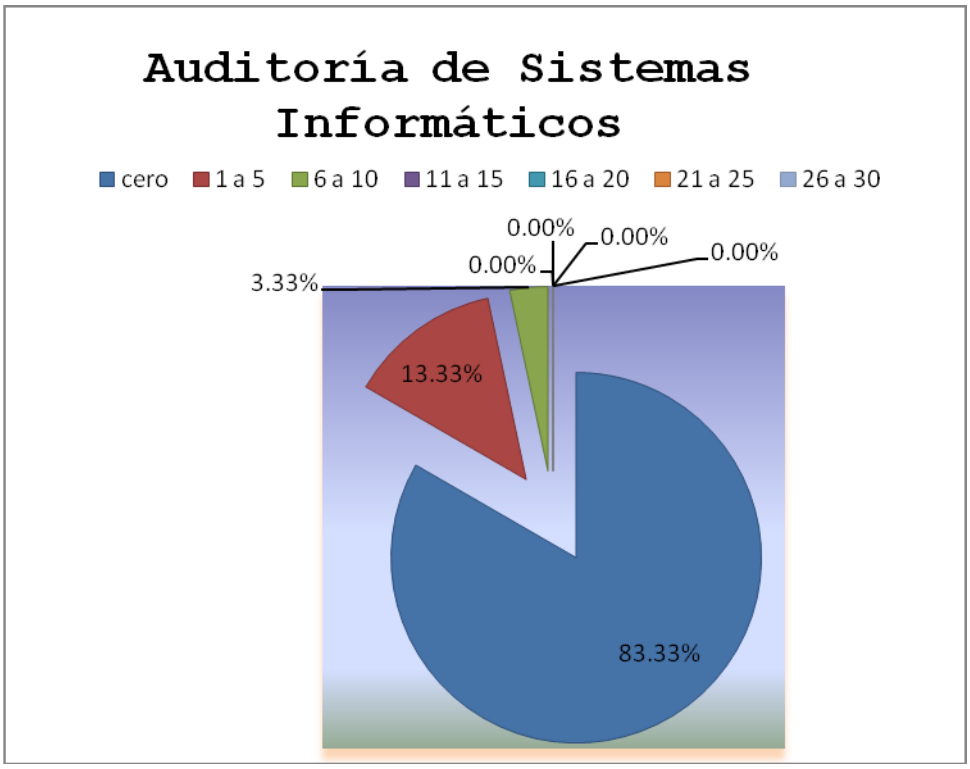
La tabla anterior nos muestra un porcentaje alto en la falta de experiencia departe de los profecionales en el area de Auditoria Interna siendo un 53.33% los que no tienen ninguna experiencia en dicha area, y solamente un 23.33% son los profecionales que estan en el rango de experiencia de 1-5 años.

Alternativa	Rango en Años	Frecuencia Absoluta	Frecuencia Relativa
Auditoría Externa	cero	14	23.33%
	1 a 5	14	23.33%
	6 a 10	14	23.33%
	11 a 15	8	13.33%
	16 a 20	8	13.33%
	21 a 25	2	3.33%
	26 a 30	0	0.00%
		60	100.00%



Como se observa en la tabla anterior un 46.66% de los profesionales encuestados poseen experiencia en el área de auditoría externa entre 1 a 10 años (14 de los que contestaron a la encuesta el rango establecido entre 1 a 5 años y 14 respondieron entre 6 a 10 años) existe un porcentaje del 23.33% de los profesionales encuestados que no posee ninguna experiencia en ésta área. Dos de los encuestado afirmaron poseer experiencia entre 21 a 25 años por lo que representa tan sólo el 3.33% .

Alternativa	Rango en Años	Frecuencia Absoluta	Frecuencia Relativa
Auditoría de Sistemas Informáticos	cero	50	83.33%
	1 a 5	8	13.33%
	6 a 10	2	3.33%
	11 a 15	0	0.00%
	16 a 20	0	0.00%
	21 a 25	0	0.00%
	26 a 30	0	0.00%
Total		60	100.00%



De acuerdo al gráfico anterior el 83.33 % de los profesionales encuestados no tiene ninguna experiencia en el área de Auditoría de Sistemas Informáticos y tan sólo un 13.3% inician sus conocimiento poseyendo experiencia entre 1-5 años.

PREGUNTA No 2

¿Que clases de auditoria conoce?

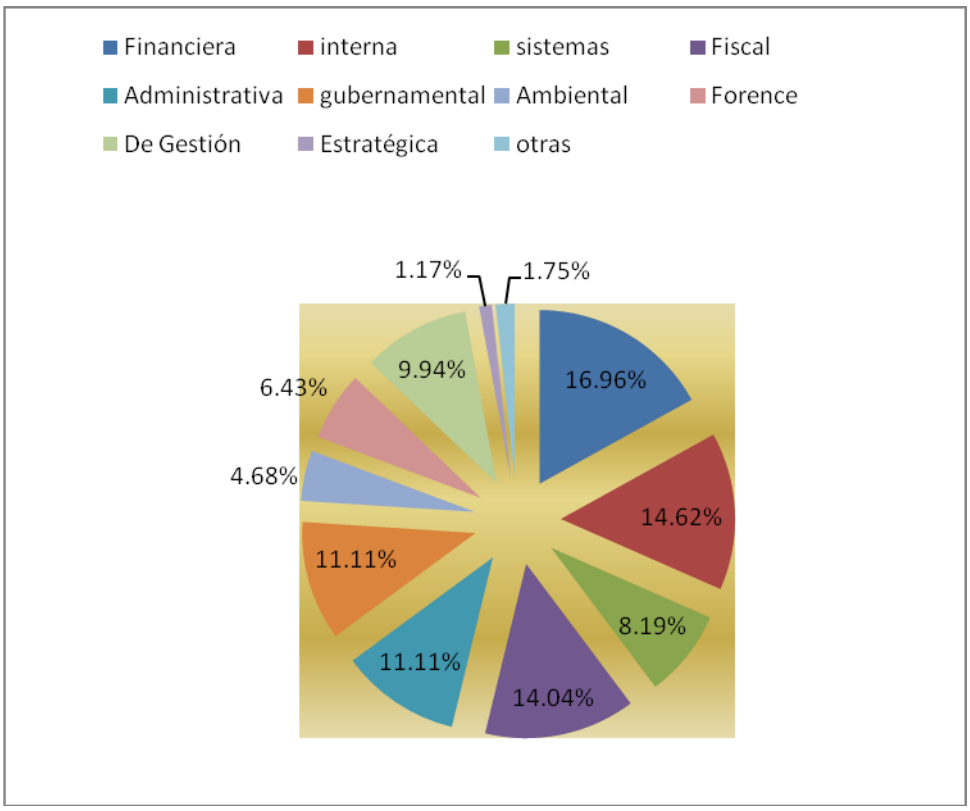
Financiera,	☐	Gubernamental	☐
Interna,	☐	Ambiental	☐
Sistemas,	☐	Forense	☐
Fiscal,	☐	De Gestión	☐
Administrativa	☐	Estratégica	☐

Otras, Especifique _____

_____

Objetivo: Identificar los tipos de auditorías que conoce el Profesional de la Contaduría Pública

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Financiera	58	96.67%
interna	50	83.33%
sistemas	28	46.67%
Fiscal	48	80.00%
Administrativa	38	63.33%
gubernamental	38	63.33%
Ambiental	16	26.67%
Forense	22	36.67%
De Gestión	34	56.67%
Estratégica	4	6.67%
otras	6	10.00%



La tambla anterior muestra que 58 de los 60 encuestados afirmaron conocer la Auditoría de Estados Financieros 50 conocen la auditoría interna, 48 de los encuestados conocen la auditoría fiscal, 38 de los encuestados conocen de la auditoría administrativa y gubernamental y tan sólo 4 de los encuestados afirmaron conocer la auditoría Estratégica lo cual representa el 6.67%

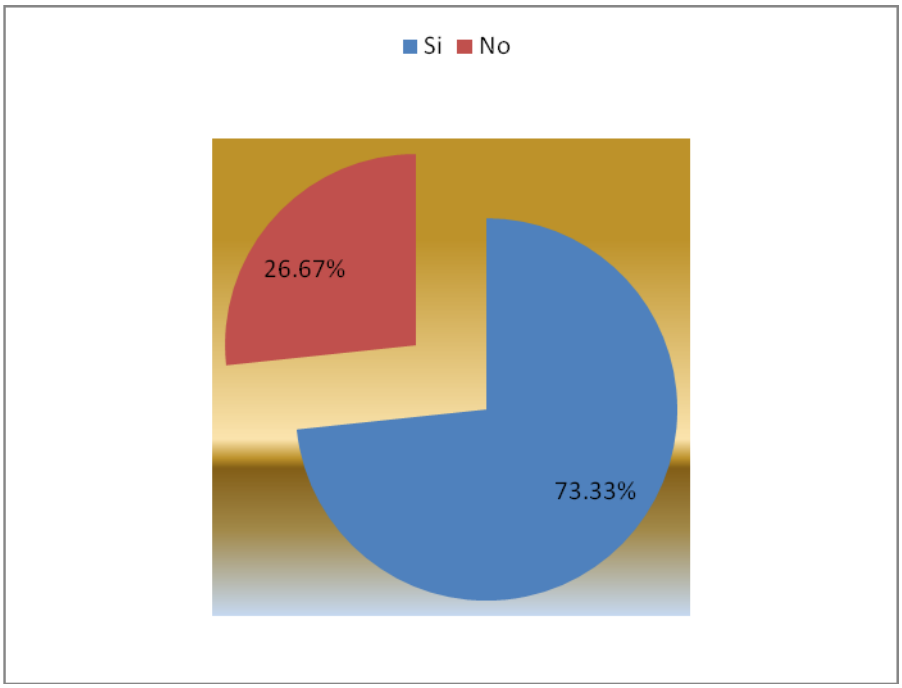
PREGUNTA No 3

¿Conoce de algunos lineamientos para realizar la auditoría a los sistemas de información?

SI ☐ NO ☐

Objetivo: Medir el grado de conocimiento que posee el Contador Público sobre lineamientos para realizar la auditoría a los Sistemas de Información

Alternativas	Frecuencia Absoluta	Frecuencia Relativa
Si	44	73.33%
No	16	26.67%
Total	60	100.00%



ANALISIS: De acuerdo al grafico anterior el 73.33% de los encuestados conocen de algunos lineamientos para realizar auditoría a los Sistemas de Información

PREGUNTA No 4

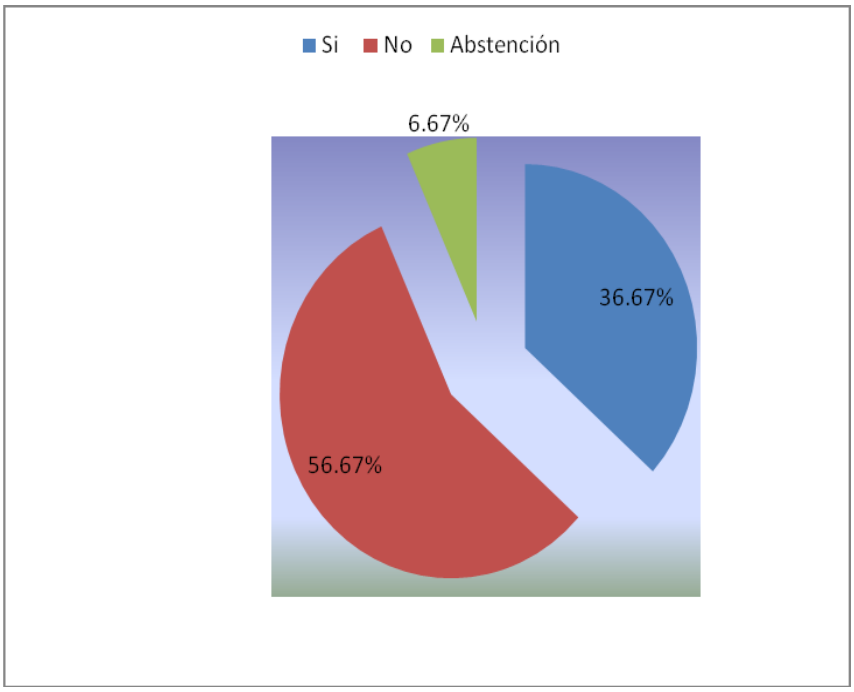
¿Considera que en el país existen suficientes lineamientos para asegurar la confiabilidad de los Estados Financieros de las entidades que utilizan sistemas de información?

SI ☐ NO ☐

¿Porqué?_____

Objetivo: Medir la opinión del Contador Público sobre la existencia de lineamientos para asegurar la confiabilidad de los Estados financieros, de las entidades que utilizan Sistemas de Información

Alternativas	Frecuencia Absoluta	Frecuencia Relativa
Si	22	36.67%
No	34	56.67%
Abstención	4	6.67%
Total	60	100.00%



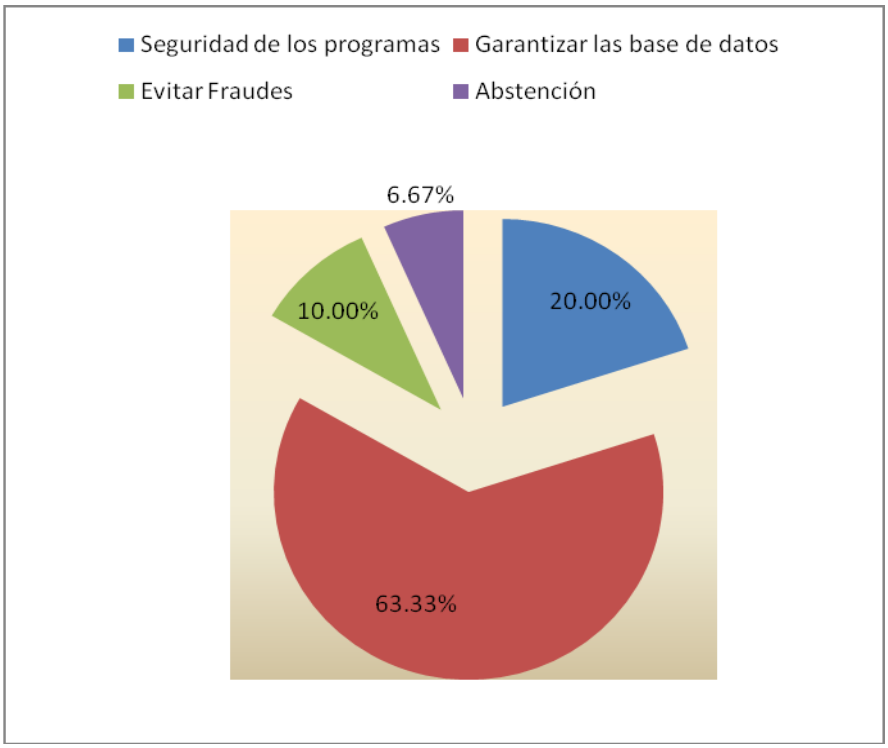
ANALISIS: De acuerdo a la tabla anterior el 56.67% de los profesionales encuestados consideran que en el país no existen suficientes lineamientos para asegurar la confiabilidad de los estados financieros, frente a un 36.67% que consideran que si existen.

PREGUNTA No 5

¿Cuál cree que ha sido la razón por la cual las empresas se ven en la necesidad de realizar algún tipo de auditoría a los sistemas de información?

Objetivo: Conocer la opinión del Contador Público sobre la razón por la cual las empresas se ven en la necesidad de realizar algún tipo de auditoría a los Sistemas de Información.

Alternativas	Frecuencia Absoluta	Frecuencia Relativa
Seguridad de los programas	12	20.00%
Garantizar las base de datos	38	63.33%
Evitar Fraudes	6	10.00%
Abstención	4	6.67%
Total	60	100.00%



ANALISIS: De acuerdo a la tabla anterior el 63.33% de los encuestados consideran que garantizar la base de datos es la razón por la cual las empresas se ven en la necesidad de realizar algún tipo de auditoría a los Sistemas de Información, sin embargo un 20.00% consideran que se debe a la seguridad de los programas.

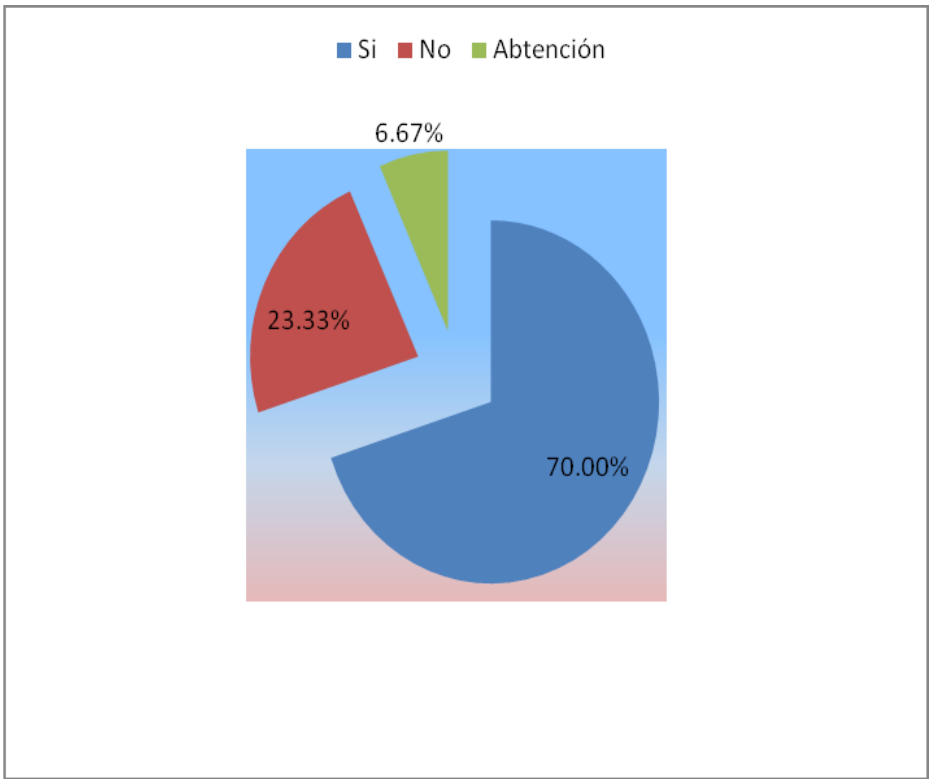
PREGUNTA No 6

¿Conoce sobre la seguridad informática?

SI ☐ NO ☐

Objetivo: Medir el grado de conocimiento que posee el contador Público sobre la seguridad Informática

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Si	42	70.00%
No	14	23.33%
Abstención	4	6.67%
Total	60	100.00%



ANALISIS: En base al gráfico anterior un 70.00% de los encuestados, afirmaron conocer de la seguridad informática, frente a un 23.33% que dijeron no conocer sobre esta; cuatro de los encuestados que representa el 6.67% se abstuvieron de responder a dicha pregunta

PREGUNTA No 7

Si su respuesta fue afirmativa, ¿Qué planes preventivos considera, que deben implementarse ante los errores del software para el resguardo de la información financiera?

a) Mantenimiento preventivo periódicamente ☐

b) Backup ☐

c) programas auxiliares de retroalimentación para comparación de errores

d) Todos los anteriores ☐

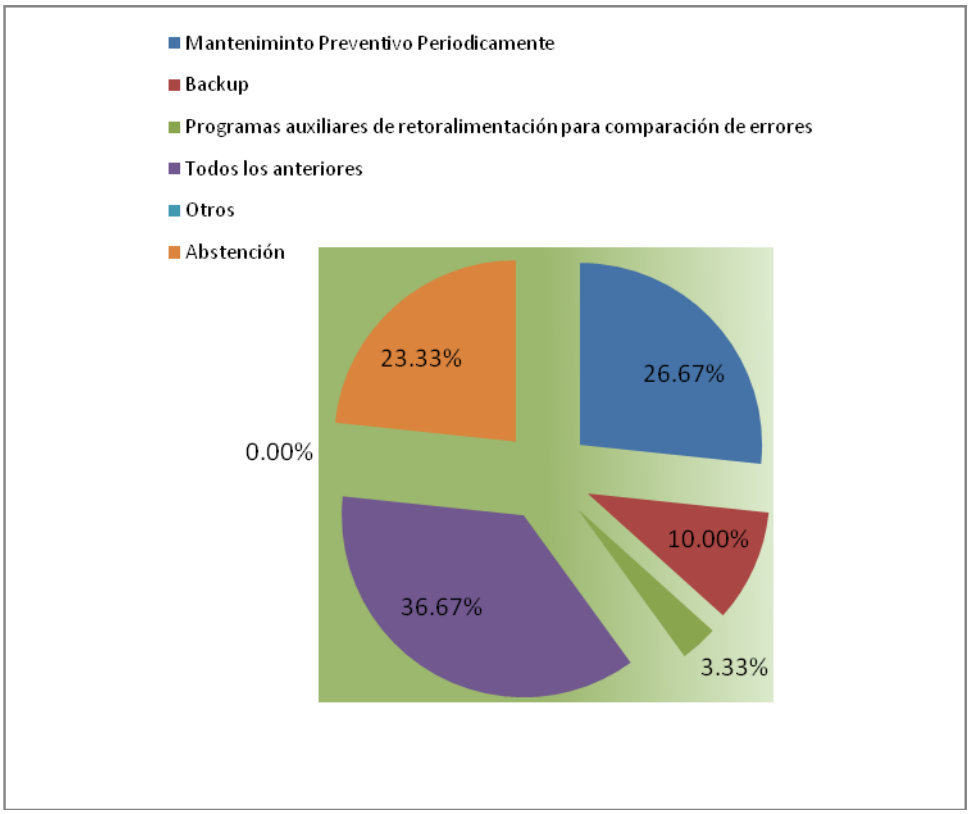
Otros, Especifique

_____

_____

Objetivo: Conocer la opinión del Contador Público sobre que tipo de planes preventivos deben implementarse ante los errores del software para resguardar la información financiera.

