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

"PROCESO DE AUDITORÍA DE SISTEMAS BASADO EN EL DOMINIO DE ENTREGAR Y DAR SOPORTE DEL MODELO COBIT APLICADO AL SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL"

TRABAJO DE GRADUACIÓN PRESENTADO POR:
CONSTANZA RODRÍGUEZ, ANA MARÍA
AVALOS CHÁVEZ, ISABEL CRISTINA
GALDÁMEZ CANALES, MERCEDES GUADALUPE

PARA OPTAR AL GRADO DE:
LICENCIATURA EN CONTADURIA PÚBLICA

AGOSTO DE 2008

SAN SALVADOR, EL SALVADOR, CENTRO AMÉRICA

AUTORIDADES UNIVERSITARIAS

Rector	:	Ing. Rufino Antonio Quesada Sánchez
Secretario	:	Lic. Vladimir Alfaro Chávez
Decano de la Facultad de Ciencias Económicas	:	Msc. Roger Armando Arias Alvarado
Secretario de la Facultad de Ciencias Económicas	:	Ing. José Cariaco Gutiérrez Contreras
Asesor Director	:	Lic. Mario Hernan Cornejo Perez
Jurado examinador	:	Lic. Mario Hernan Cornejo Perez
		Lic. Roberto Carlos Jovel

Agosto de 2008

San Salvador, El Salvador, Centro América

AGRADECIMIENTOS

A Dios Todo Poderoso, por guiar mis pasos y hacer que tome las decisiones correctas, por darme fuerza y sabiduría para poder lograr mis metas. A mis padres Benedicto y Haydee por el inmenso amor y apoyo incondicional brindado durante mi vida, a mis hermanos y amigos por los ánimos y oraciones que me sirvieron para seguir adelante.

Ana María Constanza Rodríguez

A Dios y a la Virgencita María, por guiar mi vida y darme sabiduría en las decisiones correctas para el logro de mis metas, a mis padres William e Isabel que siempre han estado conmigo apoyándome con mucho amor y cariño a mis hermanos y amigos por estar a mi lado en las alegrías y en las angustias de verdad gracias. Este logro se lo dedico a mi mami por su infinito amor incondicional conmigo, te amo mami.

Isabel Cristina Avalos Chávez

A Dios todo poderoso por estar siempre en mi vida a Virgencita María por guiar mis pasos como madre e hija, a mis padres por su apoyo condicional e infinito amor, a mi hijo por estar siempre conmigo en cada paso de este logro, a mi hermana, familia y amigos por estar siempre a mi lado.

Mercedes Guadalupe Galdámez Canales

RESUMEN EJECUTIVO

El origen del presente trabajo titulado “PROCESO DE AUDITORIA DE SISTEMAS BASADO EN EL DOMINIO ENTREGAR Y DAR SOPORTE DEL MODELO COBIT APLICADO AL SISTEMA DE ADMINISTRACION FINANCIERA INTEGRADO MUNICIPAL” se fundamenta en el auge del uso de tecnologías de información para el procesamiento de las operaciones y actividades de las instituciones públicas y privadas.

El objetivo de este trabajo es desarrollar un proceso de Auditoría de Sistemas, tomando como base la metodología COBIT que específicamente está diseñada para la evaluación de Sistemas de Información.

Para el desarrollo de la investigación se realizó un estudio analítico, con el fin de comprobar y comprender la problemática identificada, para lo cual se consideraron como unidades de observación las alcaldías que tienen implementado SAFIMU II, las cuales son: Antiguo Cuscatlán, Ciudad Arce, San Antonio del Monte, Acajutla, Juayua y San Martin; en tal sentido se desarrollo un cuestionario para recabar información, dirigido al personal de Tesorería, Contabilidad e Informática de las instituciones anteriormente mencionadas.
Los resultados obtenidos se analizaron e interpretaron a través de la tabulación y gráficos de los mismos.

La información obtenida reveló que las municipalidades tienen deficiencias con respeto al control interno debido a que no se practica auditorías al sistema donde se dé a conocer las vulnerabilidades, áreas a mejorar y áreas de oportunidad de sistema; esto conlleva a errores u omisiones en el procesamiento de la información, razón por la cual los usuarios consideran que la confiabilidad de la reportes que suministra el sistema se considera medio.

INDICE

CAPITULO II METODOLOGIA DE LA INVESTIGACIÓN Y DIAGNOSTICO

CAPITULO III PROCESO DE AUDITORÍA DE SISTEMAS BASADO EN EL DOMINIO DE ENTREGAR Y DAR SOPORTE DEL MODELO COBIT APLICADO AL SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADA MUNICIPAL

CAPITULO IV CONCLUSIONES Y RECOMENDACIONES

INDICE DE FIGURAS Y TABLAS

CAPITULO I
MARCO TEORICO

1. MARCO TEORICO
1.1 AUDITORÍA
1.1.1 ANTECEDENTES DE AUDITORÍA

La Auditoría existe hace mucho tiempo, desde que los propietarios entregaron la administración de sus bienes a otras personas, lo que hacía que en sus inicios fuera en esencia un control contra el desfalco y el incumplimiento de las normas establecidas por el propietario, el Estado u otros.

En un principio se limito a las verificaciones de los registros contables, dedicándose a observar si los mismos eran exactos. Por lo tanto esta era la forma primaria: Confrontar lo escrito con las pruebas de lo acontecido y las respectivas referencias de los registros.

La Auditoría surge a raíz del desarrollo producido por la Revolución Industrial del siglo XIX. En consecuencia, en el año de 1851 se crea en Venecia la primera asociación de auditores y posteriormente en ese mismo siglo se produjeron eventos que propiciaron el desarrollo de la profesión, así en 1862 se reconoció en Inglaterra la auditoría como profesión independiente.