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Mantenimiento Preventivo Periódicamente	16	26.67%
Backup	6	10.00%
Programas auxiliares de retroalimentación para comparación de errores	2	3.33%
Todos los anteriores	22	36.67%
Otros	0	0.00%
Abstención	14	23.33%
Total	60	100.00%



ANALISIS: De acuerdo a la tabla anterior un 36.67% de los encuestados, consideran que el tipo de planes preventivos que se deben implementar ante los errores del software para el resguardo de la información son: Mantenimiento preventivo periódicamente, backup, programas auxiliares de retroalimentación para comparación de errores ; por otra parte un 26.67% opino que son suficientes los mantenimientos preventivos para el resguardo de la información. El 23.33% son los que se abstuvieron a responder a la pregunta y representan los 14 encuestados que en la interrogante anterior respondieron negativamente.

PREGUNTA No 8

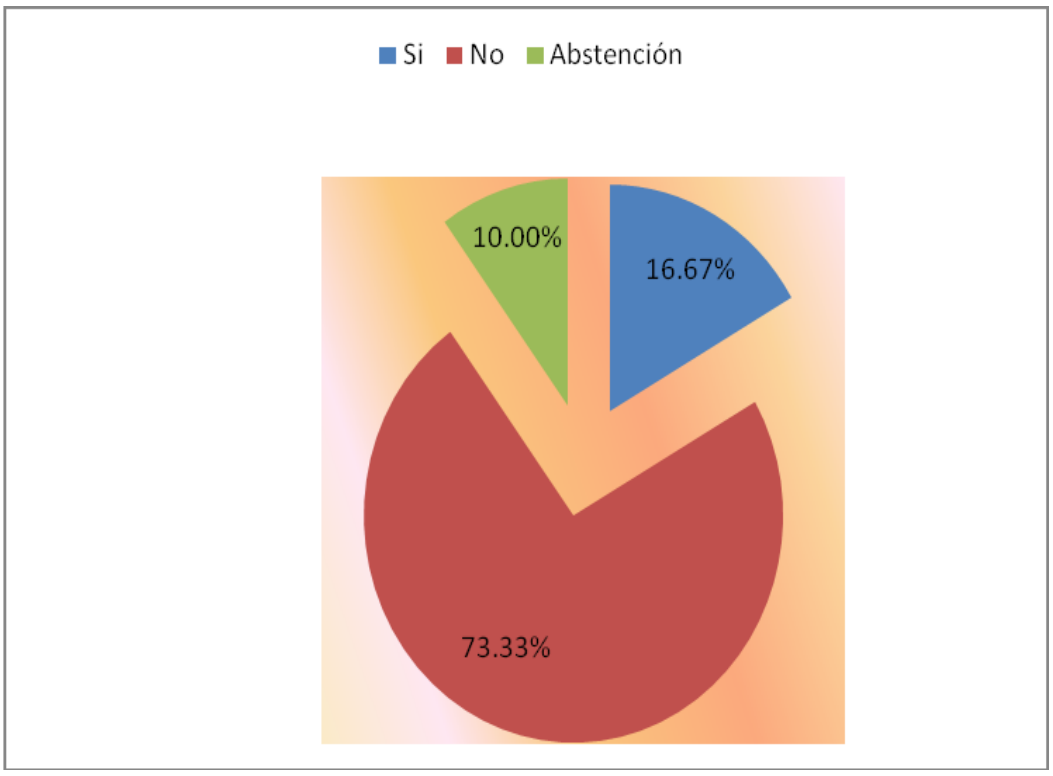
¿Cree usted que los seguros al software y al hardware son suficientes para el resguardo de la información financiera en caso de desastres?

SI ☐ NO ☐

¿Porqué?_____

Objetivo: Conocer la opinión del Contador Público sobre que si los seguros al software y al hardware son suficientes para el resguardo de la información financiera

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Si	10	16.67%
No	44	73.33%
Abstención	6	10.00%
Total	60	100.00%



ANALISIS: De acuerdo a la tabla anterior un 73.33% de los encuestados consideran que los seguros al Software y a Hardware no son suficientes para el resguardo de la Información financiera en caso de ocurrir algún desastre; sin embargo un 16.67% cree que si lo son.

PREGUNTA No 9

¿Qué planes estratégicos de seguridad, cree usted que se deben aplicar a los Sistemas de Información en caso de desastres?

a) Planes de contingencia que contemplen simulacros de desastres . ☐

b) Focalizar áreas prioritarias ☐

c) Sitios auxiliares de operación ☐

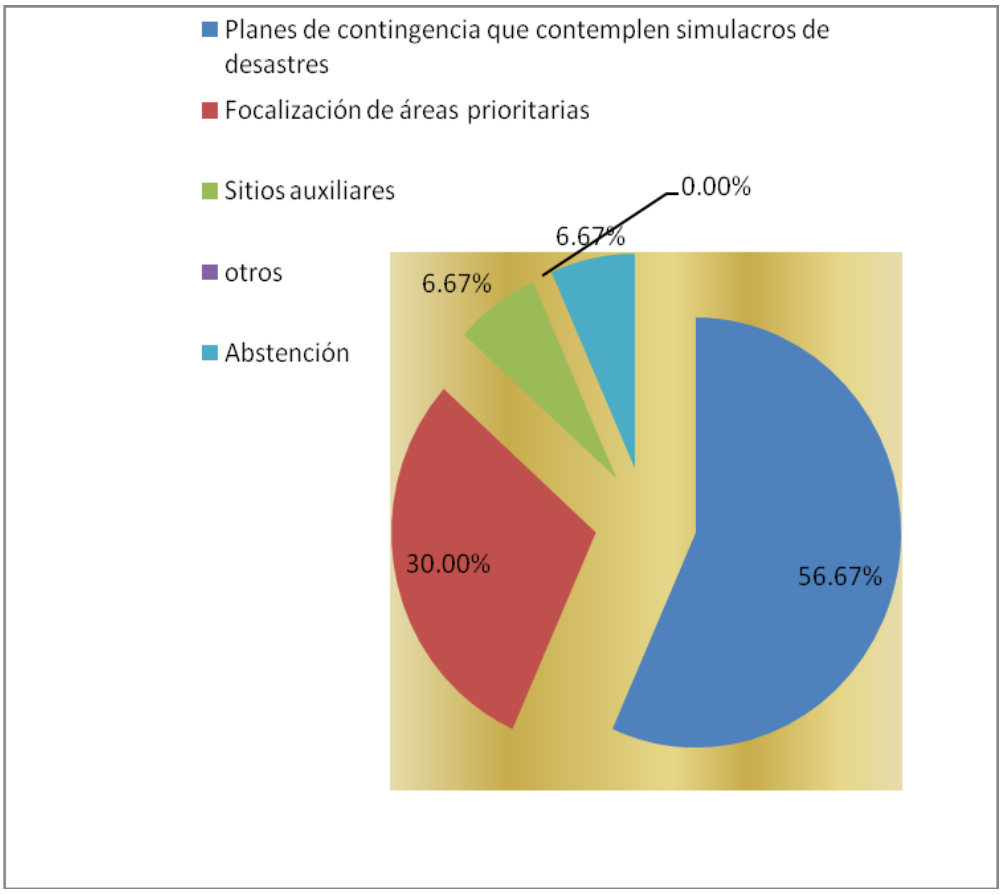
Otros, Especifique

_____

_____

Objetivo: Identificar los Planes Estratégicos de seguridad que considera el Contador Público encuestado que se deben aplicar en los casos de desastres.

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Planes de contingencia que contemplen simulacros de desastres	34	56.67%
Focalización de áreas prioritarias	18	30.00%
Sitios auxiliares	4	6.67%
otros	0	0.00%
Abstención	4	6.67%
	60	100.00%



ANALISIS: De acuerdo a la grafica anterior un 56.67% de los profesionales encuestados, consideran que el plan estratégico de seguridad que se debe aplicar a los sistemas de información son los que contemplen simulacros de desastres; un 30.00% de los encuestados consideran que el plan estratégico, debe estar focalizado en áreas prioritarias de la empresa.

PREGUNTA No 10

¿Qué medidas de seguridad cree que son las más importantes para resguardar la información financiera de los sistemas de información?

a) Controles al Hardware ☐

b) Controles al Soffware ☐

d) Controles de Operación de Cómputo ☐

e) Controles de seguridad de datos ☐

f) Controles de implementación ☐

g) Controles administrativos ☐

h) Todos los anteriores ☐

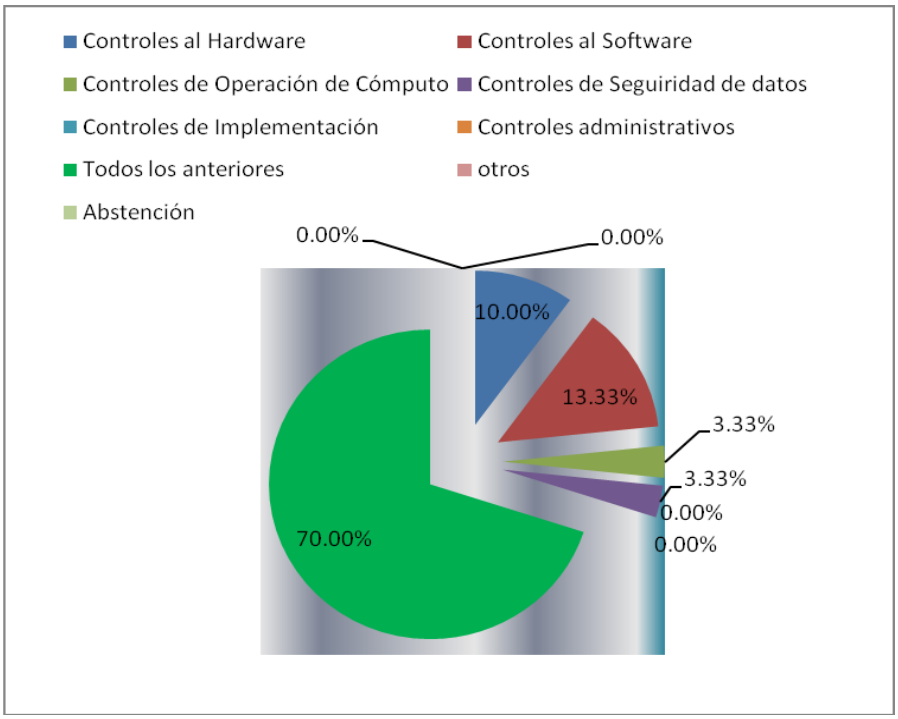
Otros, Especifique

_____

_____

Objetivo: Identificar las medidas de seguridad que considera importantes el Contador Público, para el resguardo de la información financiera de los Sistemas de Información

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Controles al Hardware	6	10.00%
Controles al Software	8	13.33%
Controles de Operación de Cómputo	2	3.33%
Controles de Seguridad de datos	2	3.33%
Controles de Implementación	0	0.00%
Controles administrativos	0	0.00%
Todos los anteriores	42	70.00%
otros	0	0.00%
Abstención	0	0.00%
Total	60	100.00%



ANALISIS: De acuerdo a la grafica anterior un 70.00% de los profesionales encuestados, cree que las medidas de seguridad que se deben implementar para el resguardo de la información financiera en los sistemas de información son: Controles al Hardware, al Software, controles de operación de cómputo, controles de seguridad de datos, controles de implementación, controles administrativo; mientras que un 13.33% considera que los controles al software es la única medida de seguridad que se debe implementar para el resguardo de la información financiera.

PREGUNTA No 11

¿Qué tipo de conocimientos posee para desarrollar un plan de auditoría estratégica a los sistemas de información; el cual esta directamente ligado a la auditoría financiera?

a) Mucho ☐

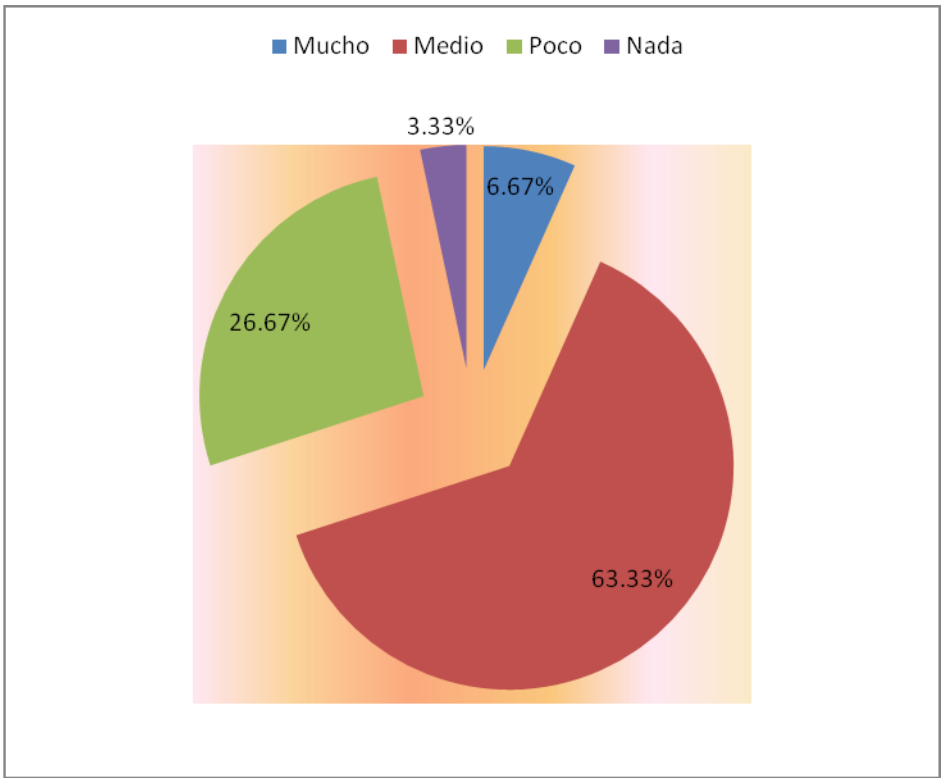
b) Medio ☐

c) Poco ☐

d) Nada ☐

Objetivo: Medir el nivel de conocimiento, que posee el contador Público para desarrollar una planeación de auditoría estratégica a los Sistemas de Información

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Mucho	4	6.67%
Medio	38	63.33%
Poco	16	26.67%
Nada	2	3.33%
Total	60	100.00%



ANALISIS: De acuerdo a la tabla anterior un 63.33% posee un conocimiento medio para desarrollar una planeación de una auditoría estratégica a los sistemas de información; mientras que un 16.67% afirma poseer poco conocimiento para el desarrollo de un plan de este tipo de auditoría, tan solo un 3.33% afirma no poseer ningún conocimiento.

PREGUNTA No 12

¿Porque medios adquirió estos conocimientos?

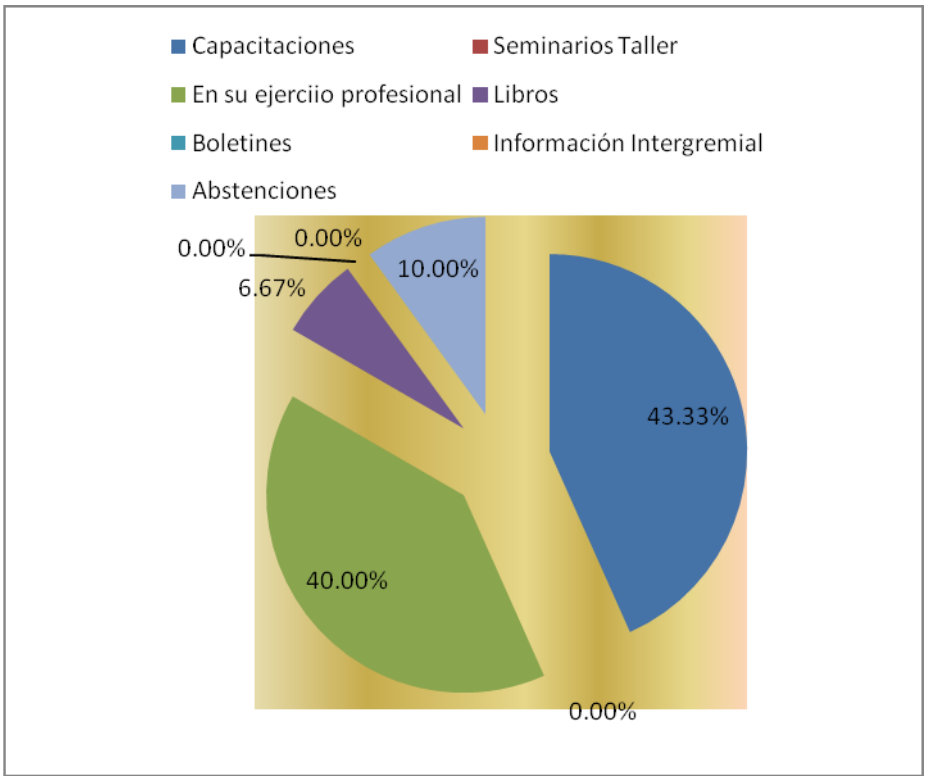
a) Capacitaciones ☐
b) Seminarios taller ☐
c) En su ejercicio profesional ☐
d) Libros ☐
e) Boletines ☐
f) Información intergremial ☐

Otros, Especifique

_____

Objetivo: Identificar los medios por los cuales adquirió los conocimientos el profesional para desarrollar una planeación de auditoría estratégica a los Sistemas de Información.

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Capacitaciones	26	43.33%
Seminarios Taller	0	0.00%
En su ejercicio profesional	24	40.00%
Libros	4	6.67%
Boletines	0	0.00%
Información Intergremial	0	0.00%
Abstenciones	6	10.00%
Total	60	100.00%



ANALISIS: De acuerdo a la tabla anterior un 43.33% de los profesionales encuestados afirma haber adquirido los conocimientos para desarrollar un plan de auditoría estratégica a los sistemas de información en capacitaciones; un 40.00% en el ejercicio profesional y un 6.67 afirma haberlo adquirido en libros.