Con el transcurrir del tiempo y debido al desarrollo de la auditoría en Inglaterra, se trasladaron hacia los Estados Unidos de Norte América muchos auditores ingleses que venían a auditar y revisar los diferentes intereses en este país de las compañías inglesas, dando así lugar al desarrollo de la profesión en Norte América y América Latina, creándose en los primeros años de ese siglo el Instituto Americano de Contadores.

En la actualidad en nuestro país la auditoría es perfilada como una gran profesión ya que el sector es realmente muy amplio, debido a que además de ser un requerimiento legal, es de vital importancia para las empresas ya que por medio de ella se verifica la razonabilidad de la información financiera.

1.1.2 DEFINICION

La palabra auditoría proviene del latín **auditorius** y de esta surge auditor, que es definido como el que tiene la virtud de oír y revisar cuentas, pero debe estar encaminado a un objetivo específico que es el de evaluar la eficiencia y eficacia con que se está operando para que, por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación.

La auditoría también se define como "La revisión independiente que realiza un auditor profesional, aplicando técnicas, métodos y procedimientos especializados, a fin de evaluar el cumplimiento de las funciones, actividades, tareas y procedimientos de una entidad administrativa, así como dictaminar sobre el resultado de dicha evaluación".

1.1.3 TIPOS DE AUDITORÍA

1.1.3.1 AUDITORÍA POR SU LUGAR DE APLICACIÓN:

- Auditoría Externa
- Auditoría Interna

1.1.3.2 AUDITORÍA POR SU ÁREA DE APLICACIÓN:

- Auditoría Financiera
- Auditoría Administrativa
- Auditoría Operacional

- Auditoría Integral
- Auditoría Gubernamental y
- Auditoría de Sistemas

1.1.3.4 AUDITORÍAS EN ÁREAS ESPECÍFICAS:

- Auditorías al área médica (evaluación medico-sanitaria)
- Auditoría al desarrollo de obras y construcciones (evaluación de ingeniería)
- Auditoría Fiscal
- Auditoría Laboral
- Auditoría de proyectos de Inversión
- Auditoría a la caja chica o caja mayor (arqueo)
- Auditoría al manejo de mercancías (inventarios)
- Auditoría Ambiental
- Auditoría de Sistemas

1.2 SISTEMAS DE INFORMACIÓN

Antes de introducir conceptos sobre auditoría informática es necesario conocer un poco acerca de los sistemas de información, los cuales son el objeto de análisis de la propia auditoría informática.

1.2.1 DEFINICION

Un sistema de información se define como un conjunto de procedimientos interrelacionados que forman un todo, es decir, obtiene, procesa, almacena y distribuye información (datos manipulados) para apoyar la toma de decisiones y el control en una organización. Igualmente apoya la coordinación, análisis de problemas, visualización de aspectos complejos, entre otros aspectos.

1.2.2 IMPORTANCIA

La información es de vital importancia para la gerencia porque permite el logro de las metas establecidas previamente, el objetivo principal de los sistemas es sintetizar la información para la toma decisiones y obtener los objetivos trazados a corto, mediano y largo plazo por la administración.
En la actualidad todas las organizaciones están concientes de la importancia de la información y cuanto mas precisa y oportuna sea esta, mayor será la utilidad de esta en la toma de decisiones. Muchos miembros de la alta gerencia están concientes que la información es una fuente de fuerza competitiva la cual les da la fuerza de actuar más rápido en momentos críticos principalmente en la aplicación de nuevos servicios, y toma de decisiones.

1.2.3 CARACTERÍSTICAS

Un sistema de información gerencial esta dirigido a asistir a la gerencia y al personal operativo, especialmente en cuanto al control, planeación de las actividades de la organización para producir la salida de información deseada. Dentro estas características tenemos:

- Tipo de sistema.
  Sistema de búsqueda global con sus sistemas integrados en donde se dan énfasis a la planeación y al control de las actividades del negocio.
- Reportes desarrollados.
  Se elaboran reportes que ayuden a la planeaciòn y al control de las actividades actuales y futuras del negocio. Además los reportes de control se distribuyen entre los gerentes para mostrar los resultados de operaciones anteriores.
- Reportes por excepción.

El Principio de “administración por excepción” se emplea para resaltar desviaciones contrarias a los planes actuales, tales como variación estándar y variación contra el presupuesto.

- Extenso uso de terminales de entrada/salida.
  Las terminales de entrada/salida para permitir al gerente la recuperación rápida de la información oportuna sobre las operaciones de planeación y control, así como para permitir el procesamiento de datos transaccionales.
- Modo de procesamiento.
  Se da énfasis en el procesamiento interactivo para producir rápidamente la información deseada, además, el procesamiento por lote se emplea donde se considera conveniente.
- Elementos de datos.
  Se utiliza una base de datos para almacenar los elementos de datos requeridos por los usuarios autorizados.
- Tipos de archivo.
  Se da énfasis a archivos ubicados en almacenamiento aleatorio o de acceso directo para permitir al gerente obtener la información almacenada en línea.
- Modelos matemáticos.
  Se emplean modelos matemáticos estándar y medida de investigación de operaciones para controlar constantemente las operaciones.

1.2.4 TIPOS

Existen diferentes tipos de sistemas de información, entre ellos se pueden mencionar:

- Sistemas de Transacciones
- Sistemas de Conocimiento
- Sistemas Expertos
- Sistemas de Apoyo a Grupos
- Sistema de ejecutivos

1.2.5 COMPONENTES

Los elementos básicos de un sistema de información se listan a continuación:

- Herramientas tecnológicas (hardware, software)
- Procedimientos
- El equipo computacional: el hardware necesario para que el sistema de información pueda operar.
- El recurso humano que interactúa con el Sistema de Información (usuarios).