PREGUNTA No 13

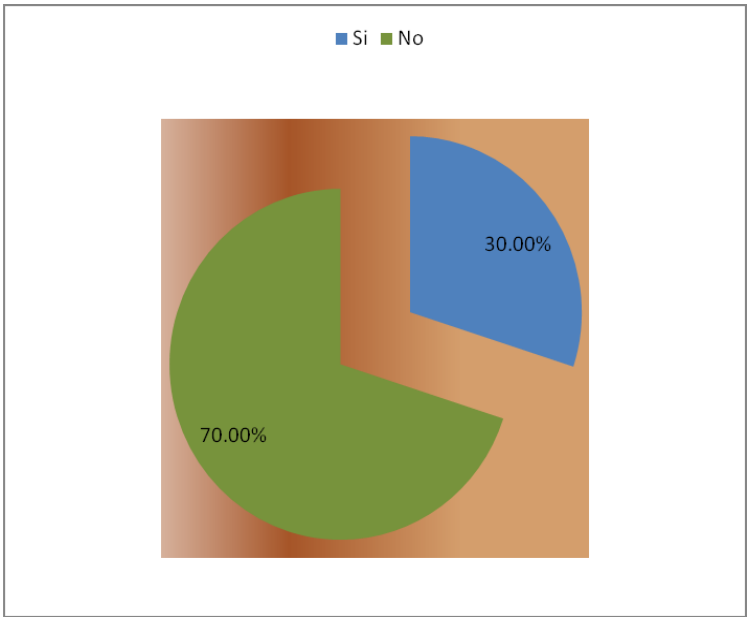
¿Ha realizado algún tipo de auditoria a los sistemas de información, en alguna entidad?

SI ☐ NO ☐

¿Porqué?_____

Objetivo: Conocer el nivel de experiencia que posee el auditor, sobre el desarrollo de auditoría de Sistemas.

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Si	18	30.00%
No	42	70.00%
Total	60	100.00%



ANALISIS: De acuerdo a la tabla anterior un 70.00% de los profesionales encuestados afirma no haber realizado una auditoría de sistemas; sin embargo un 30% afirma haber realizado algún tipo de auditoría de sistemas.

PREGUNTA No 14

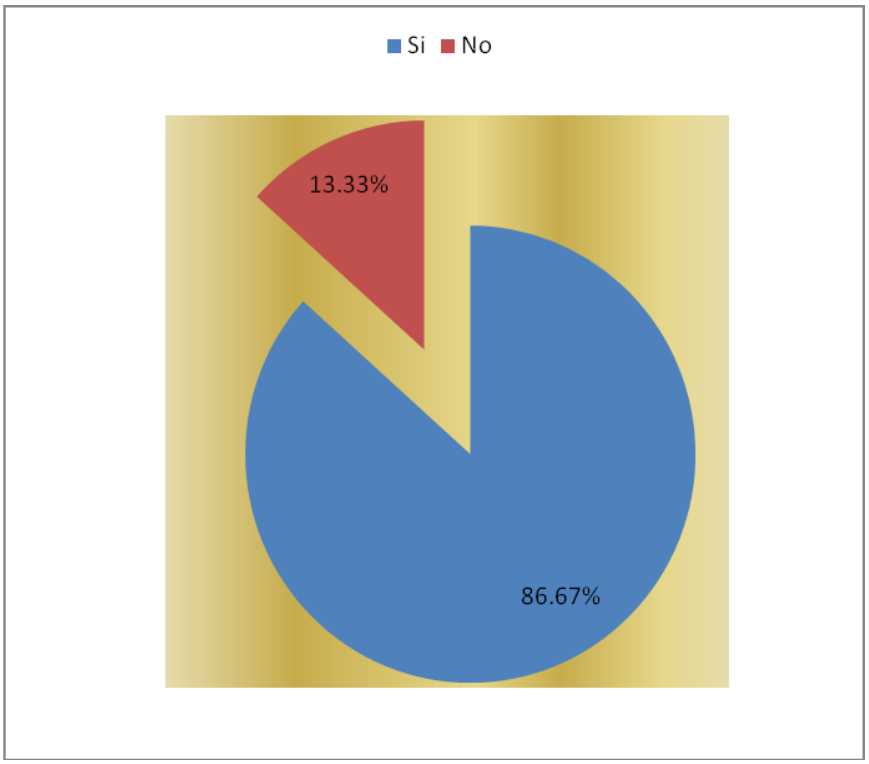
¿Cree usted que este tipo de auditoria le ayudaría a sustentar y garantizar mejor su opinión de los estados financieros?

SI ☐ NO ☐

¿Porqué?_____

Objetivo: Conocer la opinión del auditor con relación a que si la auditoría de Sistemas, contribuye a sustentar mejor su opinión de los estados financieros auditados.

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Si	52	86.67%
No	8	13.33%
Total	60	100.00%



ANALISIS: De acuerdo a la tabla anterior un 86.67% considera que la auditoría a los sistemas de información contribuiría a sustentar mejor su opinión de los estados financieros; mientras que un 13.33% considera que no ayuda a sustentar la opinión sobre los estados financieros. Uno de los encuestados de los que contestaron negativamente afirmó que existen Normas y eso no cambia la opinión del auditor.

PREGUNTA No 15

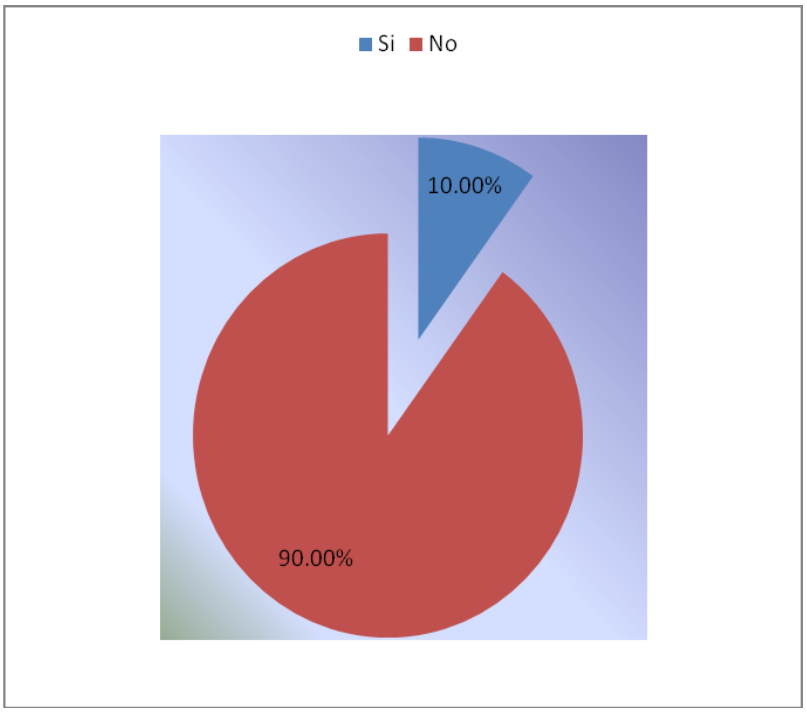
¿Ha recibido recientemente algún tipo de capacitación relacionada con el tema de las TIC, que contribuya a mejorar su conocimiento para realizar un plan estratégico de auditoría a los Sistemas de Información?

SI ☐ NO ☐

Especifique_____

Objetivo: Identificar el nivel de capacitaciones que recibe el Contador Público encuestado con relación a los cambios constantes en las Tecnologías de la Información y Comunicación, para enriquecer los conocimientos sobre la auditoría estratégica a los Sistemas de Información

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Si	6	10.00%
No	54	90.00%
Total	60	100.00%



ANALISIS: De acuerdo a la gráfica anterior un 90.00% afirma no haber recibido recientemente algún tipo de capacitaciones relacionadas al tema de las TIC, la cual ayudaría a enriquecer sus conocimientos sobre la auditoría estratégica a los sistemas de información; solamente el 10.00% de los encuestados afirmaron si haber recibido algún tipo de capacitaciones relacionadas con éste tema.

PREGUNTA No 16

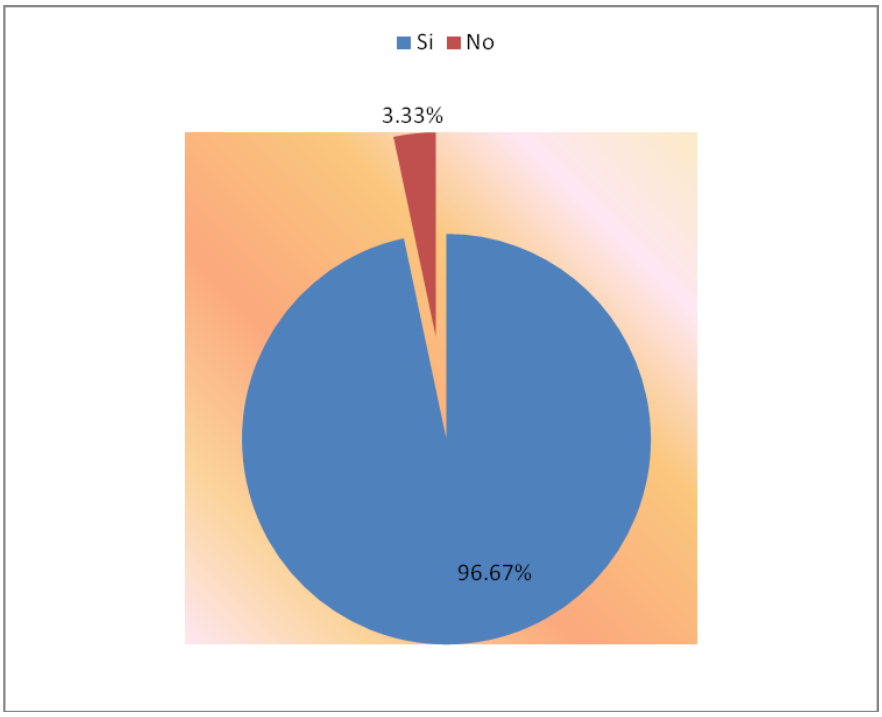
¿Cree que es necesario que el contador público actualice sus conocimientos constantemente de acuerdo a las demandas del medio y los avances en la Tecnología de la Información y Comunicación (TIC)?

SI ☐ NO ☐

¿Porqué?_____

Objetivo: conocer la opinión del Contador Público en relación, a si es importante la actualización de conocimientos de acuerdo a las demandas del medio y los avances en las TIC.

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Si	58	96.67%
No	2	3.33%
Total	60	100.00%



ANALISIS: De acuerdo a la gráfica anterior un 96.67% de los encuestados afirman que si es importante la actualización de los conocimientos de acuerdo a las demandas del medio y a los avances tecnológicos; dos de los encuestados los cuales representan el 3.33% consideran que no son importantes; pues afirman que la auditoría es con base a documentos y no de tipo magnética.

PREGUNTA No 17

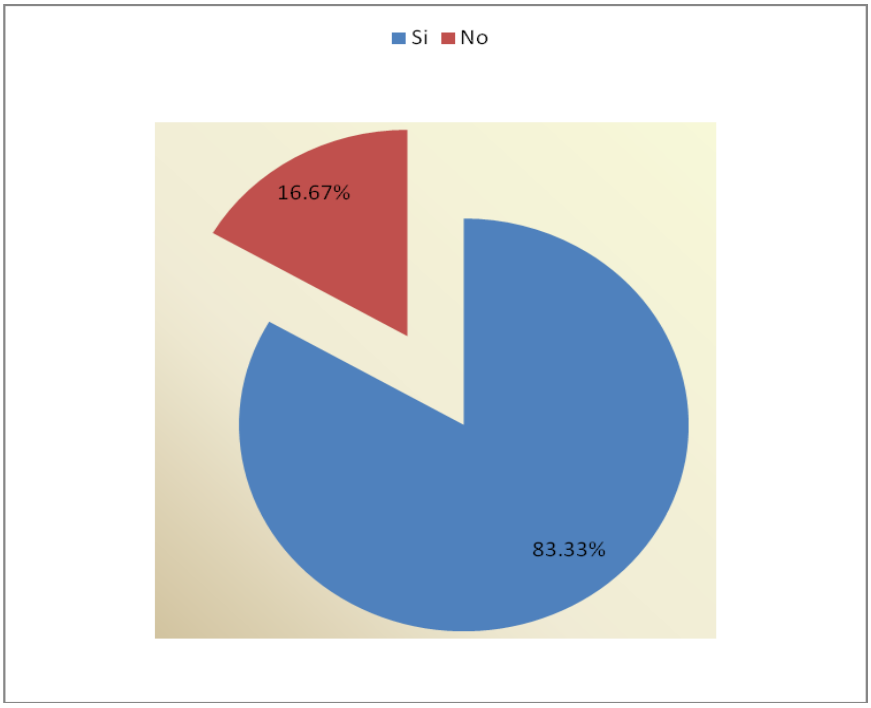
¿Considera que implementar un modelo de planeación de Auditoria Estratégica es rentable y útil para la compañía que lo utilice?

SI ☐ NO ☐

¿Porqué?_____

Objetivo: conocer la opinión del Contador Público en relación, a si considera que es rentable y útil para las empresas implementar una auditoría estratégica a los sistemas de información

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Si	50	83.33%
No	10	16.67%
Total	60	100.00%



ANALISIS: De acuerdo a la gráfica anterior un 86.33% de los encuestados consideran que si es rentable y útil implementar un plan de auditoría estratégica para las empresas que lo utilicen; por tora parte un 16.67% consideran que no lo es.

PREGUNTA No 18

¿Que tipo de medidas de control implementa al realizar una auditoría considerando los riesgos existentes en el uso de TIC?

Controles Preventivas ☐

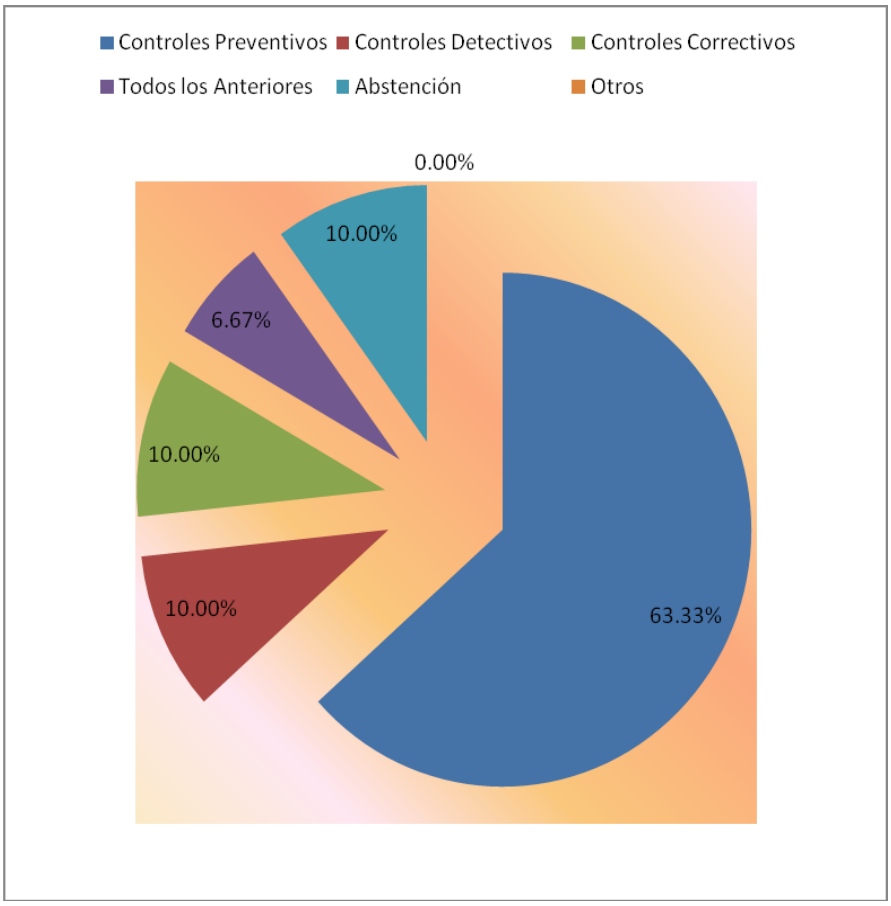
Controles Defectivas ☐

Controles Correctivos. ☐

Otros, Especifique

Objetivo: Identificar las medidas de control implementadas por el Contador Público encuestado considerando los riegos que existen con el uso de TIC.

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Controles Preventivos	38	63.33%
Controles Detectivos	6	10.00%
Controles Correctivos	6	10.00%
Todos los Anteriores	4	6.67%
Abstención	6	10.00%
Otros	0	0.00%
Total	60	100.00%



ANALISIS: De acuerdo a la tabla anterior un 63.33% de los encuestados afirman implementar controles preventivos en al realizar una auditoría tomando en cuenta los riesgos existentes en el uso de TIC`s; un 6.67% afirman implementar controles preventivos, controles detectivos y controles correctivos al realizar una auditoría

PREGUNTA No 19

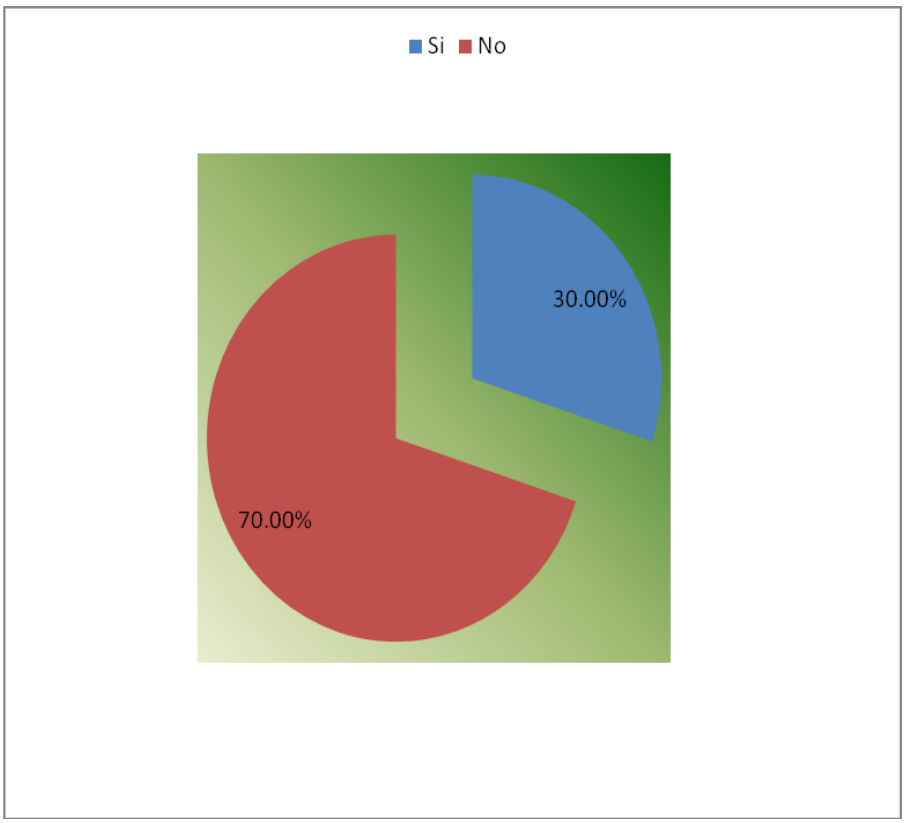
¿Considera que las medidas implementadas actualmente para el desarrollo de las auditorías son suficientes; partiendo del hecho que la mayoría de entidades utilizan sistemas de información para el proceso y almacenamiento de datos?

SI ☐ NO ☐

¿Porqué?_____

Objetivo: Conocer la opinión del auditor, en relación a que si considera que las medidas implementadas actualmente para el desarrollo de las auditorías son suficientes ya que la mayoría de empresas utilizan sistemas de información

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Si	18	30.00%
No	42	70.00%
Total	60	100.00%



ANALISIS: De acuerdo a la tabla anterior un 70.00% de los encuestados afirman que las medidas implementadas actualmente para el desarrollo de las auditorías no son suficientes, ya que la mayoría de empresas utilizan sistemas de información para el procesamiento de datos; el 30.00% consideran que las medidas implementadas actualmente son suficientes para el desarrollo de las auditorías.

PREGUNTA No 20

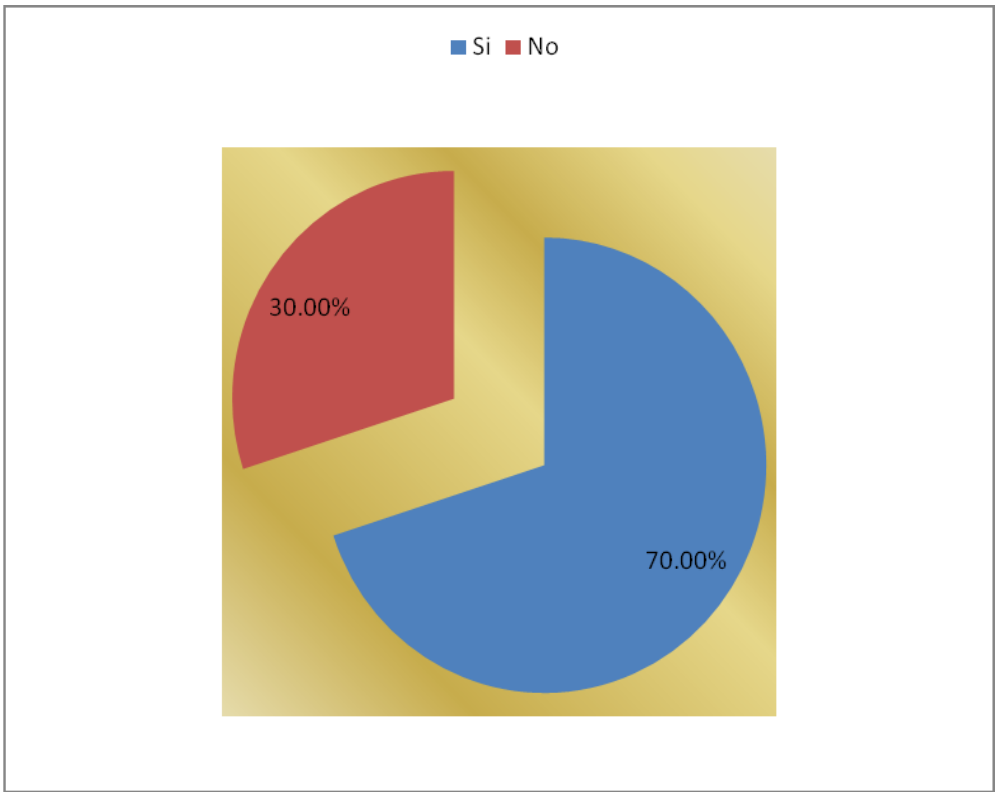
¿Considera usted que los gremios de profesionales toman un papel protagónico en cuanto a la difusión de nuevos conocimientos sobre la profesión contable?

SI ☐ NO ☐

¿Porqué?_____

Objetivo: Conocer la opinión del Contador Público con relación a que si considera que los gremios de profesionales juegan un papel protagónico, en la difusión de nuevos conocimientos contables

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Si	42	70.00%
No	18	30.00%
Total	60	100.00%



ANALISIS: De acuerdo a la tabla anterior un 70.00% de los encuestados afirman que los gremios de profesionales si toman un papel protagónico en la difusión de nuevos conocimientos contables; mientras que un 30.00% considera que los gremios de profesionales no toman ese papel protagónico.

PREGUNTA No 21

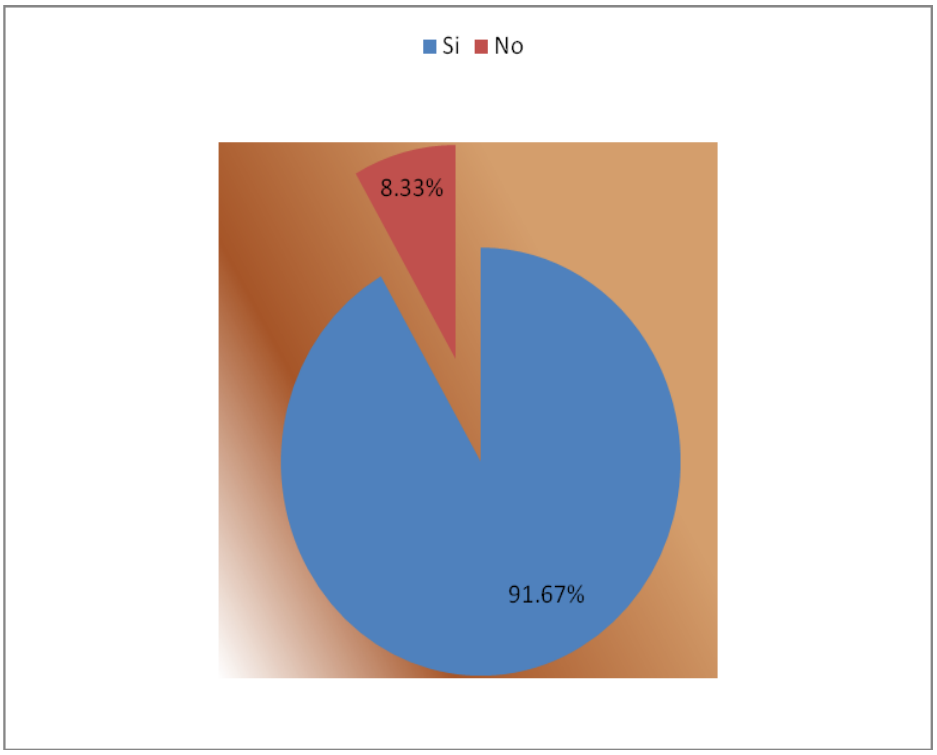
¿Cree usted que es necesario la creación de un modelo de planeación de auditoria estratégica a los sistemas de información que sirva de parámetro para poder implementarlo en cualquier tipo de empresa?

SI ☐ NO ☐

¿Porqué?_____

Objetivo: Indagar sobre la posibilidad de la ejecución de un modelo de planeación de una Auditoría Estratégica a los Sistemas de Información, que sirva de parámetro para los profesionales de la Contaduría Pública que ejecuten este tipo de auditoría.

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Si	55	91.67%
No	5	8.33%
Total	60	100.00%



ANALISIS: De acuerdo a la tabla anterior un 91.67% de los profesionales encuestados afirman que si es necesario la creación de un modelo de planeación de una auditoría estratégica a los sistemas de información que sirva de parámetro para implementarlo en cualquier tipo de empresa.

ANEXO 3 OBJETIVOS DE CONTROL DETALLADOS DE COBIT 4.0

P01 Planear y organizar
Definir un plan estratégico de TI

Objetivos de control detallados

PO1 Definir un plan estratégico de TI

PO1.1 Administración del valor de TI
Trabajar con el negocio para garantizar que el portafolio de inversiones de TI de la empresa contenga programas con casos de negocio sólidos. Reconocer que existen inversiones obligatorias, de sustento y discrecionales que difieren en complejidad y grado de libertad en cuanto a la asignación de fondos. Los procesos de TI deben proporcionar una entrega efectiva y eficiente de los componentes TI de los programas y advertencias oportunas sobre las desviaciones del plan, incluyendo costo, calendario o funcionalidad, que pudieran impactar los resultados esperados de los programas. Los servicios de TI se deben ejecutar contra acuerdos de niveles de servicios equitativos y exigibles. La rendición de cuentas del logro de los beneficios y del control de los costos es claramente asignada y monitoreada. Establecer una evaluación de los casos de negocio que sea justa, transparente, repetible y comparable, incluyendo el valor financiero, el riesgo de no cumplir con una capacidad y el riesgo de no materializar los beneficios esperados.

PO1.2 Alineación de TI con el negocio
Educar a los ejecutivos sobre las capacidades tecnológicas actuales y sobre el rumbo futuro, sobre las oportunidades que ofrece TI, y sobre qué debe hacer el negocio para capitalizar esas oportunidades. Asegurarse de que el rumbo del negocio al cual está alineado la TI está bien entendido. Las estrategias de negocio y de TI deben estar integradas, relacionando de manera clara las metas de la empresa y las metas de TI y reconociendo las oportunidades así como las limitaciones en la capacidad actual, y se deben comunicar de manera amplia. Identificar las áreas en que el negocio (estrategia) depende de forma crítica de la TI, y mediar entre los imperativos del negocio y la tecnología, de tal modo que se puedan establecer prioridades concertadas.

PO1.3 Evaluación del desempeño actual
Evaluar el desempeño de los planes existentes y de los sistemas de información en términos de su contribución a los objetivos de negocio, su funcionalidad, su estabilidad, su complejidad, sus costos, sus fortalezas y debilidades.

PO1.4 IT Plan estratégico de TI
Crear un plan estratégico que defina, en cooperación con los interesados relevantes, cómo la TI contribuirá a los objetivos estratégicos de la empresa (metas) así como los costos y riesgos relacionados. Incluye cómo la TI dará soporte a los programas de inversión facilitados por TI y a la entrega de los servicios operacionales. Define cómo se cumplirán y medirán los objetivos y recibirá una autorización formal de los interesados. El plan estratégico de TI debe incluir el presupuesto de la inversión / operativo, las fuentes de financiamiento, la estrategia de procuración, la estrategia de adquisición, y los requerimientos legales y regulatorios. El plan estratégico debe ser lo suficientemente detallado para permitir la definición de planes tácticos de TI.

PO1.5 IT Planes tácticos de TI
Crear un portafolio de planes tácticos de TI que se deriven del plan estratégico de TI. Estos planes tácticos describen las iniciativas y los requerimientos de recursos requeridos por TI, y cómo el uso de los recursos y el logro de los beneficios serán monitoreados y administrados. Los planes tácticos deben tener el detalle suficiente para permitir la definición de planes proyectados. Administrar de forma activa los planes tácticos y las iniciativas de TI establecidas por medio del análisis de los portafolios de proyectos y servicios. Esto incluye el equilibrio de los requerimientos y recursos de forma regular, comparándolos con el logro de metas estratégicas y tácticas y con los beneficios esperados, y tomando las medidas necesarias en caso de desviaciones.

PO1.6 IT Administración del portafolio de TI
Administrar de forma activa, junto con el negocio, el portafolio de programas de inversión de TI requerido para lograr objetivos de negocio estratégicos y específicos por medio de la identificación, definición, evaluación, asignación de prioridades, selección, inicio, administración y control de los programas. Esto incluye clarificar los resultados de negocio deseados, garantizar que los objetivos de los programas den soporte al logro de los resultados, entender el alcance completo del esfuerzo requerido para lograr los resultados, definir una rendición de cuentas clara con medidas de soporte, definir proyectos dentro del programa, asignar recursos y financiamiento, delegar autoridad, y licenciar los proyectos requeridos al momento de lanzar el programa.

P02 Planear y organizar
Definir la arquitectura de la información

Objetivos de control detallados

PO2 Definir la arquitectura de la información

PO2.1 Modelo de arquitectura de información empresarial
Establecer y mantener un modelo de información empresarial que facilite el desarrollo de aplicaciones y las actividades de soporte a la toma de decisiones, consistente con los planes de TI como se describen en P01. El modelo facilita la creación, uso y compartición óptimas de la información por parte del negocio de una manera que conserva la integridad y es flexible, funcional, rentable oportuna segura y tolerante a fallas.

PO2.2 Diccionario de datos empresarial y reglas de sintaxis de datos
Mantener un diccionario de datos empresarial que incluya las reglas de sintaxis de datos de la organización. El diccionario facilita la compartición de elementos de datos entre las aplicaciones y los sistemas, fomenta un entendimiento común de datos entre los usuarios de TI y del negocio, y previene la creación de elementos de datos incompatibles.

PO2.3 Esquema de clasificación de datos
Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información (esto es, pública, confidencial, secreta) de la empresa. Este esquema incluye detalles acerca de la propiedad de datos, la definición de niveles apropiados de seguridad y de controles de protección, y una breve descripción de los requerimientos de retención y destrucción de datos, además de qué tan críticos y sensibles son. Se usa como base para aplicar controles como el control de acceso, archivo o encripción.

PO4.4 IT Administración de la integridad
Definir e implantar procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en formato electrónico, tales como bases de datos, almacenes de datos y archivos.

P03 Planear y organizar
Determinar la dirección tecnológica

Objetivos de control detallados

PO3 Determinar la dirección tecnológica

PO3.1 Planeación de la dirección tecnológica
Analizar las tecnologías existentes y emergentes y planear cuál dirección tecnológica es apropiado tomar para materializar la estrategia de TI y la arquitectura de sistemas del negocio. También identificar en el plan qué tecnologías tienen el potencial de crear oportunidades de negocio. El plan debe abarcar la arquitectura de sistemas, la dirección tecnológica, las estrategias de migración y los aspectos de contingencia de los componentes de la infraestructura.

PO3.2 Plan de infraestructura tecnológica
Crear y mantener un plan de infraestructura tecnológica que esté de acuerdo con los planes estratégicos y tácticos de TI. El plan se basa en la dirección tecnológica e incluye acuerdos para contingencias y orientación para la adquisición de recursos tecnológicos. También toma en cuenta los cambios en el ambiente competitivo, las economías de escala en la obtención de equipo de sistemas de información, y la mejora en la interoperabilidad de las plataformas y las aplicaciones.

PO3.3 Monitoreo de tendencias y regulaciones futuras
Establecer un proceso para monitorear las tendencias ambientales del sector / industria, tecnológicas, de infraestructura, legales y regulatorias. Incluir las consecuencias de estas tendencias en el desarrollo del plan de infraestructura tecnológica de TI.

PO3.4 Estándares tecnológicos
Proporcionar soluciones tecnológicas consistentes, efectivas y seguras para toda la empresa, establecer un foro tecnológico para brindar directrices tecnológicas, asesoría sobre los productos de la infraestructura y guías sobre la selección de la tecnología, y medir el cumplimiento de estos estándares y directrices. Este foro impulsa los estándares y las prácticas tecnológicas con base en su importancia y riesgo para el negocio y en el cumplimiento de requerimientos externos.

PO3.4 Consejo de arquitectura
Establecer un consejo de arquitectura de TI que proporcione directrices sobre la arquitectura y asesoría sobre su aplicación y que verifique el cumplimiento. Esta entidad orienta el diseño de la arquitectura de TI garantizando que facilite la estrategia del negocio y tome en cuenta el cumplimiento regulatorio y los requerimientos de continuidad. Estos aspectos se relacionan con la arquitectura de la información

Objetivos de control detallados

PO4 Definir los procesos, la organización y las relaciones de TI

PO4.1 Marco de trabajo del proceso
Definir un marco de trabajo para el proceso de TI para ejecutar el plan estratégico de TI. Este marco incluye estructura y relaciones de procesos de TI (administrando brechas y superposiciones de procesos), propiedad, medición del desempeño, mejoras, cumplimiento, metas de calidad y planes para alcanzarlas. Proporciona integración entre los procesos que son específicos para TI, administración del portafolio de TI, procesos de negocio y procesos de cambio del negocio. El marco de trabajo de procesos de TI debe estar integrado en un sistema de administración de calidad y en un marco de trabajo de control interno.

PO4.2 Comité estratégico
Establecer un comité estratégico de TI a nivel del consejo directivo. Este comité garantiza que el gobierno de TI, como parte del gobierno corporativo, se maneja de forma adecuada, asesora sobre la dirección estratégica y revisa las inversiones principales a nombre del consejo directivo.

PO4.3 Comité directivo (Steering Committee)
Establecer un comité directivo de TI (o su equivalente) compuesto por la gerencia ejecutiva, del negocio y de TI para:
- Determinar las prioridades de los programas de inversión de TI alineadas con la estrategia y prioridades de negocio de la empresa
- Hacer seguimiento al estatus de los proyectos y resolver los conflictos de recursos
- Monitorear los niveles de servicio y las mejoras del servicio

PO4.4 Ubicación organizacional de la función de TI
Ubicar a la función de TI dentro de la estructura organizacional general con un modelo de negocios supeditado a la importancia de TI dentro de la empresa, en especial en función de que tan crítica es para la estrategia del negocio y el nivel de dependencia operativa sobre TI. La línea de reporte del CIO es proporcional con la importancia de TI dentro de la empresa.

PO4.5 Estructura organizacional
Establecer una estructura organizacional de TI interna y externa que refleje las necesidades del negocio. Además implantar un proceso para revisar la estructura organizacional de TI de forma periódica para ajustar los requerimientos de personal y las estrategias internas para satisfacer los objetivos de negocio esperados y las circunstancias cambiantes.

PO4.6 Roles y responsabilidades
Definir y comunicar los roles y las responsabilidades para todo el personal en la organización con respecto a los sistemas de información para permitir que ejerzan los roles y responsabilidades asignados con suficiente autoridad. Crear y actualizar periódicamente la descripción de roles. Estas descripciones deben estar alineadas con la responsabilidad y la autoridad incluyendo definiciones de habilidades y experiencia necesarias en cada posición y que serán aplicables en el uso y evaluación del desempeño.

PO4.7 Responsabilidad de aseguramiento de calidad de TI
Asignar la responsabilidad para el desempeño de la función de aseguramiento de calidad y proporcionar al grupo de aseguramiento los sistemas de aseguramiento de calidad, los controles y la experiencia para comunicarlos. La ubicación organizacional y las responsabilidades y tamaño del grupo de aseguramiento de calidad satisfacen los requerimientos de la organización.

PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento
Incluir la propiedad y la responsabilidad de los riesgos relacionados con TI a un nivel senior apropiado. Definir y asignar roles críticos para administrar los riesgos de TI, incluyendo la responsabilidad específica de la seguridad de la información, la seguridad física y el cumplimiento. Establecer responsabilidad sobre la administración del riesgo y la seguridad a nivel de toda la organización para manejar los problemas a nivel de toda la empresa. Puede ser necesario asignar responsabilidades adicionales de administración de la seguridad a nivel de sistema específico para manejar problemas relacionados con seguridad. Obtener orientación de la alta dirección con respecto al apetito de riesgo de TI y la aprobación de cualquier riesgo residual de TI.

PO4.9 Propiedad de datos y de sistemas
Proporcionar al negocio los procedimientos y herramientas que le permitan enfrentar sus responsabilidades de propiedad sobre los datos y los sistemas de información. Los propietarios toman decisiones sobre la clasificación de la información y de los sistemas y sobre cómo protegerlos de acuerdo a esta clasificación.

PO4.10 Supervisión
Implantar prácticas adecuadas de supervisión dentro de la función de TI para garantizar que los roles y las responsabilidades se ejerzan de forma apropiada, para evaluar si todo el personal cuenta con la suficiente autoridad y recursos para ejecutar sus roles y responsabilidades y para revisar en general los indicadores clave de desempeño.

PO4.11 Segregación de funciones
Implantar una división de roles y responsabilidades que reduzca la posibilidad de que un solo individuo afecte negativamente un proceso crítico. La gerencia también se asegura de que el personal realice solo las tareas autorizadas, relevantes a sus puestos y posiciones respectivas.

PO4.12 Personal de TI
Evaluar los requerimientos de personal de forma regular o cuando existan cambios importantes en el ambiente de negocios, operativo o de TI para garantizar que la función de TI cuente con un número suficiente de personal competente. La consecución de personal toma en cuenta la co-ubicación de personal de negocios / TI, el entrenamiento cruzado- funcional, la rotación de puestos y las oportunidades de personal externo.

PO4.13 Personal clave de TI
Definir e identificar al personal clave de TI y minimizar la dependencia excesiva en ellos. Debe existir un plan para contactar al personal clave en caso de emergencia.

PO4.14 Políticas y procedimientos para personal contratado
Definir e implantar políticas y procedimientos para controlar las actividades de los consultores y otro personal contratado por la función de TI para garantizar la protección de los activos de información de la empresa y satisfacer los requerimientos contractuales.

PO4.15 Relaciones
Establecer y mantener una estructura óptima de enlace, comunicación y coordinación entre la función de TI y otras funciones dentro y fuera de la función de TI, tales como el consejo directivo, ejecutivos, unidades de negocio, usuarios individuales, proveedores, oficiales de seguridad, gerentes de riesgo, el grupo corporativo de cumplimiento, los contratistas externos y la gerencia externa (offsite).

P05 Planear y organizar
Administrar la inversión en TI

Objetivos de control detallados

PO5 Administrar la inversión en TI

PO5.1 Marco de trabajo para la administración financiera
Establecer un marco de trabajo financiero para TI que impulse el presupuesto y el análisis de rentabilidad, con base en los portafolios de inversión, servicios y activos. Dar mantenimiento a los portafolios de los programas de inversión de TI, de servicios y de activos de TI, los cuales forman la base para el presupuesto corriente de TI. Brindar información de entrada hacia los casos de negocio de nuevas inversiones, tomando en cuenta los portafolios actuales de activos y servicios de TI. Las nuevas inversiones y el mantenimiento a los portafolios de servicios y de activos influenciarán el futuro presupuesto de TI. Comunicar los aspectos de costo y beneficio de estos portafolios a los procesos de priorización de presupuestos, administración de costos y administración de beneficios.