1.2.6 RELACION DE LA INFORMACION CON UN SISTEMA

Dicha de relación en términos simples es transformar datos en información que puede ser utilizada por la gerencia, por medio de un sistema que cumpla con las exigencias de la organización, estas generalmente siguen el siguiente proceso:

- Datos.
  Son la materia prima no estructuradas previamente para su posterior procesamiento por medio del sistema establecido.
- Sistema.
  Se define como un conjunto ordenado de métodos, procedimientos y recursos diseñados para facilitar el logro de objetivos.
- Información.
  Es la selección y organización de datos en base a las necesidades del usuario, del problema a ser resuelto o algún otro criterio especifico.

1.3 AUDITORÍA DE SISTEMAS

1.3.1 DEFINICION

Es la revisión técnica especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del centro de computo.

1.3.2 OBJETIVOS

La evaluación a los sistemas computacionales, a la administración del centro de cómputo, al desarrollo de proyectos informáticos, a la seguridad de los sistemas computacionales y a todo lo relacionado con ellos será considerada bajo los siguientes objetivos:

- Realizar una evaluación con personal multidisciplinario y capacitado en el área de sistemas, con el fin de emitir un dictamen independiente sobre la razonabilidad de las operaciones del sistema y la gestión administrativa del área de informática.
- Hacer una evaluación sobre el uso de recursos financieros en las áreas del centro de información, así como el aprovechamiento del sistema computacional, sus equipos periféricos e instalaciones.
- Evaluar el uso y aprovechamiento de los equipos de cómputo sus periféricos, la instalación inmobiliaria del centro de cómputo, así como el uso de sus recursos técnicos y materiales para el procesamiento de información.

- Evaluar el aprovechamiento de los sistemas de procesamiento, sus sistemas operativos, los lenguajes, programas y paquetería de aplicación y desarrollo, así como el desarrollo e instalación de nuevos sistemas.
- Evaluar el cumplimiento de planes, programas, estándares, políticas, normas y lineamientos que regulan las funciones y actividades de las áreas y de los sistemas de procesamiento de información, así como de su personal y de los usuarios del centro de información.
- Realizar la evaluación de las áreas, actividades y funciones de una empresa, contando con el apoyo de los sistemas computacionales, de los programas especiales para auditoría y de la paquetería que sirven de soporte para el desarrollo de auditorías por medio de la computadora.

1.3.3 TIPOS

1.3.3.1 AUDITORÍA AL CICLO DE VIDA DEL DESARROLLO DE SISTEMAS

La auditoría a los sistemas en desarrollo se encarga de evaluar, según el ciclo de vida del desarrollo de un sistema, los controles y el uso de una metodología hasta la liberación del sistema
En la actualidad el principal desafió en el desarrollo del software es reducir los costos e incrementar la calidad, explotando al máximo los recursos disponibles para lograr el máximo costo-beneficio.

ATRIBUTOS INDISPENSABLES DE LOS SISTEMAS

Cuatro atributos son indispensables para todo sistema:

- **Mantenimiento**
  Inicialmente se pensaba que un sistema no necesitaba mantenimiento, pues este nunca cambiaria. Sin embargo, es

cada vez mayor la flexibilidad que los usuarios requieren con respecto al sistema, por lo tanto los sistemas actuales deben contemplar modificaciones, por lo que el software no debe estar bien documentado para facilitar cualquier modificación.

- **Confiabilidad**
  Debe cumplir con las expectativas del usuario y no fallar mas de lo permitido.
- **Eficiencia**
  Se debe maximizar el uso de memoria y procesador.
- **Interfases amigables**
  Para facilitar su uso

Es muy común encontrarse con sistemas que no cumplen con dichos atributos, pues no cuentan con una planeación adecuada, y se desarrollan de manera desorganizada. Estos sistemas generalmente se desechan antes de concluirse y si llegan a su fin tienen un uso mínimo por no cumplir con las necesidades del usuario, ser muy complicados, defectuosos y costosos.

CONTROLES

Los controles presentes en el desarrollo de un sistema tienen como finalidad asegurar el desarrollo de sistemas de calidad dentro de los costos y tiempos estimados, contando con altos niveles de eficiencia y confiabilidad.

CLASIFICACION DE CONTROLES

- **Controles principales**
  Existen cinco tipos principales de controles dentro del desarrollo de sistemas:
  - Participación activa y aprobación dentro tanto de directivos como de usuarios
  - Estándares y lineamientos de desarrollo
  - Administración del proyecto

- Controles en las pruebas y conversiones
- Revisiones de post-implementación

- **Controles preventivos**
  - Metodología apropiada
  - Administración del proyecto
  - Contratación y entrenamiento de personal
  - Listas de puntos a revisar
  - Documentación

- **Controles detectivos**
  - Revisiones y aprobaciones técnicas
  - Revisiones y aprobaciones de la gerencia y el usuario
  - Participación del auditor
  - Prueba del sistema
  - Revisión posterior a la implantación

- **Controles correctivos**
  - Documentación

FASES SUJETAS A CONTROL

El reconocer que hay un ciclo para el desarrollo de sistemas es el primer paso para su control, el hecho de dividir el desarrollo en fases permite predecir el proyecto integro, analizar y evaluar cada parte con mayor concentración y monitorear continuamente la calidad y avance del trabajo.

Cada fase de control se divide en fases que involucran diversas actividades, responsabilidades y productos finales. Los proyectos de desarrollo se reestructuran como acumulativos, cada actividad o etapa descansa en la precedente.

Cada sistema de información tiene cuatro principales áreas o fases sujetas a control durante el proceso del ciclo de vida del desarrollo de sistemas.

PLANEACION

Requisición de servicios

La requisición de servicios es un documento en que se solicita el desarrollo de un nuevo sistema de información, el cual debe contener:

- Definición del proyecto
  - Justificación
  - Ambiente (operativo, personal sindicalizado, estudiantes, cursos muy remotos)
  - Alcance
  - Restricciones (No después de 3 meses)
  - Beneficios (ahorro de papel, optimización del tiempo de consulta)
- Integración del equipo de trabajo y sus responsabilidades
- Definición de requisitos de información, nuevos y existentes
- Aprobación del proyecto

Estudio de factibilidad

- Factibilidad tecnológica

  Debe hacerla informática.