PO5.2 Prioridades dentro del presupuesto de TI
Implantar un proceso de toma de decisiones para dar prioridades a la asignación de recursos a TI para operaciones, proyectos y mantenimiento, para maximizar la contribución de TI a optimizar el retorno del portafolio empresarial de programas de inversión en TI y otros servicios y activos de TI.

PO5.3 Proceso presupuestal
Establecer un proceso para elaborar y administrar un presupuesto que refleje las prioridades establecidas en el portafolio empresarial de programas de inversión en TI, incluyendo los costos recurrentes de operar y mantener la infraestructura actual. El proceso debe dar soporte al desarrollo de un presupuesto general de TI así como al desarrollo de presupuestos para programas individuales, con énfasis especial en los componentes de TI de esos programas. El proceso debe permitir la revisión, el refinamiento y la aprobación constantes del presupuesto general y de los presupuestos de programas individuales.

PO5.4 IT Administración de costos
Implantar un proceso de administración de costos que compare los costos reales con los presupuestados. Los costos se deben monitorear y reportar. Cuando existan desviaciones, estas se deben identificar de forma oportuna y el impacto de esas desviaciones sobre los programas se debe evaluar y, junto con el patrocinador del negocio para estos programas, se deberán tomar las medidas correctivas apropiadas y, en caso de ser necesario, el caso de negocio del programa de inversión se deberá actualizar.

PO5.5 Administración de beneficios
Implantar un proceso de monitoreo de beneficios. La contribución esperada de TI a los resultados del negocio, ya sea como un componente de programas de inversión en TI o como parte de un soporte operativo regular, se debe identificar, acordar, monitorear y reportar. Los reportes se deben revisar y, donde existan oportunidades para mejorar la contribución de TI, se deben definir y tomar las medidas apropiadas. Siempre que los cambios en la contribución de TI tengan impacto en el programa, o cuando los cambios a otros proyectos relacionados impacten al programa, el caso de negocio deberá ser actualizado.

P06 Planear y organizar
Comunicar las aspiraciones y la dirección de la gerencia

Objetivos de control detallados

PO6 Comunicar las aspiraciones y la dirección de la gerencia

PO6.1 Ambiente de políticas y de control
Definir los elementos de un ambiente de control para TI, alineados con la filosofía administrativa y el estilo operativo de la empresa. Estos elementos incluyen las expectativas / requerimientos respecto a la entrega de valor proveniente de las inversiones en TI, el apetito de riesgo, la integridad, los valores éticos, la competencia del personal, la rendición de cuentas y la responsabilidad. El ambiente de control se basa en una cultura que apoya la entrega de valor, mientras que al mismo tiempo administra riesgos significativos, fomenta la colaboración inter-divisional y el trabajo en equipo, promueve el cumplimiento y la mejora continua de procesos, y maneja las desviaciones (incluyendo las fallas) de forma adecuada.

PO6.2 Riesgo Corporativo y Marco de Referencia de Control Interno de TI
Elaborar y dar mantenimiento a un marco de trabajo que establezca el enfoque empresarial general hacia los riesgos y hacia el control interno para entregar valor mientras al mismo tiempo se protegen los recursos y sistemas de TI. El marco de trabajo debe estar integrado por el marco de procesos de TI y el sistema de administración de calidad, y debe cumplir los objetivos generales de la empresa. Debe tener como meta maximizar el éxito de la entrega de valor mientras minimiza los riesgos para los activos de información por medio de medidas preventivas, la identificación oportuna de irregularidades, la limitación de pérdidas y la oportuna recuperación de activos del negocio.

PO6.3 Administración de políticas para TI
Elaborar y dar mantenimiento a un conjunto de políticas que apoyen la estrategia de TI. Estas políticas deben incluir la intención de las políticas, roles y responsabilidades, procesos de excepción, enfoque de cumplimiento y referencias a procedimientos, estándares y directrices. Las políticas deben incluir tópicos clave como calidad, seguridad, confidencialidad, controles internos y propiedad intelectual. Su relevancia se debe confirmar y aprobar de forma regular.

PO6.4 Implantación de políticas de TI
Asegurarse de que las políticas de TI se implantan y se comunican a todo el personal relevante, y se refuerzan, de tal forma que estén incluidas y sean parte integral de las operaciones empresariales. Los métodos de implantación deben resolver necesidades e implicaciones de recursos y concientización.

PO6.5 Comunicación de los objetivos y la dirección de TI
Asegurarse de que la conciencia y el entendimiento de los objetivos y la dirección del negocio y de TI se comunican a toda la organización. La información comunicada debe abarcar una misión claramente articulada, los objetivos de servicio, la seguridad, los controles internos, la calidad, el código de ética y conducta, políticas y procedimientos, etc., y se deben incluir dentro de un programa de comunicación continua, apoyado por la alta dirección con acciones y palabras. La dirección debe dar especial atención a comunicar la conciencia sobre la seguridad de TI y el mensaje de que la seguridad de TI es responsabilidad de todos.

P07 Planear y organizar
Administrar los recursos humanos de TI

Objetivos de control detallados

PO7 Administrar los recursos humanos de TI

PO7.1 Reclutamiento y Retencion del Personal
Asegurarse que los procesos de reclutamiento del personal de TI estén de acuerdo a las políticas y procedimientos generales de personal de la organización (ej. contratación, un ambiente positivo de trabajo y orientación). La gerencia implementa procesos para garantizar que la organización cuente con una fuerza de trabajo posicionada de forma apropiada, que tenga las habilidades necesarias para alcanzar las metas organizacionales.

PO7.2 Competencias del personal
Verificar de forma periódica que el personal tenga las habilidades para cumplir sus roles con base en su educación, entrenamiento y/o experiencia. Definir los requerimientos esenciales de habilidades para TI y verificar que se les dé mantenimiento, usando programas de calificación y certificación según sea el caso.

PO7.3 Asignacion de roles
Definir, monitorear y supervisar los marcos de trabajo para los roles, responsabilidades y compensación del personal, incluyendo el requisito de adherirse a las políticas y procedimientos administrativos, así como al código de ética y prácticas profesionales. Los términos y condiciones de empleo deben enfatizar la responsabilidad del empleado respecto a la seguridad de la información, al control interno y al cumplimiento regulatorio. El nivel de supervisión debe estar de acuerdo con la sensibilidad del puesto y el grado de responsabilidades asignadas.

PO7.4 Entrenamiento del personal de TI
Proporcionar a los empleados de TI la orientación necesaria al momento de la contratación y entrenamiento continuo para conservar su conocimiento, aptitudes, habilidades, controles internos y conciencia sobre la seguridad, al nivel requerido para alcanzar las metas organizacionales.

PO7.5 Dependencia sobre los individuos
Minimizar la exposición a dependencias críticas sobre individuos clave por medio de la captura del conocimiento (documentación), compartir el conocimiento, planeación de la sucesión y respaldos de personal.

PO7.6 Procedimientos de Investigación del personal
Incluir verificaciones de antecedentes en el proceso de reclutamiento de TI. El grado y la frecuencia de estas verificaciones dependen de que tan delicada ó crítica sea la función y se deben aplicar a los empleados, contratistas y proveedores.

PO7.7 Evaluación del desempeño del empleado
Es necesario que las evaluaciones de desempeño se realicen periódicamente, comparando contra los objetivos individuales derivados de las metas organizacionales, estándares establecidos y responsabilidades específicas del puesto. Los empleados deben recibir adiestramiento sobre su desempeño y conducta, según sea necesario.

PO7.8 Cambios y terminación de trabajo
Tomar medidas expeditas respecto a los cambios en los puestos, en especial las terminaciones. Se debe realizar la transferencia del conocimiento, reasignar responsabilidades y se deben eliminar los privilegios de acceso, de tal modo que los riesgos se minimicen y se garantice la continuidad de la función.

P08 Planear y organizar
Administrar la calidad

Objetivos de control detallados

PO8 Administrar la calidad

PO8.1 Sistema de administración de calidad
Establecer y mantener un QMS que proporcione un enfoque estándar, formal y continuo, con respecto a la administración de la calidad, que esté alineado con los requerimientos del negocio. El QMS identifica los requerimientos y los criterios de calidad, los procesos claves de TI, y su secuencia e interacción, así como las políticas, criterios y métodos para definir, detectar, corregir y prever las no conformidades. El QMS debe definir la estructura organizacional para la administración de la calidad, cubriendo los roles, las tareas y las responsabilidades. Todas las áreas clave desarrollan sus planes de calidad de acuerdo a los criterios y políticas, y registran los datos de calidad. Monitorear y medir la efectividad y aceptación del QMS y mejorarla cuando sea necesario.

PO8.2 Estándares y prácticas de calidad
Identificar y mantener estándares, procedimientos y prácticas para los procesos clave de TI para orientar a la organización hacia el cumplimiento del QMS. Usar las mejores prácticas de la industria como referencia al mejorar y adaptar las prácticas de calidad de la organización.

PO8.3 Estándares de desarrollo y de adquisición
Adoptar y mantener estándares para todo el desarrollo y adquisición que siguen el ciclo de vida, hasta el último entregable e incluyen la aprobación en puntos clave con base en criterios de aprobación acordados. Los temas a considerar incluyen estándares de codificación de software, normas de nomenclatura; formatos de archivos, estándares de diseño para esquemas y diccionario de datos; estándares para la interfaz de usuario; inter-operabilidad; eficiencia de desempeño de sistemas; escalabilidad; estándares para desarrollo y pruebas; validación contra requerimientos; planes de pruebas; y pruebas unitarias, de regresión y de integración.

PO8.4 IT Enfoque en el cliente
Garantiza que la administración de calidad se enfoque en los clientes, al determinar sus requerimientos y alinearlos con los estándares y prácticas de TI. Se definen los roles y responsabilidades respecto a la resolución de conflictos entre el usuario/cliente y la organización de TI.

PO8.5 Mejora continua
Se elabora y comunica un plan global de calidad que promueva la mejora continua, de forma periódica.

PO8.6 Medición, monitoreo y revisión de la calidad
Definir, planear e implantar mediciones para monitorear el cumplimiento continuo del QMS, así como el valor que QMS proporciona. La medición, el monitoreo y el registro de la información deben ser usados por el dueño del proceso para tomar las medidas correctivas y preventivas apropiadas.

P09 Planear y organizar
Evaluar y administrar los riesgos de TI

Objetivos de control detallados

PO9 Evaluar y administrar los riesgos de TI

PO9.1 Alineación de la administración de riesgos de TI y del negocio
Integrar el gobierno, la administración de riesgos y el marco de control de TI, al marco de trabajo de administración de riesgos de la organización. Esto incluye la alineación con el apetito de riesgo y con el nivel de tolerancia al riesgo de la organización

PO9.2 Establecimiento del contexto del riesgo
Establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados. Esto incluye la determinación del contexto interno y externo de cada evaluación de riesgos, la meta de la evaluación y los criterios contra los cuales se evalúan los riesgos.

PO9.3 Identificación de eventos
Identificar todos aquellos eventos (amenazas y vulnerabilidades) con un impacto potencial sobre las metas o las operaciones de la empresa, aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos. Determinar la naturaleza del impacto – positivo, negativo o ambos – y dar mantenimiento a esta información.

PO9.4 IT Evaluación de riesgos
Evaluar de forma recurrente la posibilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La posibilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio.

PO9.5 Respuesta a los riesgos
Identificar los propietarios de los riesgos y a los dueños de procesos afectados, y elaborar y mantener respuestas a los riesgos que garanticen que los controles rentables y las medidas de seguridad mitigan la exposición a los riesgos de forma continua. La respuesta a los riesgos debe identificar estrategias de riesgo tales como evitar, reducir, compartir o aceptar. Al elaborar la respuesta, considerar los costos y beneficios y seleccionar respuestas que limiten los riesgos residuales dentro de los niveles de tolerancia de riesgos definidos.

PO9.6 Mantenimiento y monitoreo de un plan de acción de riesgos
Asignar prioridades y planear las actividades de control a todos los niveles para implantar las respuestas a los riesgos, identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución. Buscar la aprobación para las acciones recomendadas y la aceptación de cualquier riesgo residual, y asegurarse de que las acciones comprometidas son propiedad del dueño (s) de los procesos afectados. Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección.

P010 Planear y organizar
Administrar proyectos

Objetivos de control detallados

P010 Administrar proyectos

P010.1 Marco de trabajo para la administración de programas
Mantener el programa de los proyectos, relacionados con el portafolio de programas de inversión en TI, por medio de la identificación, definición, evaluación, otorgamiento de prioridades, selección, inicio, administración y control de los proyectos. Asegurarse de que los proyectos apoyen los objetivos del programa. Coordinar las actividades e interdependencias de múltiples proyectos, administrar la contribución de todos los proyectos dentro del programa hasta obtener los resultados esperados, y resolver los requerimientos y conflictos de recursos.

P010.2 Marco de trabajo para la administración de proyectos
Establecer y mantener un marco de trabajo para la administración de proyectos que defina el alcance y los límites de la administración de proyectos, así como las metodologías a ser adoptadas y aplicadas a cada proyecto emprendido. Las metodologías deben cubrir, como mínimo, el inicio, la planeación, la ejecución, el control y el cierre de las etapas de los proyectos, así como los puntos de verificación y las aprobaciones. El marco de trabajo y las metodologías de soporte se deben integrar con la administración del portafolio empresarial y con los procesos de administración de programas.

P010.3 Enfoque de administración de proyectos
Establecer un enfoque de administración de proyectos que corresponda al tamaño, complejidad y requerimientos regulatorios de cada proyecto. La estructura de gobierno de proyectos puede incluir los roles, las responsabilidades y la rendición de cuentas del patrocinador del programa, patrocinadores del proyecto, comité de dirección, oficina de proyectos, y gerente del proyecto, así como los mecanismos por medio de los cuales pueden satisfacer esas responsabilidades (tales como reportes y revisiones por etapa). Asegurarse que todos los proyectos de TI cuenten con patrocinadores con la suficiente autoridad para apropiarse de la ejecución del proyecto dentro del programa estratégico global.

P010.4 Compromiso de los interesados
Obtener el compromiso y la participación de los interesados afectados en la definición y ejecución del proyecto dentro del contexto del programa global de inversión en TI.

P010.5 Estatuto de alcance del proyecto
Definir y documentar la naturaleza y alcance del proyecto para confirmar y desarrollar, entre los interesados, un entendimiento común del alcance del proyecto y cómo se relaciona con otros proyectos dentro del programa global de inversión en TI. La definición se debe aprobar de manera formal por parte de los patrocinadores del programa y del proyecto antes de arrancar el proyecto.

P010.6 Inicio de las fases del proyecto
Asegurarse que el arranque de las etapas importantes del proyecto se apruebe de manera formal y se comunique a todos los interesados. La aprobación de la fase inicial se debe basar en las decisiones de gobierno del programa. La aprobación de las fases subsiguientes se debe basar en la revisión y aceptación de los entregables de la fase previa, y la aprobación de un caso de negocio actualizado en la próxima revisión importante del programa. En el caso de fases traslapadas, se debe establecer un punto de aprobación por parte de los patrocinadores del programa y del proyecto, para autorizar así el avance del proyecto.

P010.7 Plan integrado del proyecto
Establecer un plan integrado para el proyecto, aprobado y formal (que cubra los recursos de negocio y de los sistemas de información) para guiar la ejecución y el control del proyecto a lo largo de la vida del éste. Las actividades e interdependencias de múltiples proyectos dentro de un mismo programa se deben entender y documentar. El plan del proyecto se debe mantener a lo largo de la vida del mismo. El plan del proyecto, y las modificaciones a éste, se deben aprobar de acuerdo al marco de trabajo de gobierno del programa y del proyecto.

P010.8 Recursos del proyecto
Definir las responsabilidades, relaciones, autoridades y criterios de desempeño de los miembros del equipo del proyecto y especificar las bases para adquirir y asignar a los miembros competentes del equipo y/o a los contratistas al proyecto. La obtención de productos y servicios requeridos para cada proyecto se debe planear y administrar para alcanzar los objetivos del proyecto, usando las prácticas de adquisición de la organización.

P010.9 Administración de riesgos del proyecto
Eliminar o minimizar los riesgos específicos asociados con los proyectos individuales por medio de un proceso sistemático de planeación, identificación, análisis, respuestas, monitoreo y control de las áreas o eventos que tengan el potencial de ocasionar cambios no deseados. Los riesgos afrontados por el proceso de administración de proyectos y el producto entregable del proyecto se deben establecer y registrar de forma central.

PO10.10 Plan de calidad del proyecto
Preparar un plan de administración de la calidad que describa el sistema de calidad del proyecto y cómo será implantado. El plan debe ser revisado y acordado de manera formal por todas las partes interesadas para luego ser incorporado en el plan integrado del proyecto.

PO10.11 Control de cambios del proyecto
Establecer un sistema de control de cambios para cada proyecto, de tal modo que todos los cambios a la línea base del proyecto (ej. costos, cronograma, alcance y calidad) se revisen, aprueben e incorporen de manera apropiada al plan integrado del proyecto, de acuerdo al marco de trabajo de gobierno del programa y del proyecto.

PO10.12 Planeación del proyecto y métodos de aseguramiento
Identificar las tares de aseguramiento requeridas para apoyar la acreditación de sistemas nuevos o modificados durante la planeación del proyecto e incluirlos en el plan integrado. Las tareas deben proporcionar la seguridad de que los controles internos y las características de seguridad satisfagan los requerimientos definidos.

PO10.13 Medición del desempeño, reportes y monitoreo del proyecto
Medir el desempeño del proyecto contra los criterios clave del proyecto (ej. alcance, calendario, calidad, costos y riesgos); identificar las desviaciones con respecto al plan; evaluar su impacto sobre el proyecto y sobre el programa global; reportar los resultados a los interesados clave; y recomendar, implantar y monitorear las medidas correctivas, según sea requerido, de acuerdo con el marco de trabajo de gobierno del programa y del proyecto.

PO10.14 Cierre del proyecto
Solicitar que al finalizar cada proyecto, los interesados del proyecto se cercioren de que el proyecto haya proporcionado los resultados y los beneficios esperados. Identificar y comunicar cualquier actividad sobresaliente requerida para alcanzar los resultados planeados del proyecto y los beneficios del programa, e identificar y documentar las lecciones aprendidas a ser usadas en futuros proyectos y programas

Objetivos de control detallados

AI2 Adquirir y mantener software aplicativo

AI2.1 Diseño de alto nivel
Traducir los requerimientos del negocio a una especificación de diseño de alto nivel para desarrollo de software, tomando en cuenta las directivas tecnológicas y la arquitectura de información dentro de la organización, y aprobar las especificaciones de diseño para garantizar que el diseño de alto nivel responde a los requerimientos.

AI2.2 Diseño detallado
Preparar el diseño detallado y los requerimientos técnicos del software de aplicación. Definir el criterio de aceptación de los requerimientos. Aprobar los requerimientos para garantizar que corresponden al diseño de alto nivel. Los conceptos a considerar incluyen, pero no se limitan a, definir y documentar los requerimientos de entrada de datos, definir interfaces, la interface de usuario, el diseño para la recopilación de datos fuente, la especificación de programa, definir y documentar los requerimientos de archivo, requerimientos de procesamiento, definir los requerimientos de salida, control y auditabilidad, seguridad y disponibilidad, y pruebas. Realizar una reevaluación para cuando se presenten discrepancias técnicas o lógicas significativas durante el desarrollo o mantenimiento.

AI2.3 Control y auditabilidad de las aplicaciones
Asegurar que los controles del negocio se traduzcan correctamente en controles de aplicación de manera que el procesamiento sea exacto, completo, oportuno, aprobado y auditable. Los aspectos que se consideran especialmente son: mecanismos de autorización, integridad de la información, control de acceso, respaldo y diseño de pistas de auditoría.

AI2.4 Seguridad y disponibilidad de las aplicaciones.
Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados, de acuerdo con la clasificación de datos, la arquitectura de seguridad en la información de la organización y el perfil de riesgo. Los asuntos a considerar incluyen derechos de acceso y administración de privilegios, protección de información sensible en todas las etapas, autenticación e integridad de las transacciones y recuperación automática.

.
AI2.5 Configuración e implantación de software aplicativo adquirido
Personalizar e implantar la funcionalidad automatizada adquirida con el uso de procedimientos de configuración, aceptación y prueba. Los aspectos a considerar incluyen la validación contra los términos contractuales, la arquitectura de información de la organización, las aplicaciones existentes, la interoperabilidad con las aplicaciones existentes y los sistemas de bases de datos, la eficiencia en el desempeño del sistema, la documentación y los manuales de usuario, integración y planes de prueba del sistema.

AI2.6 Actualizaciones importantes en sistemas existentes
Seguir un proceso de desarrollo similar al de desarrollo de sistemas nuevos en el caso que se presenten modificaciones importantes en los sistemas existentes, que resulten en un cambio significativo de los diseños y/o funcionalidad actuales. Los aspectos a considerar incluyen análisis de impacto, justificación costo/beneficio y administración de requerimientos.

AI2.7 Desarrollo de software aplicativo
Garantizar que la funcionalidad de automatización se desarrolla de acuerdo con las especificaciones de diseño, los estándares de desarrollo y documentación y los requerimientos de calidad. Aprobar y autorizar cada etapa clave del proceso de desarrollo de software aplicativo, dando seguimiento a la terminación exitosa de revisiones de funcionalidad, desempeño y calidad. Los aspectos a considerar incluyen aprobar las especificaciones de diseño que satisfacen los requerimientos de negocio, funcionales y técnicos; aprobar las solicitudes de cambio; y confirmación de que el software aplicativo es compatible con la producción y está listo para su migración. Además, garantizar que se identifican y consideran todos los aspectos legales y contractuales para el software aplicativo que desarrollan terceros.

AI2.8 Aseguramiento de la Calidad del Software
Desarrollar, implantar los recursos y ejecutar un plan de aseguramiento de calidad del software, para obtener la calidad que se especifica en la definición de los requerimientos y en las políticas y procedimientos de calidad de la organización. Los asuntos a considerar en el plan de aseguramiento de calidad incluyen especificar el criterio de calidad y los procesos de validación y verificación, incluyendo inspección, revisión de algoritmos y código fuente y pruebas.

AI2.9 Administración de los requerimientos de aplicaciones
Garantizar que durante el diseño, desarrollo e implantación, se da seguimiento al estatus de los requerimientos particulares (incluyendo todos los requerimientos rechazados), y que las modificaciones a los requerimientos se aprueban a través de un proceso establecido de administración de cambios.

AI2.10 Mantenimiento de software aplicativo
Desarrollar una estrategia y un plan para el mantenimiento y liberación de aplicaciones de software. Los asuntos a considerar incluyen liberación planeada y controlada, planeación de recursos, reparación de defectos de programa y corrección de fallas, pequeñas mejoras, mantenimiento de documentación, cambios de emergencia, interdependencia con otras aplicaciones e infraestructura, estrategias de actualización, condiciones contractuales tales como aspectos de soporte y actualizaciones, revisión periódica de acuerdo a las necesidades del negocio, riegos y requerimientos de seguridad.

AI3 **Adquirir e implantar**
Adquirir y mantener infraestructura tecnológica

Objetivos de control detallados

AI3 Adquirir y mantener infraestructura tecnológica

AI3.1 Plan de adquisición de infraestructura tecnológica
Generar un plan para adquirir, implantar y mantener la infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio, y que esté de acuerdo con la dirección tecnológica de la organización. El plan debe considerar extensiones futuras para adiciones de capacidad, costos de transición, riesgos tecnológicos y vida útil de la inversión para actualizaciones de tecnología. Evaluar los costos de complejidad y la viabilidad comercial del proveedor y el producto al añadir nueva capacidad técnica.

AI3.2 Protección y disponibilidad del recurso de infraestructura
Implantar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad. Se deben definir y comprender claramente las responsabilidades al utilizar componentes de infraestructura sensitivos por todos aquellos que desarrollan e integran los componentes de infraestructura. Se debe monitorear y evaluar su uso.

AI3.3 Mantenimiento de la Infraestructura
Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el procedimiento de administración de cambios de la organización. Incluir una revisión periódica contra las necesidades del negocio, administración de parches y estrategias de actualización, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.

AI3.4 Ambiente de prueba de factibilidad
Establecer el ambiente de desarrollo y pruebas para soportar la efectividad y eficiencia de las pruebas de factibilidad e integración de aplicaciones e infraestructura, en las primeras fases del proceso de adquisición y desarrollo. Hay que considerar la funcionalidad, la configuración de hardware y software, pruebas de integración y desempeño, migración entre ambientes, control de la versiones, datos y herramientas de prueba y seguridad.

AI4 **Adquirir e implantar**
Facilitar la operación y el uso

Objetivos de control detallados

AI4 Facilitar la operación y el uso

AI4.1 Plan para soluciones de operación
Desarrollar un plan para identificar y documentar todos los aspectos técnicos, la capacidad de operación y los niveles de servicio requeridos, de manera que todos los interesados puedan tomar la responsabilidad oportunamente por la producción de procedimientos de administración, de usuario y operacionales, como resultado de la introducción o actualización de sistemas automatizados o de infraestructura.

AI4.2 Transferencia de conocimiento a la gerencia del negocio
Transferir el conocimiento a la gerencia de la empresa para permitirles tomar posesión del sistema y los datos y ejercer la responsabilidad por la entrega y calidad del servicio, del control interno, y de los procesos administrativos de la aplicación. La transferencia de conocimiento incluye la aprobación de acceso, administración de privilegios, segregación de tareas, controles automatizados del negocio, respaldo/recuperación, seguridad física y archivo de la documentación fuente.

AI4.3 Transferencia de conocimiento a usuarios finales
Transferencia de conocimiento y habilidades para permitir que los usuarios finales utilicen con efectividad y eficiencia el sistema de aplicación como apoyo a los procesos del negocio. La transferencia de conocimiento incluye el desarrollo de un plan de entrenamiento que aborde al entrenamiento inicial y al continuo, así como el desarrollo de habilidades, materiales de entrenamiento, manuales de usuario, manuales de procedimiento, ayuda en línea, asistencia a usuarios, identificación del usuario clave, y evaluación.

AI4.4 Transferencia de conocimiento al personal de operaciones y soporte
Transferir el conocimiento y las habilidades para permitir al personal de soporte técnico y de operaciones que entregue, apoye y mantenga la aplicación y la infraestructura asociada de manera efectiva y eficiente de acuerdo a los niveles de servicio requeridos. La transferencia del conocimiento debe incluir al entrenamiento inicial y continuo, el desarrollo de las habilidades, los materiales de entrenamiento, los manuales de operación, los manuales de procedimientos y escenarios de atención al usuario.

AI5 Adquirir e implantar
Adquirir recursos de TI

Objetivos de control detallados

AI5 Adquirir recursos de TI

AI5.1 Control de adquisición
Desarrollar y seguir un conjunto de procedimientos y estándares consistente con el proceso general de adquisiciones de la organización y con la estrategia de adquisición, para garantizar que la adquisición de infraestructura, instalaciones, hardware, software y servicios relacionados con TI, satisfagan los requerimientos del negocio.

AI5.2 Administración de contratos con proveedores
Formular un procedimiento para establecer, modificar y concluir contratos que apliquen a todos los proveedores. El procedimiento debe cubrir, al mínimo, responsabilidades y obligaciones legales, financieras, organizacionales, documentales, de desempeño, de seguridad de propiedad intelectual y de conclusión, así como obligaciones (que incluya cláusulas de penalización). Todos los contratos y las modificaciones a contratos las deben revisar asesores legales.

AI5.3 Selección de proveedores
Seleccionar proveedores mediante una práctica justa y formal para garantizar la escogencia del mejor con base en los requerimientos qu se han desarrollado con información de proveedores potenciales y acordados entre el cliente y el(los) proveedor(es).

AI5.4 Adquisición de software
Garantizar que se protegen los intereses de la organización en todos los acuerdos contractuales de adquisición. Incluir y reforzar los derechos y obligaciones de todas las partes en los términos contractuales para la adquisición de software involucrados en el suministro y uso continuo de software. Estos derechos y obligaciones pueden incluir la propiedad y licencia de propiedad intelectual, mantenimiento, garantías, procedimientos de arbitraje, condiciones para la actualización y aspectos de conveniencia que incluyen seguridad, custodia y derechos de acceso.

AI5.5 Adquisición de recursos de desarrollo
Garantizar la protección de los intereses de la organización en todos los acuerdos contractuales de adquisición. Incluir y hacer cumplir los derechos y obligaciones de todas las partes en los términos contractuales para la adquisición de recursos de desarrollo. Estos derechos y obligaciones pueden incluir la propiedad y licenciamiento de propiedad intelectual, aspectos de conveniencia incluyendo metodologías de desarrollo, lenguajes, pruebas, procesos de administración de calidad que comprenden los criterios de desempeño requeridos, revisión de desempeño, términos de pago, garantías, procedimientos de arbitraje, administración de recursos humanos y cumplimiento con las políticas de la organización.

AI5.6 Adquisición de infraestructura, instalaciones y servicios relacionados
Incluir y hacer cumplir los derechos y obligaciones de todas las partes en los términos contractuales, que comprendan los criterios de aceptación, para la adquisición de infraestructura, instalaciones y servicios relacionados. Estos derechos y obligaciones pueden abarcar los niveles de servicio, procedimientos de mantenimiento, controles de acceso, seguridad, revisión de desempeño, términos de pago y procedimientos de arbitraje.

AI6 Adquirir e implantar
Administrar cambios

Objetivos de control detallados

AI6 Administrar cambios

AI6.1 Estándares y procedimientos para cambios
Establecer procedimientos de administración de cambio formales para manejar de manera estándar todas las solicitudes (incluyendo mantenimiento y patches) para cambios a aplicaciones, procedimientos, procesos, parámetros de sistema y servicio, y las plataformas fundamentales.

AI6.2 Evaluación de impacto, priorización y autorización
Garantizar que todas las solicitudes de cambio se evalúan de una estructurada manera en cuanto a impactos en el sistema operacional y su funcionalidad. Esta evaluación deberá incluir categorización y priorización de los cambios. Previo a la migración hacia producción, los interesados correspondientes autorizan los cambios.

AI6.3 Cambios de emergencia
Establecer un proceso para definir, plantear, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido. La documentación y pruebas se realizan, posiblemente, después de la implantación del cambio de emergencia.

AI6.4 Seguimiento y reporte del estatus de cambio
Establecer un sistema de seguimiento y reporte para mantener actualizados a los solicitantes de cambio y a los interesados relevantes, acerca del estatus del cambio a las aplicaciones, a los procedimientos, a los procesos, parámetros del sistema y del servicio y las plataformas fundamentales.

AI6.5 Cierre y documentación del cambio
Siempre que se implantan cambios al sistema, actualizar el sistema asociado y la documentación de usuario y procedimientos correspondientes. Establecer un proceso de revisión para garantizar la implantación completa de los cambios.

AI7 **Adquirir e implantar**
Instalar y acreditar soluciones y cambios

Objetivos de control detallados

AI7 Instalar y acreditar soluciones y cambios

AI7.1 Entrenamiento
Entrenar al personal de los departamentos de usuario afectados y al grupo de operaciones de la función de TI de acuerdo con el plan definido de entrenamiento e implantación y a los materiales asociados, como parte de cada proyecto de desarrollo, implantación o modificación de sistemas de información.

AI7.2 Plan de prueba
Establecer un plan de pruebas y obtener la aprobación de las partes relevantes. El plan de pruebas se basa en los estándares de toda la organización y define roles, responsabilidades y criterios de éxito. El plan considera la preparación de pruebas (incluye la preparación del sitio), requerimientos de entrenamiento, instalación o actualización de un ambiente de pruebas definido, planear / ejecutar / documentar / retener casos de prueba, manejo y corrección de errores y aprobación formal. Con base en la evaluación de riesgos de fallas en el sistema y en la implantación, el plan deberá incluir los requerimientos de prueba de desempeño, stress, de usabilidad, piloto y de seguridad.

AI7.3 Plan de implantación
Establecer un plan de implantación y obtener la aprobación de las partes relevantes. El plan define el diseño de versiones (release), construcción de paquetes de versiones, procedimientos de implantación / instalación, manejo de incidentes, controles de distribución (incluye herramientas), almacenamiento de software, revisión de la versión y documentación de cambios. El plan deberá también incluir medidas de respaldo/ y vuelta atrás.

AI7.4 Ambiente de prueba
Establecer un ambiente de prueba separado para pruebas. Este ambiente debe reflejar el ambiente futuro de operaciones (por ejemplo, seguridad similar, controles internos y cargas de trabajo) para permitir pruebas acertadas. Se deben tener presentes los procedimientos para garantizar que los datos utilizados en el ambiente de prueba sean representativos de los datos (se limpian si es necesario) que se utilizarán eventualmente en el ambiente de operación. Proporcionar medidas adecuadas para prevenir la divulgación de datos sensibles. La documentación de los resultados de las pruebas se debe archivar.

AI7.5 Conversión de sistema y datos
Garantizar que los métodos de desarrollo de la organización, contemplen para todos los proyectos de desarrollo, implantación o modificación, que todos los elementos necesarios, tales como hardware, software, datos de transacciones, archivos maestros, respaldos y archivos, interfases con otros sistemas, procedimientos, documentación de sistemas, etc., sean convertidos del viejo al nuevo sistema de acuerdo con un plan preestablecido. Se desarrolla y mantiene una pista de auditoría de los resultados previos y posteriores a la conversión. Los propietarios del sistema llevan a cabo una verificación detallada del proceso inicial del nuevo sistema para confirmar una transición exitosa.

AI7.6 Prueba de cambios
Garantizar que se prueban los cambios de acuerdo con el plan de aceptación definido y en base en una evaluación de impacto y recursos que incluye el dimensionamiento del desempeño en un ambiente separado de prueba, por parte de un grupo de prueba independiente (de los constructores) antes de comenzar su uso en el ambiente de operación regular. Las pruebas paralelas o piloto se consideran parte del plan. Los controles de seguridad se prueban y evalúan antes de la liberación, de manera que se pueda certificar la efectividad de la seguridad. Los planes de respaldo/vuelta atrás se deben desarrollar y probar antes de transferir el cambio a producción.

AI7.7 Prueba final de aceptación
Garantizar que los procedimientos proporcionan, como parte de la aceptación final o prueba de aseguramientos de la calidad de los sistemas de información nuevos o modificados, una evaluación formal y la aprobación de los resultados de prueba por parte de la gerencia de los departamentos afectados del usuario y la función de TI. Las pruebas deberán cubrir todos los componentes del sistema de información (ejemplo, software aplicativo, instalaciones, procedimientos de tecnología y usuario) y garantizar que los requerimientos de seguridad de la información se satisfacen para todos los componentes. Los datos de prueba se deben salvar para propósitos de pistas de auditoría y para pruebas futuras.

AI7.8 Transferencia a producción
Implantar procedimientos formales para controlar la transferencia del sistema desde el ambiente de desarrollo al de pruebas, de acuerdo con el plan de implantación. La gerencia debe requerir que se obtenga la autorización del propietario del sistema antes de que se mueva un nuevo sistema a producción y que, antes de que se descontinúe el viejo sistema, el nuevo haya operado exitosamente a través de ciclos de producción diarios, mensuales, trimestrales y de fin de año.

AI7.9 Liberación de software
Garantizar que la liberación del software se regula con procedimientos formales que aseguren la autorización, acondicionamiento, pruebas de regresión, distribución, transferencia de control, rastreo de estatus, procedimientos de respaldo y notificación de usuario.

AI7.10 Distribución del sistema
Establecer procedimientos de control para asegurar la distribución oportuna y correcta, y la actualización de los componentes aprobados de la configuración. Esto implica controles de integridad; segregación de funciones entre los que construyen, prueban y operan; y adecuadas pistas de auditoría de todas las actividades.

AI7.11 Registro y rastreo de cambios
Automatizar el sistema utilizado para monitorear cambios a sistemas aplicativos para soportar el registro y rastreo de cambios hechos en aplicaciones, procedimientos, procesos, sistemas y parámetros de servicio, y a las plataformas subyacentes.

AI7.12 Revisión posterior a la implantación
Establecer procedimientos de acuerdo con los estándares de desarrollo y de cambios de la empresa, que requieren una revisión posterior a la implantación del sistema de información en operación para evaluar y reportar si el cambio satisfizo los requerimientos del cliente y entregó los beneficios visualizados, de la forma más rentable.

DS1 Entregar y dar soporte
Definir y administrar los niveles de servicio

Objetivos de control detallados

DS1 Definir y administrar los niveles de servicio

DS1.1 Marco de trabajo de la administración de los niveles de servicio
Definir un marco de trabajo que brinde un proceso formal de administración de niveles de servicio entre el cliente y el prestador de servicio. El marco de trabajo mantiene una alineación continua con los requerimientos y las prioridades de negocio y facilita el entendimiento común entre el cliente y el(los) prestador(es) de servicio. El marco de trabajo incluye procesos para la creación de requerimientos de servicio, definiciones de servicio, acuerdos de niveles de servicio (SLAs), acuerdos de niveles de operación (OLAs) y las fuentes de financiamiento. Estos atributos están organizados en un catálogo de servicios. El marco de trabajo define la estructura organizacional para la administración del nivel de servicio, incluyendo los roles, tareas y responsabilidades de los proveedores externos e internos y de los clientes.

DS1.2 Definición de servicios
Definiciones base de los servicios de TI sobre las características del servicio y los requerimientos de negocio, organizados y almacenados de manera centralizada por medio de la implantación de un enfoque de catálogo/portafolio de servicios.

DS1.3 Acuerdos de niveles de servicio
Definir y acordar convenios de niveles de servicio para todos los procesos críticos de TI con base en los requerimientos del cliente y las capacidades en TI. Esto incluye los compromisos del cliente, los requerimientos de soporte para el servicio, métricas cualitativas y cuantitativas para la medición del servicio firmado por los interesados, en caso de aplicar, los arreglos comerciales y de financiamiento, y los roles y responsabilidades, incluyendo la revisión del SLA. Los puntos a considerar son disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte, planeación de continuidad, seguridad y restricciones de demanda.

DS1.4 Acuerdos de niveles de operación
Asegurar que los acuerdos de niveles de operación expliquen cómo serán entregados técnicamente los servicios para soportar el (los) SLA(s) de manera óptima. Los OLAs especifican los procesos técnicos en términos entendibles para el proveedor y pueden soportar diversos SLAs.

DS1.5 Monitoreo y reporte del cumplimento de los niveles de servicio
Monitorear continuamente los criterios de desempeño especificados para el nivel de servicio. Los reportes sobre el cumplimiento de los niveles de servicio deben emitirse en un formato que sea entendible para los interesados. Las estadísticas de monitoreo son analizadas para identificar tendencias positivas y negativas tanto de servicios individuales como de los servicios en conjunto.

DS1.6 Revisión de los acuerdos de niveles de servicio y de los contratos
Revisar regularmente con los proveedores internos y externos los acuerdos de niveles de servicio y los contratos de apoyo, para asegurar que son efectivos, que están actualizados y que se han tomado en cuenta los cambios en requerimientos.

DS2 Entregar y dar soporte
Administrar los servicios de terceros

Objetivos de control detallados

DS2 Administrar los servicios de terceros

DS2.1 Identificación de las relaciones con todos los proveedores
Identificar todos los servicios de los proveedores y catalogarlos de acuerdo con el tipo de proveedor, la importancia y la criticidad. Mantener documentación formal de las relaciones técnicas y organizacionales incluyendo los roles y responsabilidades, metas, expectativas, entregables esperados y credenciales de los representantes de estos proveedores.

DS2.2 Administración de las relaciones con los proveedores
Formalizar el proceso de administración de relaciones con proveedores por cada proveedor. Los responsables de las relaciones deben coordinar a los proveedores y los clientes y asegurar la calidad de las relaciones con base en la confianza y la transparencia (por ejemplo, a través de acuerdos de niveles de servicio).

DS2.3 Administración de riesgos del proveedor
Identificar y mitigar los riesgos relacionados con la habilidad de los proveedores para mantener una efectiva entrega de servicios de forma segura y eficiente sobre una base de continuidad. Asegurar que los contratos están de acuerdo con los estándares universales del negocio de conformidad con los requerimientos legales y regulatorios. La administración del riesgo debe considerar además acuerdos de confidencialidad (NDAs), contratos de garantía, viabilidad de la continuidad del proveedor, conformidad con los requerimientos de seguridad, proveedores alternativos, penalizaciones e incentivos, etc.