  Disponibilidad de la tecnología que satisfaga las necesidades del usuario, actualización o complemento a los recursos actuales.
- Factibilidad económica

  Debe hacerla: Informática, adquisiciones y finanzas
  - Costos actuales contra costos de cada alternativa (personal de desarrollo, equipo, software, entrenamiento, preparación de la entrada, conversión de archivos de prueba, operación, costo del software, etc.)
  - Identificación y cuantificación de beneficios

- Factibilidad operativa
  Debe hacerla el usuario
  Determinar que se operara, utilizara, tomando en cuenta factores como la resistencia al cambio, características del personal, ubicación de las instalaciones, etc.
- Plan maestro del proyecto (Puntos de control y calendarización de actividades). Cantidad de actividades y tiempo que se requiere.
- Estado general de la función de desarrollo
- Aprobación del proyecto

ANÁLISIS Y DISEÑO

Análisis y diseño general del sistema

Esta fase se encarga de determinar las especificaciones del usuario, es decir todo aquel que dentro del contexto de la organización se relaciona con el sistema. Existen usuarios primarios y secundarios. El primario es aquel que usa directamente en sus tareas los resultados del sistema de información; el secundario es que introduce datos al sistema.

Esta fase incluye:

- Estructura general del sistema
- Definición y documentación de los informes
  - Contenido y formato de los informes
  - Frecuencia de producción de reportes
  - Lista de distribución de reportes
  - Periodos de retención de informes
  - Controles sobre la salida
- Definición y documentación de los requisitos de entrada
  - Requisitos de edición y validación (control). Edición: requisitos y características de los datos de entrada.
  - Revisiones de seguridad para la protección de la exclusividad

- Controles sobre la entrada
- Definición y documentación de los requisitos de archivos
  - Definición de los tipos de registros o estructuración de bases de datos
  - Métodos de organización
  - Niveles de seguridad y controles de acceso
  - Periodos de respaldo y retención
- Definición y documentación de los requisitos de procesamiento (Manuales y computarizados)

Análisis y diseño detallado del sistema

En esta etapa se definen las especificaciones técnicas; es decir las características y definiciones técnicas y operativas del sistema, lo cual es responsabilidad del líder del proyecto en informática.

Las especificaciones incluyen:

- Instrucciones para programación
- Itinerario para el desarrollo de programas/módulos
- Matrices de archivos, programas, módulos/programas
- Selección de los lenguajes de programación
- Controles del operador
- Instrucciones al operador en caso de interrupciones
- Procedimientos de respaldo, reinicio y recuperación

En específico, esta fase incluye:

- Especificaciones de programas de computo y controles programados (costo-beneficio)
- Diseño de pistas de auditoría
- Estándares de documentación de programas
  - Nombre de la aplicación
  - Diagrama del sistema
  - Aspectos generales del programa
  - Formato de archivos de entrada
  - Diseño y muestra de reporte
  - Diseño y muestra de pantalla

- Descripción detallada de los principales procedimientos de cálculo, clasificación, incorporados al programa
- Criterios de selección
- Procedimientos de conexión de cifras
- Instrucciones de corrida y listado de procedimientos de ejecución
- Método de almacenamiento y localización del programa
- Requerimiento de equipo
- Listado de programa fuente

- Estándares para la prueba de programas y del sistema total
  - Procedimientos para establecer datos de prueba
  - Asignación de responsabilidades para la preparación de datos y evaluación de los resultados
  - autorización y aceptación escrita

DESARROLLO

Es hacer en el sistema

Programación

Consiste en el desarrollo y elaboración de la documentación de programas, cada programa que se desarrolla debe documentarse.

Prueba modular e integral del sistema

Se debe ejercer presiones para hacer fallar el sistema. Las pruebas deben efectuarse con volúmenes de datos y bajo condiciones reales de operación, cualquier error detectado debe ser cuidadosamente analizado y corregido, preparándose un reporte de excepciones: problema, causa y solución, indicando la fecha de corrección. La prueba debe estar bien dirigida, organizada, exhaustiva y eficiente y debe involucrar:

- Los procedimientos manuales, incluyendo el área de mesa de control.
- Los programas de cómputo y procedimientos de ejecución.

- Archivos de prueba, las cuales deben ser realizadas bajo condiciones reales en cuanto a volúmenes de de información deben hacerse convivir con todo el ambiente operativo en el que van a operar.

En el caso de proyectos grandes conviene desarrollar un plan de instalación piloto o por módulos así como asignando responsabilidades.

Las pruebas deben realizarse en el siguiente orden: primero el programador, segundo el analista programador y tercero el usuario.

Desarrollo de manuales

La revisión de la documentación de una aplicación involucra identificar su existencia, analizar su contenido y juzgar su oportunidad y disponibilidad. La calidad del mantenimiento de sistemas depende en gran medida de la calidad de la documentación, además de la claridad y organización de la documentación, debe dedicarse especial atención al tipo de personas a quien va dirigido.

La documentación de los sistemas consiste en los manuales correspondientes:

- **Manual de operación**

  Cuando se realiza descentralizadamente en el centro de computo, caso contrario, puede ser uno solo en el manual de usuario.

  - Representación grafica de la estructura del sistema
  - Función de cada programa
  - Requerimientos de equipo
  - Tamaño estimado de archivos (normal y máximo)
  - Explicación de los mensajes de la consola, junto con las respuesta adecuada del operador
  - Instrucciones de corrida y listado de procedimientos de ejecución
  - Calendarización de procesos
  - Parámetro para alimentar

- Creación de salida y su distribución
- Identificación adecuada de la etiquetas de los archivos de salida
- Puntos de reinicio y recuperación
- Procedimientos para notificar errores o condiciones defectuosas
- Procedimientos para casos de emergencias

- **Manual de usuario**

  Ayuda al usuario primario y secundario a trabajar con el sistema.