DS2.4 Monitoreo del desempeño del proveedor
Establecer un proceso para monitorear la prestación del servicio para asegurar que el proveedor está cumpliendo con los requerimientos del negocio actuales y que se apega de manera continua a los acuerdos del contrato y a los convenios de niveles de servicio, y que el desempeño es competitivo respecto a los proveedores alternativos y a las condiciones del mercado.

DS3 **Entregar y dar soporte**
Administrar el desempeño y la capacidad

Objetivos de control detallados

DS3 Administrar el desempeño y la capacidad

DS3.1 Planeación del desempeño y la capacidad
Establecer un proceso de planeación para la revisión del desempeño y la capacidad de los recursos de TI, para asegurar la disponibilidad de la capacidad y del desempeño, con costos justificables, para procesar las cargas de trabajo acordadas tal como se determina en los SLAs. Los planes de capacidad y desempeño deben hacer uso de técnicas de modelado apropiadas para producir un modelo de desempeño, de capacidad y de rendimiento de los recursos de TI, tanto actual como pronosticado.

DS3.2 Capacidad y desempeño actual
Revisar la capacidad y desempeño actual de los recursos de TI en intervalos regulares para determinar si existe suficiente capacidad y desempeño para prestar los servicios con base en los niveles de servicio acordados.

DS3.3 Capacidad y desempeño futuros
Llevar a cabo un pronóstico de desempeño y capacidad de los recursos de TI en intervalos regulares para minimizar el riesgo de interrupciones del servicio originadas por falta de capacidad o degradación del desempeño. Identificar también el exceso de capacidad para una posible redistribución. Identificar las tendencias de las cargas de trabajo y determinar los pronósticos que serán parte de los planes de capacidad y de desempeño.

DS3.4 Disponibilidad de recursos de TI
Brindar la capacidad y desempeño requeridos tomando en cuenta aspectos como cargas de trabajo normales, contingencias, requerimientos de almacenamiento y ciclos de vida de los recursos de TI. Deben tomarse medidas cuando el desempeño y la capacidad no están en el nivel requerido, tales como dar prioridad a las tareas, mecanismos de tolerancia de fallas y prácticas de asignación de recursos. La gerencia debe garantizar que los planes de contingencia consideran de forma apropiada la disponibilidad, capacidad y desempeño de los recursos individuales de TI.

DS3.5 Monitoreo y reporte
Monitorear continuamente el desempeño y la capacidad de los recursos de TI. La información reunida sirve para dos propósitos:
- Mantener y poner a punto el desempeño actual dentro de TI y atender temas como resiliencia, contingencia, cargas de trabajo actuales y proyectadas, planes de almacenamiento y adquisición de recursos.
- Para reportar la disponibilidad hacia el negocio del servicio prestado como se requiere en los SLAs. Acompañar todos los reportes de excepción con recomendaciones para llevar a cabo acciones correctivas.

DS4 **Entregar y dar soporte**
Garantizar la continuidad del servicio

Objetivos de control detallados

DS4 Garantizar la continuidad de los servicios

DS4.1 IT Marco de trabajo de continuidad
Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización. El objetivo del marco de trabajo es ayudar en la determinación de la resistencia requerida de la infraestructura y de guiar el desarrollo de los planes de recuperación de desastres y de contingencias. El marco de trabajo debe tomar en cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes; así como las reglas y estructuras para documentar, probar y ejecutar la recuperación de desastres y los planes de contingencia de TI. El plan debe también considerar puntos tales como la identificación de recursos críticos, el monitoreo y reporte de la disponibilidad de recursos críticos, el procesamiento alternativo y los principios de respaldo y recuperación.

DS4.2 Planes de continuidad de TI
Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio. Los planes deben considerar requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TI. También deben cubrir los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas.

DS4.3 Recursos críticos de TI
Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación. Evitar la distracción de recuperar los puntos menos críticos y asegurarse de que la respuesta y la recuperación están alineadas con las necesidades prioritarias del negocio, asegurándose también que los costos se mantienen a un nivel aceptable y se cumple con los requerimientos regulatorios y contractuales. Considerar los requerimientos de resistencia, respuesta y recuperación para diferentes niveles de prioridad, por ejemplo, de una a cuatro horas, de cuatro a 24 horas, más de 24 horas y para periodos críticos de operación del negocio.

DS4.4 Mantenimiento del plan de continuidad de TI
Exhortar a la gerencia de TI a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio. Es esencial que los cambios en los procedimientos y las responsabilidades sean comunicados de forma clara y oportuna.

DS4.5 Pruebas del plan de continuidad de TI
Probar el plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas y, de acuerdo con los resultados, la implementación de un plan de acción. Considerar el alcance de las pruebas de recuperación en aplicaciones individuales, en escenarios de pruebas integrados, en pruebas de punta a punta y en pruebas integradas con el proveedor.

DS4.6 Entrenamiento del plan de continuidad de TI
Asegurarse de que todos las partes involucradas reciban sesiones de capacitación de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre. Verificar e incrementar el entrenamiento de acuerdo con los resultados de las pruebas de contingencia.

DS4.7 Distribución del plan de continuidad de TI
Determinar que existe una estrategia de distribución definida y administrada para asegurar que los planes se distribuyan de manera apropiada y segura y que estén disponibles entre las partes involucradas y autorizadas cuando y donde se requiera. Se debe prestar atención en hacerlos accesibles bajo cualquier escenario de desastre.

DS4.8 Recuperación y reanudación de los servicios de TI
Planear las acciones a tomar durante el periodo en que TI está recuperando y reanudando los servicios. Esto puede representar la activación de sitios de respaldo, el inicio de procesamiento alternativo, la comunicación a clientes y a los interesados, realizar procedimientos de reanudación, etc. Asegurarse de que los responsables del negocio entienden los tiempos de recuperación de TI y las inversiones necesarias en tecnología para soportar las necesidades de recuperación y reanudación del negocio.

DS4.9 Almacenamiento de respaldos fuera de las instalaciones
Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio. El contenido de los respaldos a almacenar debe determinarse en conjunto entre los responsables de los procesos de negocio y el personal de TI. La administración del sitio de almacenamiento externo a las instalaciones, debe apegarse a la política de clasificación de datos y a las prácticas de almacenamiento de datos de la empresa. La gerencia de TI debe asegurar que los acuerdos con sitios externos sean evaluados periódicamente, al menos una vez por año, respecto al contenido, a la protección ambiental y a la seguridad. Asegurarse de la compatibilidad del hardware y del software para poder recuperar los datos archivados y periódicamente probar y renovar los datos archivados.

DS4.10 Revisión post-reanudación
Una vez lograda una exitosa reanudación de las funciones de TI después de un desastre, determinar si la gerencia de TI ha establecido procedimientos para valorar lo adecuado del plan y actualizar el plan en consecuencia.

DS5 Entregar y dar soporte
Garantizar la seguridad de los sistemas

Objetivos de control detallados

DS5 Garantizar la seguridad de los sistemas

DS5.1 Administración de la seguridad de TI
Administrar la seguridad de TI al nivel más apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.

DS5.2 Plan de seguridad de TI
Trasladar los requerimientos de información del negocio, la configuración de TI, los planes de acción del riesgo de la información y la cultura sobre la seguridad en la información a un plan global de seguridad de TI. El plan se implementa en políticas y procedimientos de seguridad en conjunto con inversiones apropiadas en servicios, personal, software y hardware. Las políticas y procedimientos de seguridad se comunican a los interesados y a los usuarios.

DS5.3 Administración de identidad
Todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, operación del sistema, desarrollo y mantenimiento) deben ser identificables de manera única. Los derechos de acceso del usuario a sistemas y datos deben estar alineados con necesidades de negocio definidas y documentadas y con requerimientos de trabajo. Los derechos de acceso del usuario son solicitados por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se implementan y se mantienen actualizadas medidas técnicas y procedimientos rentables, para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso.

DS5.4 Administración de cuentas del usuario
Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por la gerencia de cuentas de usuario. Debe incluirse un procedimiento que describa al responsable de los datos o del sistema como otorgar los privilegios de acceso. Estos procedimientos deben aplicar para todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relacionados al acceso a los sistemas e información de la empresa son acordados contractualmente para todos los tipos de usuarios. La gerencia debe llevar a cabo una revisión regular de todas las cuentas y los privilegios asociados.

DS5.5 Pruebas, vigilancia y monitoreo de la seguridad
Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser reacreditada periódicamente para garantizar que se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema (logging) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención. El acceso a la información de ingreso al sistema está alineado con los requerimientos del negocio en términos de requerimientos de retención y de derechos de acceso.

DS5.6 Definición de incidente de seguridad
Garantizar que las características de los posibles incidentes de seguridad sean definidas y comunicadas de forma clara, de manera que los problemas de seguridad sean atendidos de forma apropiada por medio del proceso de administración de problemas o incidentes. Las características incluyen una descripción de lo que se considera un incidente de seguridad y su nivel de impacto. Un número limitado de niveles de impacto se definen para cada incidente, se identifican las acciones específicas requeridas y las personas que necesitan ser notificadas.

DS5.7 Protección de la tecnología de seguridad
Garantizar que la tecnología importante relacionada con la seguridad no sea susceptible de sabotaje y que la documentación de seguridad no se divulgue de forma innecesaria, es decir, que mantenga un perfil bajo. Sin embargo no hay que hacer que la seguridad de los sistemas dependa de la confidencialidad de las especificaciones de seguridad.

DS5.8 Administración de llaves criptográficas
Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas.

DS5.9 Prevención, detección y corrección de software malicioso
Garantizar que se cuente con medidas de prevención, detección y corrección (en especial contar con parches de seguridad y control de virus actualizados) a lo largo de toda la organización para proteger a los sistemas de información y a la tecnología contra software malicioso (virus, gusanos, spyware, correo basura, software fraudulento desarrollado internamente, etc.).

DS5.10 Seguridad de la red
Garantizar que se utilizan técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.

DS5.11 Intercambio de datos sensitivos
Garantizar que las transacciones de datos sensibles sean intercambiadas solamente a través de una ruta o medio confiable con controles para brindar autenticidad de contenido, prueba de envío, prueba de recepción y no rechazo del origen.

DS6 Entregar y dar soporte
Identificar y asignar costos

Objetivos de control detallados

DS6 Identificar y asignar costos

DS6.1 Definición de servicios
Identificar todos los costos de TI y equipararlos a los servicios de TI para soportar un modelo de costos transparente. Los servicios de TI deben vincularse a los procesos del negocio de forma que el negocio pueda identificar los niveles de facturación de los servicios asociados.

DS6.2 Contabilización de TI
Registrar y asignar los costos actuales de acuerdo con el modelo de costos definido. Las variaciones entre los presupuestos y los costos actuales deben analizarse y reportarse de acuerdo con los sistemas de medición financiera de la empresa.

DS6.3 Modelación de costos y cargos
Con base en la definición del servicio, definir un modelo de costos que incluya costos directos, indirectos y fijos de los servicios, y que ayude al cálculo de tarifas de reintegros de cobro por servicio. El modelo de costos debe estar alineado con los procedimientos de contabilización de costos de la empresa. El modelo de costos de TI debe garantizar que los cargos por servicios son identificables, medibles y predecibles por parte de los usuarios para propiciar el adecuado uso de recursos. La gerencia del usuario debe poder verificar el uso actual y los cargos de los servicios.

DS6.4 Mantenimiento del modelo de costos
Revisar y comparar de forma regular lo apropiado del modelo de costos/recargos para mantener su relevancia para el negocio en evolución y para las actividades de TI.

DS7 Entregar y dar soporte
Educar y entrenar a los usuarios

Objetivos de control detallados

DS7 Educar y entrenar a los usuarios

DS7.1 Identificación de necesidades de entrenamiento y educación
Establecer y actualizar de forma regular un programa de entrenamiento para cada grupo objetivo de empleados, que incluya:

- Estrategias y requerimientos actuales y futuros del negocio.
- Valores corporativos (valores éticos, cultura de control y seguridad, etc.)
- Implementación de nuevo software e infraestructura de TI (paquetes y aplicaciones)
- Habilidades, perfiles de competencias y certificaciones actuales y/o credenciales necesarias.
- Métodos de impartición (por ejemplo, aula, web), tamaño del grupo objetivo, accesibilidad y tiempo.

DS7.2 Impartición de entrenamiento y educación
Con base en las necesidades de entrenamiento identificadas, identificar: a los grupos objetivo y a sus miembros, a los mecanismos de impartición eficientes, a maestros, instructores y consejeros. Designar instructores y organizar el entrenamiento con tiempo suficiente. Debe tomarse nota del registro (incluyendo los prerrequisitos), la asistencia, y de las evaluaciones de desempeño.

DS7.3 Evaluación del entrenamiento recibido
Al finalizar la entrenamiento, evaluar el contenido de la entrenamiento respecto a la relevancia, calidad, efectividad, percepción y retención del conocimiento, costo y valor. Los resultados de esta evaluación deben contribuir en la definición futura de los planes de estudio y de las sesiones de entrenamiento.

DS8 Entregar y dar soporte
Administrar la mesa de servicio y los incidentes

Objetivos de control detallados

DS8 Administrar la mesa de servicio y los incidentes

DS8.1 Mesa de Servicios
Establecer la función de mesa de servicio, la cual es la conexión del usuario con TI, para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Deben existir procedimientos de monitoreo y escalamiento basados en los niveles de servicio acordados en los SLAs, que permitan clasificar y priorizar cualquier problema reportado como incidente, solicitud de servicio o solicitud de información. Medir la satisfacción del usuario final respecto a la calidad de la mesa de servicios y de los servicios de TI.

DS8.2 Registro de consultas de clientes
Establecer una función y sistema que permita el registro y rastreo de llamadas, incidentes, solicitudes de servicio y necesidades de información. Debe trabajar estrechamente con los procesos de administración de incidentes, administración de problemas, administración de cambios, administración de capacidad y administración de disponibilidad. Los incidentes deben clasificarse de acuerdo al negocio y a la prioridad del servicio y enrutarse al equipo de administración de problemas apropiado y se debe mantener informados a los clientes sobre el estatus de sus consultas.

DS8.3 Escalamiento de incidentes
Establecer procedimientos de mesa de servicios de manera que los incidentes que no puedan resolverse de forma inmediata sean escalados apropiadamente de acuerdo con los límites acordados en el SLA y, si es adecuado, brindar soluciones alternas. Garantizar que la asignación de incidentes y el monitoreo del ciclo de vida permanecen en la mesa de servicios, independientemente de qué grupo de TI esté trabajando en las actividades de resolución.

DS8.4 Cierre de incidentes
Establecer procedimientos para el monitoreo puntual de la resolución de consultas de los clientes. Cuando se resuelve el incidente la mesa de servicios debe registrar la causa raíz, si la conoce, y confirmar que la acción tomada fue acordada con el cliente.

DS8.5 Análisis de tendencias
Emitir reportes de la actividad dela mesa de servicios para permitir a la gerencia medir el desempeño del servicio y los tiempos de respuesta, así como para identificar tendencias de problemas recurrentes de forma que el servicio pueda mejorarse de forma continua.

DS9 Entregar y dar soporte
Administrar la configuración

Objetivos de control detallados

DS9 Administrar la configuración

DS9.1 Repositorio de configuración y línea base
Establecer un repositorio central que contenga toda la información referente a los elementos de configuración. Este repositorio incluye hardware, software aplicativo, middleware, parámetros, documentación, procedimientos y herramientas para operar, acceder y utilizar los sistemas y los servicios. La información importante a considerar es el nombre, números de versión y detalles de licenciamiento. Una línea base de elementos de configuración debe mantenerse para cada sistema y servicio, como un punto de control al cual regresar después de realizar cambios.

DS9.2 Identificación y mantenimiento de elementos de configuración
Contar con procedimientos en orden para:
- Identificar elementos de configuración y sus atributos
- Registrar elementos de configuración nuevos, modificados y eliminados
- Identificar y mantener las relaciones entre los elementos de configuración y el repositorio de configuraciones.
- Actualizar los elementos de configuración existentes en el repositorio de configuraciones.
- Prevenir la inclusión de software no-autorizado

Estos procedimientos deben brindar una adecuada autorización y registro de todas las acciones sobre el repositorio de configuración y estar integrados de forma apropiada con los procedimientos de administración de cambios y administración de problemas.

DS9.3 Revisión de integridad de la configuración
Revisar y verificar de manera regular, utilizando cuando sea necesario herramientas apropiadas, el estatus de los elementos de configuración para confirmar la integridad de la configuración de datos actual e histórica y para comparar con la situación actual. Revisar periódicamente contra la política de uso de software, la existencia de cualquier software personal o no autorizado de cualquier instancia de software por encima de los acuerdos de licenciamiento actuales. Los errores y las desviaciones deben reportarse, atenderse y corregirse.

DS10 Entregar y dar soporte
Administración de problemas

Objetivos de control detallados

DS10 Administración de problemas

DS10.1 Identificación y clasificación de problemas
Implementar procesos para reportar y clasificar problemas que han sido identificados como parte de la administración de incidentes. Los pasos involucrados en la clasificación de problemas son similares a los pasos para clasificar incidentes; son determinar la categoría, impacto, urgencia y prioridad. Los problemas deben categorizarse de manera apropiada en grupos o dominios relacionados (por ejemplo, hardware, software, software de soporte). Estos grupos pueden coincidir con las responsabilidades organizacionales o con la base de usuarios y clientes, y son la base para asignar los problemas al personal de soporte.

DS10.2 Rastreo y resolución de problemas
El sistema de administración de problemas debe mantener pistas de auditoría adecuadas que permitan rastrear, analizar y determinar la causa raíz de todos los problemas reportados considerando:
- Todos los elementos de configuración asociados
- Problemas e incidentes sobresalientes
- Errores conocidos y sospechados

Identificar e iniciar soluciones sostenibles indicando la causa raíz, incrementando las solicitudes de cambio por medio del proceso de administración de cambios establecido. En todo el proceso de resolución, la administración de problemas debe obtener reportes regulares de la administración de cambios sobre el progreso en la resolución de problemas o errores. La administración de problemas debe monitorear el continuo impacto de los problemas y errores conocidos en los servicios a los usuarios. En caso de que el impacto se vuelva severo, la administración de problemas debe escalar el problema, tal vez refiriéndolo a un comité determinado para incrementar la prioridad de la solicitud del cambio (RFC) o para implementar un cambio urgente, lo que resulte más pertinente. El avance de la resolución de un problema debe ser monitoreado contra los SLAs.

DS10.3 Cierre de problemas
Disponer de un procedimiento para cerrar registros de problemas ya sea después de confirmar la eliminación exitosa del error conocido o después de acordar con el negocio cómo manejar el problema de manera alternativa.

DS10.4 Integración de las administraciones de cambios, configuración y problemas
Para garantizar una adecuada administración de problemas e incidentes, integrar los procesos relacionados de administración de cambios, configuración y problemas. Monitorear cuánto esfuerzo se aplica en apagar fuegos, en lugar de permitir mejoras al negocio y, en los casos que sean necesarios, mejorar estos procesos para minimizar los problemas.

DS11 Entregar y dar soporte
Administración de datos

Objetivos de control detallados

DS11 Administración de la información

DS11.1 Requerimientos del negocio para administración de datos
Establecer mecanismos para garantizar que el negocio reciba los documentos originales que espera, que se procese toda la información recibida por parte del negocio, que se preparen y entreguen todos los reportes de salida que requiere el negocio y que las necesidades de reinicio y reproceso estén soportadas.

DS11.2 Acuerdos de almacenamiento y conservación
Definir e implementar procedimientos para el archivo y almacenamiento de los datos, de manera que los datos permanezcan accesibles y utilizables. Los procedimientos deben considerar los requerimientos de recuperación, la rentabilidad, la integridad continua y los requerimientos de seguridad. Para cumplir con los requerimientos legales, regulatorios y de negocio, establecer mecanismos de almacenamiento y conservación de documentos, datos, archivos, programas, reportes y mensajes (entrantes y salientes), así como la información (claves, certificados) utilizada para encripción y autenticación.