  - Representación grafica de la estructura del sistema
  - Procedimientos de preparación de datos
  - Asignación de prioridades
  - Tiempo probable de respuesta y recepción de productos finales
  - Especificaciones y diseño de entrada de datos (formatos y pantallas de captura)
  - Especificaciones y diseño de salidas de datos (reportes y pantallas de consultas)
  - Controles de usuario
  - Procedimientos para resolver errores e incongruencias
  - Controles sobre las entradas y salidas

- **Manual del sistema**

  Permite al informático hacer modificaciones con menor grado de riesgo.

  - Representación grafica de la estructura del sistema
  - Documentación de cada programa de computo

ENTRENAMIENTO

Se tiene que programar en varias fechas para que quien no pueda asistir la primera vez, asista a otra. Debe incluir:

- Métodos de la enseñanza
- Mecanismos para la evaluación del aprendizaje

IMPLANTACION

Es la puesta en marcha del sistema.

Conversión

La etapa de conversión significa abandonar el sistema actual, manual o computarizado, para emigrar a uno nuevo y conciliar los resultados. Los controles en la etapa de conversión persiguen en asegurar que los archivos iniciales proporcionan en punto de arranque adecuado, marcando: itinerarios, compromisos, condiciones de éxito.

Normalmente, la etapa de conversión que requiere el desarrollo de programas de conversión de archivos de un formato a otro.

Esta fase incluye:

- Identificar fuentes de información
- Recopilación de información
- Revisiones de exactitud de los documentos previos a la conversión
- Evaluación de los resultados de la conversión

Revisión de Post implantación

(Lo logrado versus lo planeado)

La revisión post implantación es una revisión formalmente planeada, que debe realizarse después de transcurridos tres o seis meses de la instalación definitiva. La revisión post implantación normalmente involucra:

- Evaluación del cumplimiento de las necesidades del usuario
- Análisis de costo-beneficio
- Oportunidad de la información
- Efectividad de los controles
- Control de modificaciones al sistema

MANTENIMIENTO

Debido a que lo único constante en sistemas es el cambio, en esta fase se analiza y evalúa como ha sido el mantenimiento de sistemas

para proteger a la instalación de cambios incorrectos, no autorizados i decisiones equivocadas. El primer cambio surge el día que se instala el sistema.

En mantenimiento de sistemas se origina por los siguientes factores:

- Cambios en la normativa interna y externa de la entidad
- Desarrollo tecnológico
- Comportamiento del entorno, competencia
- Costos excesivos

Normalmente los cambios obligatorios se efectúan con menos controles, por la presión implícita, mientras que los cambios por mejoras (refinamiento, creatividad, ventajas tecnológicas) se atienden más controladamente. El auditor le preocupa que haya un sistema para administrar los cambios.

La documentación de los cambios debe mostrar:

- Control numérico
- Fecha de implantación
- Persona solicitante
- Persona que efectuó el cambio
- Justificación
- Descripción narrativa
- Documentación de las pruebas
- Autorización formal

Todo cambio deberá originar la actualización de la documentación correspondiente. La conciencia de la calidad, seguridad y control debe iniciarse en las áreas de desarrollo, contemplando un balance adecuado con la productividad de lo sistemas.

1.4.3.2 AUDITORÍA A SISTEMAS DE INFORMACIÓN EN OPERACIÓN

La auditoría de sistemas en operación se refiere a aquellos sistemas que se encuentran ya liberados, es decir que han pasado de la etapa de pruebas y están en uso en el área usuaria correspondiente. Las auditorias a los sistemas en operación generalmente surgen cuando se presenta algún problema en su funcionamiento y más aun si dicho problema tiene consecuencias graves para el negocio, es decir, si el nivel de riesgo que presenta el sistema es alto.

El propósito de los auditores dentro de los sistemas en operación es evaluar la suficiencia y cumplimiento de controles para administrar operar y utilizar los sistemas en operación con el objeto de garantizar la confiabilidad, seguridad, y utilidad de los mismos.

OBJETIVOS BASICOS DE CONTROL

En una auditoría de sistemas, los objetivos se refieren a lo que el sistema se debe controlar, siendo específico los siguientes elementos:

- **Totalidad**

  Este objetivo persigue que todas las operaciones:

  - Se registren inicialmente
  - Se suministren a procesamiento electrónico de datos
  - Se alimente al computador
  - Actualicen los diferentes archivos manejados en la aplicación
  - Se consideren en los procedimientos de cálculo, totalización, categorización, etc.

- **Exactitud**

  Este objetivo persigue que los datos importantes de cada operación o actividad sean correctos:

  - Inicialmente (manualmente-automáticamente: intereses, depreciaciones)
  - Una ves alimentados al computador
  - Al actualizar los diferentes archivos manejados en la aplicación
  - Al considerarse por los procedimientos de calculo, totalización, categorización.

- **Autorización**

  Se debe introducir el PED lo autorizado

  El control primario de una operación dada es el acto de su autorización, la que consiste en que alguien, comparándola con los planees condiciones, limitaciones o conocimiento general de lo que constituye una operación correcta, decide si es o no valida; el acto debe de ser ejecutado por un persona reconocida en el sistema, establecido como quien tiene la facultad (jerárquico) y a competencia (capacidad) para hacerlo.

- **Mantenimiento**

  Este objetivo persigue que las operaciones/actividades permanezcan completas y exactas en el tiempo.

- **Oportunidad**

  Este objetivo persigue que el registro de las operaciones/actividades y que la información que se produce sea oportuna para la toma de decisiones.