DS11.3 Sistema de administración de librerías de medios
Definir e implementar procedimientos para mantener un inventario de medios en sitio y garantizar su integridad y su uso. Los procedimientos deben permitir la revisión oportuna y el seguimiento de cualquier discrepancia que se perciba.

DS11.4 Eliminación
Definir e implementar procedimientos para prevenir el acceso a datos sensitivos y al software desde equipos o medios una vez que son eliminados o transferidos para otro uso. Dichos procedimientos deben garantizar que los datos marcados como borrados o desechados no puedan recuperarse.

DS11.5 Respaldo y restauración
Definir e implementar procedimientos de respaldo y restauración de los sistemas, datos y configuraciones que estén alineados con los requerimientos del negocio y con el plan de continuidad. Verificar el cumplimiento de los procedimientos de respaldo y verificar la capacidad y el tiempo requerido para tener una restauración completa y exitosa. Probar los medios de respaldo y el proceso de restauración.

DS11.6 Requerimientos de seguridad para la administración de datos
Establecer mecanismos para identificar y aplicar requerimientos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos. Esto incluye registros físicos, transmisiones de datos y cualquier información almacenada fuera del sitio.

DS12 Entregar y dar soporte
Administración del ambiente físico

Objetivos de control detallados

DS12 Administración del ambiente físico

DS12.1 Selección y diseño del centro de datos
Definir y seleccionar los centros de datos físicos para el equipo de TI para soportar la estrategia de tecnología ligada a la estrategia del negocio. Esta selección y diseño del esquema de un centro de datos debe tomar en cuenta el riesgo asociado con desastres naturales y causados por el hombre. También debe considerar las leyes y regulaciones correspondientes, tales como regulaciones de seguridad y de salud en el trabajo.

DS12.2 Medidas de seguridad física
Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio. Las medidas deben incluir, pero no limitarse al esquema del perímetro de seguridad, de las zonas de seguridad, la ubicación de equipo crítico y de las áreas de envío y recepción. En particular, mantenga un perfil bajo respecto a la presencia de operaciones críticas de TI. Deben establecerse las responsabilidades sobre el monitoreo y los procedimientos de reporte y de resolución de incidentes de seguridad física.

DS12.3 Acceso Físico
Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo las emergencias. El acceso a locales, edificios y áreas debe justificarse, autorizarse, registrarse y monitorearse. Esto aplica para todas las personas que accedan a las instalaciones, incluyendo personal, clientes, proveedores, visitantes o cualquier tercera persona.

DS12.4 Protección contra factores ambientales
Diseñar e implementar medidas de protección contra factores ambientales. Deben instalarse dispositivos y equipo especializado para monitorear y controlar el ambiente.

DS12.5 Administración de instalaciones físicas
Administrar las instalaciones, incluyendo el equipo de comunicaciones y de suministro de energía, de acuerdo con las leyes y los reglamentos, los requerimientos técnicos y del negocio, las especificaciones del proveedor y los lineamientos de seguridad y salud.

DS13 Entregar y dar soporte
Administración de operaciones

Objetivos de control detallados

DS13 Administración de operaciones

DS13.1 Procedimientos e instrucciones de operación
Definir, implementar y mantener procedimientos estándar para operaciones de TI y garantizar que el personal de operaciones está familiarizado con todas las tareas de operación relativas a ellos. Los procedimientos de operación deben cubrir los procesos de entrega de turno (transferencia formal de la actividad, estatus, actualizaciones, problemas de operación, procedimientos de escalamiento, y reportes sobre las responsabilidades actuales) para garantizar la continuidad de las operaciones.

DS13.2 Programación de tareas
Organizar la programación de trabajos, procesos y tareas en la secuencia más eficiente, maximizando el rendimiento y la utilización para cumplir con los requerimientos del negocio. Deben autorizarse los programas iniciales así como los cambios a estos programas. Los procedimientos deben implementarse para identificar, investigar y aprobar las salidas de los programas estándar agendados.

DS13.3 Monitoreo de la infraestructura de TI
Definir e implementar procedimientos para monitorear la infraestructura de TI y los eventos relacionados. Garantizar que en los registros de operación se almacena suficiente información cronológica para permitir la reconstrucción, revisión y análisis de las secuencias de tiempo de las operaciones y de las otras actividades que soportan o que están alrededor de las operaciones.

DS13.4 Documentos sensitivos y dispositivos de salida.
Establecer resguardos físicos, prácticas de registro y administración de inventarios adecuados sobre los activos de TI más sensitivos tales como formas, instrumentos negociables, impresoras de uso especial o dispositivos de seguridad.

DS13.5 Mantenimiento preventivo del hardware
Definir e implementar procedimientos para garantizar el mantenimiento oportuno de la infraestructura para reducir la frecuencia y el impacto de las fallas o de la disminución del desempeño.

ME1 Monitorear y evaluar
Monitorear y evaluar el desempeño de TI

Objetivos de control detallados

ME1 Monitorear y evaluar el desempeño de TI

ME1.1 Enfoque del Monitoreo
Garantizar que la gerencia establezca un marco de trabajo de monitoreo general y un enfoque que definan el alcance, la metodología y el proceso a seguir para monitorear la contribución de TI a los resultados de los procesos de administración de programas y de administración del portafolio empresarial y aquellos procesos que son específicos para la entrega de la capacidad y los servicios de TI. El marco de trabajo se debería integrar con el sistema de administración del desempeño corporativo.

ME1.2 Definición y recolección de datos de monitoreo
Garantizar que la gerencia de TI, trabajando en conjunto con el negocio, defina un conjunto balanceado de objetivos, mediciones, metas y comparaciones de desempeño y que estas se encuentren acordadas formalmente con el negocio y otros interesados relevantes. Los indicadores de desempeño deberían incluir:

- La contribución al negocio que incluya, pero que no se limite a, la información financiera
- Desempeño contra el plan estratégico del negocio y de TI
- Riesgo y cumplimiento de las regulaciones
- Satisfacción del usuario interno y externo
- Procesos clave de TI que incluyan desarrollo y entrega del servicio
- Actividades orientadas a futuro, por ejemplo, la tecnología emergente, la infraestructura re-utilizable, habilidades del personal de TI y del negocio

Se deben establecer procesos para recolectar información oportuna y precisa para reportar el avance contra las metas.

ME1.3 Método de monitoreo
Garantizar que el proceso de monitoreo implante un método (ej. Balanced Scorecard), que brinde una visión sucinta y desde todos los ángulos del desempeño de TI y que se adapte al sistema de monitoreo de la empresa.

ME1.4 Evaluación del desempeño
Comparar de forma periódica el desempeño contra las metas, realizar análisis de la causa raíz e iniciar medidas correctivas para resolver las causas subyacentes.

ME1.5 Reportes al consejo directivo y a ejecutivos
Proporcionar reportes administrativos para ser revisados por la alta dirección sobre el avance de la organización hacia metas identificadas, específicamente en términos del desempeño del portafolio empresarial de programas de inversión habilitados por TI, niveles de servicio de programas individuales y la contribución de TI a ese desempeño. Los reportes de estatus deben incluir el grado en el que se han alcanzado los objetivos planeados, los entregables obtenidos, las metas de desempeño alcanzadas y los riesgos mitigados. Durante la revisión, se debe identificar cualquier desviación respecto al desempeño esperado y se deben iniciar y reportar las medidas administrativas adecuadas.

ME1.6 Acciones correctivas
Identificar e iniciar medidas correctivas basadas en el monitoreo del desempeño, evaluación y reportes. Esto incluye el seguimiento de todo el monitoreo, de los reportes y de las evaluaciones con:
- Revisión, negociación y establecimiento de respuestas administrativas
- Asignación de responsabilidades por la corrección
- Rastreo de los resultados de las acciones comprometidas

ME2 Monitorear y evaluar

Monitorear y evaluar el control interno

Objetivos de control detallados

ME2 Monitorear y evaluar el control interno

ME2.1 Monitorear el marco de trabajo de control interno
Monitorear de forma continua el ambiente de control y el marco de control de TI. Se debe realizar la evaluación usando mejores prácticas de la industria y se debería utilizar benchmarking para mejorar el ambiente y el marco de trabajo de control de TI.

ME2.2 Revisiones de Auditoría
Monitorear y reportar la efectividad de los controles internos sobre TI por medio de revisiones de auditoría incluyendo, por ejemplo, el cumplimiento de políticas y estándares, seguridad de la información, controles de cambios y controles establecidos en acuerdos de niveles de servicio.

ME2.3 Excepciones de control
Registrar la información referente a todas las excepciones de control y garantizar que esto conduzca al análisis de las causas subyacentes y a la toma de acciones correctivas. La gerencia debería decidir cuáles excepciones se deberían comunicar al individuo responsable de la función y cuáles excepciones deberían ser escaladas. La gerencia también es responsable de informar a las partes afectadas.

ME2.4 Auto-evaluación de control
Evaluar la completitud y efectividad de los controles internos de la administración de los procesos, políticas y contratos de TI por medio de un programa continuo de auto-evaluación.

ME2.5 Aseguramiento del control interno
Obtener, según sea necesario, aseguramiento adicional de la completitud y efectividad de los controles internos por medio de revisiones de terceros. Dichas revisiones pueden ser realizadas por la función de cumplimiento corporativo o, a solicitud de la gerencia, por auditoría interna o por auditores y consultores externos o por organismos de certificación. Se deben verificar las aptitudes de los individuos que realicen la auditoria, por ej. Un Auditor de Sistemas de Información Certificado™ (CISA® por sus siglas en Inglés) debe asignarse.

ME2.6 Control interno para terceros
Determinar el estado de los controles internos de cada proveedor externos de servicios. Confirmar que los proveedores externos de servicios cumplan con los requerimientos legales y regulatorios y con las obligaciones contractuales. Esto puede ser provisto por una auditoría externa o se puede obtener de una revisión por parte de auditoría interna y por los resultados de otras auditorias.

ME2.7 Acciones correctivas
Identificar e iniciar medidas correctivas basadas en las evaluaciones y en los reportes de control. Esto incluye el seguimiento de todas las evaluaciones y los reportes con:
- La revisión, negociación y establecimiento de respuestas administrativas
- La asignación de responsabilidades para corrección (puede incluir la aceptación de los riesgos)
- El rastreo de los resultados de las acciones comprometidas

ME3 Monitorear y evaluar
Garantizar el cumplimiento regulatorio

Objetivos de control detallados

ME3 Garantizar el cumplimiento regulatorio

ME3.1 Identificar las leyes y regulaciones con impacto potencial sobre TI
Definir e implantar un proceso para garantizar la identificación oportuna de requerimientos locales e internacionales legales, contractuales, de políticas y regulatorios, relacionados con la información, con la prestación de servicios de información – incluyendo servicios de terceros – y con la función, procesos e infraestructura de TI. Tomar en cuenta las leyes y reglamentos de comercio electrónico, flujo de datos, privacidad, controles internos, reportes financieros, reglamentos específicos de la industria, propiedad intelectual y derechos de autor, además de salud y seguridad.

ME3.2 Optimizar la respuesta a requerimientos regulatorios
Revisar y optimizar las políticas, estándares y procedimientos de TI para garantizar que los requisitos legales y regulatorios se cubran de forma eficiente.

ME3.3 Evaluación del cumplimiento con requerimientos regulatorios
Evaluar de forma eficiente el cumplimiento de las políticas, estándares y procedimientos de TI, incluyendo los requerimientos legales y regulatorios, con base en la supervisión del gobierno de la gerencia de TI y del negocio y la operación de los controles internos.

ME3.4 Aseguramiento positivo del cumplimiento
Definir e implantar procedimientos para obtener y reportar un aseguramiento del cumplimiento y, donde sea necesario, que el propietario del proceso haya tomado las medidas correctivas oportunas para resolver cualquier brecha de cumplimiento. Integrar los reportes de avance y estado del cumplimiento de TI con salidas similares provenientes de otras funciones de negocio

ME3.5 Reportes integrados.
Integrar los reportes de TI sobre cumplimiento regulatorio con las salidas similares provenientes de otras funciones del negocio.

ME4 Monitorear y evaluar
Proporcionar gobierno de TI

Objetivos de control detallados

ME4 Proporcionar gobierno de TI

ME4.1 Establecer un marco de trabajo de gobierno para TI
Trabajar con el consejo directivo para definir y establecer un marco de trabajo para el gobierno de TI, incluyendo liderazgo, procesos, roles y responsabilidades, requerimientos de información, y estructuras organizacionales para garantizar que los programas de inversión habilitados por TI de la empresa ofrezcan y estén alineados con las estrategias y objetivos empresariales. El marco de trabajo debería proporcionar vínculos claros entre la estrategia empresarial, el portafolio de programas de inversiones habilitadas por TI que ejecutan la estrategia, los programas de inversión individual y los proyectos de negocio y de TI que forman los programas. El marco de trabajo debería definir una rendición de cuentas y prácticas incontrovertibles para evitar fallas de control interno y de supervisión. El marco de trabajo debería ser consistente con el ambiente completo de control empresarial y con los principios de control generalmente aceptados y estar basado en el proceso y en el marco de control de TI.

ME4.2 Alineamiento estratégico
Facilitar el entendimiento del consejo directivo y de los ejecutivos sobre temas estratégicos de TI tales como el rol de TI, características propias y capacidades de la tecnología. Garantizar que existe un entendimiento compartido entre el negocio y la función de TI sobre la contribución potencial de TI a la estrategia del negocio. Asegurarse de que exista un entendimiento claro de que el valor de TI sólo se obtiene cuando las inversiones habilitadas con TI se administran como un portafolio de programas que incluyen el alcance completo de los cambios que el negocio debe realizar para optimizar el valor proveniente de las capacidades que tiene TI para lograr la estrategia. Trabajar con el consejo directivo para definir e implantar organismos de gobierno, tales como un comité estratégico de TI, para brindar una orientación estratégica a la gerencia respecto a TI, garantizando así que tanto la estrategia como los objetivos se distribuyan en cascada hacia las unidades de negocio y hacia las unidades de TI y que se desarrolle certidumbre y confianza entre el negocio y TI. Facilitar la alineación de TI con el negocio en lo referente a estrategia y operaciones, fomentando la co-responsabilidad entre el negocio y TI en la toma de decisiones estratégicas y en la obtención de los beneficios provenientes de las inversiones habilitadas con TI.

ME4.3 Entrega de valor
Administrar los programas de inversión habilitados con TI, así como otros activos y servicios de TI, para asegurar que ofrezcan el mayor valor posible para apoyar la estrategia y los objetivos empresariales. Asegurarse de que los resultados de negocio esperados de las inversiones habilitadas por TI y el alcance completo del esfuerzo requerido para lograr esos resultados esté bien entendido, que se generen casos de negocio integrales y consistentes, y que los aprueben los interesados, que los activos y las inversiones se administren a lo largo del ciclo de vida económico, y que se lleve a cabo una administración activa del logro de los beneficios, tales como la contribución a nuevos servicios, ganancias de eficiencia y un mejor grado de reacción a los requerimientos de los clientes. Implantar un enfoque disciplinado hacia la administración por portafolio, programa y proyecto, enfatizando que el negocio asume la propiedad de todas las inversiones habilitadas con TI y que TI garantiza la optimización de los costos por la prestación de los servicios y capacidades de TI. Asegurar que las inversiones en tecnología estén estandarizadas a mayor grado posible para evitar el aumento en costo y complejidad de una proliferación de soluciones técnicas.

ME4.4 Administración de recursos
Optimizar la inversión, uso y asignación de los activos de TI por medio de evaluaciones periódicas, garantizando que TI cuente con recursos suficientes, competentes y capaces para ejecutar los objetivos estratégicos actuales y futuros y seguir el ritmo de los requerimientos del negocio. La dirección debería implantar políticas claras, consistentes y reforzadas sobre recursos humanos y políticas de sustitución para garantizar que se satisfagan los requerimientos de recursos de manera efectiva y para adaptarse a las políticas y estándares de la arquitectura. La infraestructura de TI se debe evaluar periódicamente para asegurar que esté estandarizada siempre que sea posible y que exista la interoperabilidad según sea requiera.

ME4.5 Administración de riesgos.
Trabajar en conjunto con el consejo directivo para definir el nivel de riesgo de TI aceptable por la empresa. Comunicar este nivel de riesgo hacia la organización y acordar el plan de administración de riesgos de TI. Integrar las responsabilidades de administración de riesgos en la organización, asegurando que tanto el negocio como TI evalúen y reporten periódicamente los riesgos asociados con TI y su impacto en el negocio. Garantizar que la gerencia de TI haga seguimiento a la exposición a los riesgos, poniendo especial atención en las fallas y debilidades de control interno y de supervisión, así como su impacto actual y potencial en el negocio. La posición de riesgo empresarial en TI debería ser transparente para todos los interesados.

ME4.6 Medición del desempeño.
Informar el desempeño relevante del portafolio de los programas de TI al consejo directivo y a los ejecutivos de manera oportuna y precisa. Los informes administrativos que se deben entregar a la alta dirección para su revisión deben incluir el avance de la empresa hacia metas identificadas. Los reportes de estatus deben incluir el grado al cual se han logrado los objetivos planeados, entregables obtenidos, metas de desempeño alcanzadas y los riesgos mitigados. Integrar los informes con salidas similares de otras funciones del negocio. Las mediciones de desempeño deberían ser aprobadas por los interesados clave. El consejo directivo y los ejecutivos deberían cuestionar estos informes de desempeño y la gerencia de TI debería tener la oportunidad de explicar las desviaciones y los problemas de desempeño. Después de la revisión, se deben iniciar y controlar las acciones administrativas apropiadas.

ME4.7 Aseguramiento independiente.
Garantizar que la organización establezca y mantenga una función competente y que cuente con el personal adecuado y/o busque servicios de aseguramiento externo para proporcionar al consejo directivo– esto ocurrirá probablemente a través de un comité de auditoría – aseguramiento independiente y oportuno sobre el cumplimiento que tiene TI respecto a sus políticas, estándares y procedimientos, así como con las prácticas generalmente aceptadas.

ANEXO 4

GLOSARIO

CIO:

Director de información [algunas veces Director de Tecnología (CTO, por sus siglas en inglés)].

FOCUS GROUP

El **grupo focal**, *focus group* en inglés, también conocida como **sesiones de grupo**, es una de las formas de los estudios cualitativos en el que se reúne a un grupo de personas para indagar acerca de actitudes y reacciones frente a un producto, servicio, concepto, publicidad, idea o empaque. Las preguntas son respondidas por la interacción del grupo en una dinámica donde los participantes se sienten cómodos y libres de hablar y comentar sus opiniones.

IMPLICANCIA

Contradicción de términos entre si, impedimento.

MYSTERY SHOPPING

Es un método para valorar los servicios de atención cliente de forma discreta y profesional. Siempre que exista una interacción entre cliente y dependiente, Mystery Shopping podrá entrar en acción

Es su oportunidad para valorar la calidad de los servicios ofrecidos en un gran número de establecimientos de servicios o venta al por menor, desde tiendas de moda hasta hoteles, pasando por restaurantes o bancos

GLOSARIO

PERFORMANCE

Es un **anglicismo -palabra (voz) inglesa- evitable**, que tiene dos acepciones básicas en castellano: No obstante, tal palabra se ha difundido en las artes a partir de la expresión inglesa "*performance art*" y proviene de la concepción del arte en vivo como arte conceptual contemporáneo y heredero de los *happenings*, actions, fluxus events y body art a finales de los años 1960 y con auge durante los 1970.

La historia del "performance art" empieza a principios del siglo XX, con las acciones en vivo del futurismo, el constructivismo, dadaísmo y surrealismo, por ejemplo las *exhibiciones no convencionales* llevadas a cabo en el Cabaret Voltaire por Richard Huelsenbeck, Tristan Tzara y otros

Se define como un medio de expresión alternativa, que tiene como objetivo obtener una reacción del espectador a través de acciones de un detonador, el cual puede ser un humano y al mismo tiempo utilizar otros medios como la fotografía, el video, la pintura, la música; para lograr un momento de éxtasis artístico.

TIMING:

Es la cualidad que hace o quiebra un peleador. Es la habilidad para reconocer y reaccionar inmediatamente a los cambios y oportunidades durante los entrenamientos de sparring o peleas. Por ejemplo, su oponente se tropieza. Usted ve el error, instantáneamente tomando ventaja de ello con una patada o puñetazo. Eso es timing