- **Utilidad**

  Este objetivo persigue que la información que se produce sea útil para la toma de decisiones, esto se logra por medio de:

- Manejo de términos apropiados
- Razonable tiempo de respuesta
- El sistema debe ser fácil de usar
- El sistema debe tener ayuda en línea
- Adecuados documentos fuente
- Adecuado manejo de menús

Principales Técnicas de Control

- Chequeo de secuencia numérica
- Chequeo de uno por uno, reportes de computo contra documentos fuente
- Comparación contra datos prerregistrados
- Comparación de totales de control
- Digito verificador
- Verificación de razonabilidad
- Cheque de generaciones de activo
- Reproceso selectivo de partidas
- Control de pendientes
- Lista de recordatorio

Disciplinas sobre los Controles Básicos

- Segregación de funciones
- Adecuada custodia de activos/acceso controlado o restringido:
  - Acceso físico
  - Acceso lógico
- Supervisión

Niveles de Ejercicio de los Controles de Entrada

Pueden ejercerse sobre:

- Campo
  Contiene una serie de caracteres relacionados entre si. Ejemplo en un formato de inscripción a una universidad el nombre de una persona es un campo y el apellido es otro
- Registro
  Es un conjunto de campos relacionados entre si
- Archivo
  Es un conjunto de registros relacionados entre si
- Lote
  Es una parte de todos los registros

Controles en la Entrada de Datos

Las actividades que se realizan para la alimentación de datos, frecuentemente involucran de manera importante la intervención humana. Los controles es esta etapa buscan que la información de entrada sea validada y cualquier error detectado sea controlado, de manera que la alimentación de datos al computador sea autentica, exacta, completa y oportuna.
Para los controles en la entrada de datos se usan técnicas para identificar errores en los datos antes de ser procesados y son ejercidos durante el flujo de la información. Entre estas se pueden mencionar las siguientes:

- Verificaciones sobre campos
- Verificaciones sobre registros
- Verificaciones sobre lotes
- Verificaciones sobre archivos

Etapa de Entrada de Datos

La entrada de datos a un sistema se da en tres etapas: captación, preparación y alimentación.
La captación u obtención de datos se refiere a la identificación y registro de los eventos que son relevantes en la entidad, para la adecuada operación de la misma, tal captación puede darse por los siguientes métodos:

- Documental
- Directo
- Hibrido

Controles sobre el Proceso de Datos

La etapa de proceso es la responsable de calcular, clasificar, ordenar y sumarizar los datos.

- **Principales problemas en el proceso**
  - Estilo de programación
  - Manejo del redondeo (multiplicaciones, divisiones)
  - Intervención de operador (puede equivocarse en el uso de cintas)
  - Manejo de overflow (excede formado. ejemplo: longitud para el resultado de una suma)
  - Manejo de cifras corrida a corrida
  - Manejo

- **Principales riesgos**
  - Intervención de programadores incautos o inexpertos
  - Falta de estándares
  - Utilización de la versión correcta del programa
  - Caídas del sistema
  - Desconocimiento de políticas y procedimientos (normatividad)

- **Controles requeridos**
  - El adecuado manejo de redondeo
  - La impresión de totales corrida a corrida
  - Minimización de la intervención del operador
  - Establecimiento de cálculos redundantes en el caso de campos de resultados sensibles o importantes
  - Evitar el traslape de longitud (overflow)
  - Verificación de la razonabilidad de los resultados (ejemplo pago neto)
  - Conciliar totales de corrida a corrida

Controles en la Salida de Información

- **Controles sobre la salida en procesos Batch**
  - Controles sobre diseños de reportes
  - Controles sobre papelería
  - Controles sobre programas de reporte
  - Controles sobre archivos de impresión
  - Controles sobre la recolección y distribución de reportes
  - Controles sobre la destrucción de reportes
  - Controles de la verificación de la salida

- **Controles sobre la salida en procesos en línea**
  - Estructura de las pantallas de consulta
  - Controles de tiempo
  - Controles de distribución

1.3.4 NORMATIVA APLICABLE A LA AUDITORÍA DE SISTEMAS

1.3.4.1 NORMAS INTERNACIONALES DE AUDITORÍA (NIA'S)

Dentro de la normativa Internacional para realizar auditorías, es importante recalcar que no existen criterios específicos que sean aplicables a una Auditoría de Sistemas, no obstante se toman en cuenta ciertas normas que son de carácter general ya que se aplican a cualquier proceso de auditoría y entre ellas tenemos:

300 PLANEACION DE UNA AUDITORÍA DE ESTADOS FINANCIEROS

El objetivo es establecer normas y proporcionar lineamientos sobre la planeación de una auditoría.
Planeacion significa desarrollar una estrategia general y un enfoque detallado para la naturaleza, oportunidad y alcance esperados de la auditoría.

315 ENTENDIMIENTO DE LA ENTIDAD Y SU ENTORNO Y EVALUACIÓN DE LOS RIESGOS DE REPRESENTACION ERRONEA DE IMPORTANCIA RELATIVA.

El objetivo 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 en una auditoría.

330 PROCEDIMIENTOS DEL AUDITOR EN RESPUESTA A LOS RIESGOS EVALUADOS.

El objetivo es establecer normas y proporcionar guías para determinar respuestas globales, diseñar y desempeñar procedimientos adicionales de auditoría para responder a los riesgos evaluados de representación errónea de importancia relativa.

620 USO DEL TRABAJO DE UN EXPERTO.

El objetivo 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.

700 EL DICTAMEN DEL AUDITOR INDEPENDIENTE SOBRE UN JUEGO COMPLETO DE ESTADOS FINANCIEROS DE PROPÓSITO GENERAL

El objetivo es establecer normas y proporcionar lineamientos sobre la forma y contenido del dictamen del auditor emitido como resultado de una auditoría de un juego completo de estados financieros de propósito general desempeñada por un auditor independiente.

1.3.4.2 NORMAS GENERALES PARA LOS SISTEMAS DE AUDITORÍA DE LA INFORMACIÓN (ISACA)

INTRODUCCIÓN

La Asociación de Auditoría y Control de Sistemas de Información (ISACA) determinó que por la naturaleza especializada de la auditoría de los sistemas de información y las habilidades necesarias para llevar a cabo este tipo de auditoría, requieren el desarrollo y la promulgación de Normas Generales para la Auditoría de los Sistemas de Información.

OBJETIVO

El objetivo de estas normas es informar a los auditores acerca del nivel mínimo de rendimiento aceptable para satisfacer las responsabilidades profesionales establecidas en el Código de Ética

Profesional y de informar a la gerencia y a otras partes interesadas de las expectativas de la profesión con respecto al trabajo de aquellos que la ejercen.

CONTENIDO

010 Título de auditoría

010.010 Responsabilidad, autoridad y rendimiento de cuentas

La responsabilidad, la autoridad y el rendimiento de cuentas abarcados por la función de auditoría de los sistemas de información se documentarán de la manera apropiada en un título de auditoría o carta de contratación.

020 Independencia

020.010 Independencia profesional

En todas las cuestiones relacionadas con la auditoría, el auditor de sistemas de información deberá ser independiente de la organización auditada tanto en actitud como en apariencia.

020.020 Relación organizativa

La función de auditoría de los sistemas de información deberá ser lo suficientemente independiente del área que se está auditando para permitir completar de manera objetiva la auditoría.

030 Ética y normas profesionales

030.010 Código de Ética Profesional

El auditor de sistemas de información deberá acatar el Código de Ética Profesional de la Asociación de Auditoría y Control de Sistemas de Información.

030.020 Atención profesional correspondiente

En todos los aspectos del trabajo del auditor de sistemas de información, se deberá ejercer la atención profesional correspondiente y el cumplimiento de las normas aplicables de auditoría profesional.

040 Idoneidad

040.010 Habilidades y conocimientos

El auditor de sistemas de información debe ser técnicamente idóneo, y tener las habilidades y los conocimientos necesarios para realizar el trabajo como auditor.

040.020 Educación profesional continúa.

El auditor de sistemas de información deberá mantener la idoneidad técnica por medio de la educación profesional continua correspondiente.

050 Planificación

050.010 Planificación de la auditoría

El auditor de sistemas de información deberá planificar el trabajo de auditoría de los sistemas de información para satisfacer los objetivos de la auditoría y para cumplir con las normas aplicables de auditoría profesional.

060 Ejecución del trabajo de auditoría

060.010 Supervisión

El personal de auditoría de los sistemas de información debe recibir la supervisión apropiada para proporcionar la garantía de que se cumpla con los objetivos de la auditoría y que se satisfagan las normas aplicables de auditoría profesional.

060.020 Evidencia

Durante el transcurso de una auditoría, el auditor de sistemas de información deberá obtener evidencia suficiente, confiable, relevante y útil para lograr de manera eficaz los objetivos de la auditoría. Los hallazgos y conclusiones de la auditoría se deberán apoyar por medio de un análisis e interpretación apropiados de dicha evidencia.

070 Informes

070.010 Contenido y formato de los informes

En el momento de completar el trabajo de auditoría, el auditor de sistemas de información deberá proporcionar un informe, de formato apropiado, a los destinatarios en cuestión. El informe de auditoría deberá enunciar el alcance, los objetivos, el período de cobertura y la naturaleza y amplitud del trabajo de auditoría realizado. El informe deberá identificar la organización, los destinatarios en cuestión y cualquier restricción con respecto a su circulación.

El informe deberá enunciar los hallazgos, las conclusiones y las recomendaciones, y cualquier reserva o consideración que tuviera el auditor con respecto a la auditoría.

080 Actividades de seguimiento

080.010 Seguimiento

El auditor de sistemas de información deberá solicitar y evaluar la información apropiada con respecto a hallazgos, conclusiones y recomendaciones relevantes anteriores para determinar si se han implementado las acciones apropiadas de manera oportuna.

1.3.4.3 NORMAS DE AUDITORIA DE SISTEMAS DE INFORMACIÓN

INTRODUCCIÓN

La Asociación de Auditoría y Control de Sistemas de Información (ISACA) determinó que por la naturaleza especializada de la auditoría de los sistemas de información y las habilidades necesarias para llevar a cabo este tipo de auditoría, requieren el desarrollo y la promulgación de directrices y lineamientos que ayuden al cumplimiento de las Normas de Auditoria de Sistemas de Información.

OBJETIVO

El objetivo de estas normas es proporcionar asesoramiento en la aplicación e implementación de los estándares establecidos y su cumplimiento como profesionales de Auditoria de Sistemas de Información. Estas normas son detalladas a continuación

1. **Estatuto de Auditoria No S1.**
   El propósito de este Estándar de Auditoria de SI, es establecer y proporcionar asesoramiento con respecto al Estatuto de Auditoria o la Carta Compromiso utilizado durante el proceso de Auditoria.

2. **Independencia No S2.**
   El propósito de esta Norma de Auditoria de SI es establecer estándares guías relacionadas con la Independencia durante el proceso de Auditoria.

3. **Éticas y Normas Profesionales No S3.**
   El propósito de esta Norma de Auditoria de SI es establecer un estándar y proporcionar una guía para el Auditor de SI con el fin de que cumpla con el Código de Ética Profesional de ISACA y ejerza el debido cuidado profesional al realizar tareas de Auditoria.

4. **Competencia Profesional No S4.**
   El propósito de esta Norma de Auditoria de SI es establecer y brindar asesoría a fin de que el auditor de SI logre y mantenga un nivel de competencia profesional.

5. **Planeación No S5.**
   El propósito de esta Norma de Auditoria de SI es establecer normas y brindar asesoría sobre la Planeación de una Auditoria.

6. Ejecución de la Auditoria No S6.

El propósito de este Estándar de Auditoria de SI es establecer normas y proporcionar asesoría con respecto a la realización de las labores de Auditoria.

7. Reporte No S7.

El propósito de esta Norma de Auditoria de SI es establecer y proporcionar asesoría sobre la generación del informe a fin de que el auditor de SI pueda cumplir con esta responsabilidad.

8. Actividades de Seguimiento No S8.

El propósito de esta Norma de Auditoria de SI es establecer normas y proporcionar asesoría con respecto a las actividades de seguimiento realizadas durante un proceso de Auditoria de SI.

9. Irregularidades y Acciones Ilegales No S9.

El propósito de este estándar de ISACA es establecer y proporcionar asesoría sobre irregularidades y acciones ilegales que el auditor de SI debe tener en cuenta durante el proceso de Auditoria.

10. Gobernabilidad de TI No S10.

El propósito de este estándar de ISACA es establecer y proporcionar asesoría en las áreas de gobernabilidad de TI que el Auditor de SI debe tener en cuenta durante el proceso de auditoría.

11. Uso de la evaluación de riesgos en la planeación de Auditoria No S11.

El propósito de este estándar es establecer normas y proporcionar asesoría con respecto al uso de la evaluación de riesgos en la planeación de auditoría.

12. Materialidad de Auditoria No S12.

El propósito de este Estándar de Auditoría de SI es establecer y proporcionar una guía con respecto al concepto de materialidad de la auditoría y su relación con el riesgo de auditoría.

13. Uso del Trabajo de Otros Expertos No S13.

El propósito de este Estándar de Auditoría de SI es establecer y proporcionar asesoramiento al auditor de SI que utilice el trabajo de otros expertos durante una auditoría.

14. Evidencia de Auditoria No S14.

El propósito de este estándar es establecer Estándares y proporcionar una guía sobre lo que constituye evidencia de auditoría, y calidad y cantidad de evidencia de auditoría que deberá obtener el auditor de SI.

1.3.4.4 CODIGO DE ETICA PROFESIONAL DE ASOCIACION DE AUDITORÍA Y CONTROL DE SISTEMAS DE INFORMACION (ISACA)

La Asociación de Auditoría y Control de Sistemas, creó este Código de Ética para guiar la conducta profesional y personal de los miembros de la Asociación y/o los poseedores de la designación CISA (Certificación para Auditores de Sistemas de Información).

Los Auditores de Sistemas Certificados deberán:

- Apoyar el establecimiento y cumplimiento apropiado de procedimientos estándares y controles en los sistemas de información.
- Cumplir con los Estándares de Auditoría de Sistemas de Información adoptados por la Asociación de Auditoría y Control de Sistemas de Información.

- Dar servicio a sus empleadores, accionistas, clientes y público en general en forma diligente, leal y honesta y no formar parte de actividades impropias o ilegales.
- Mantener la confidencialidad de la información obtenida en el curso de sus tareas. Dicha información no debe ser usada en beneficio propio ni ser entregada a terceros.
- Realizar sus tareas en forma objetiva e independiente, y rechazar la realización de actividades que amenacen o parezcan amenazar su independencia.
- Mantener competencia en los campos relacionados a la auditoría de sistemas de información a través de la participación en actividades de desarrollo profesional.
- Obtener suficiente material y documentación de sus observaciones que le permita respaldar sus recomendaciones y conclusiones.
- Informar a las partes que correspondieren los resultados del trabajo de auditoría realizado.
- Dar apoyo a la educación y el conocimiento de clientes, gerentes y público en general sobre la auditoría de sistemas de información.
- Mantener altos estándares de conducta y personalidad tanto en las actividades profesionales como personales.

1.4 OBJETIVOS DE CONTROL PARA LA INFORMACION Y TECNOLOGIAS AFINES (COBIT).

1.4.1 ANTECEDENTES

Information Systems Audit and Control Association ISACA (Asociación de Auditoría y Control de Sistemas de Información) comenzó en 1967, cuando un pequeño grupo de personas con trabajos similares y controles de auditoría en los sistemas computarizados que se estaban haciendo cada vez más críticos para las operaciones de sus organizaciones respectivas se sentaron a discutir la

necesidad de tener una fuente centralizada de información y guía en dicho campo. En 1969, el grupo se formalizó, incorporándose bajo el nombre de *EDP Auditors Association* (Asociación de Auditores de Procesamiento Electrónico de Datos). En 1976 la asociación formó una fundación de educación para llevar a cabo proyectos de investigación de gran escala para expandir los conocimientos y el valor del campo de gobernación y control de TI.

Hoy, los miembros de ISACA más de 65.000 en todo el mundo se caracterizan por su diversidad. Los miembros viven y trabajan en más de 140 países y cubren una variedad de puestos profesionales relacionados con TI sólo para nombrar algunos ejemplos, auditor de SI, consultor, educador, profesional de seguridad de SI, regulador, director ejecutivo de información y auditor interno. Algunos son nuevos en el campo, otros están en niveles medios de supervisión y algunos otros están en los rangos más elevados. Trabajan en casi todas las categorías de industrias, incluyendo finanzas y banca, contaduría pública, gobierno y sector público, servicios públicos y manufactura. Esta diversidad permite que los miembros aprendan unos de otros, e intercambien puntos de vista con divergencias significativas en una variedad de tópicos profesionales. Ha sido considerada durante largo tiempo como uno de los puntos fuertes de ISACA.

En las tres décadas transcurridas desde su creación, ISACA se ha convertido en una organización global que establece las pautas para los profesionales de gobernación, control, seguridad y auditoría de información. Sus normas de auditoría y control de SI son respetados por profesionales de todo el mundo. Sus investigaciones resaltan temas profesionales que desafían a sus constituyentes. Su certificación *Certified Information Systems Auditor* (Auditor Certificado de Sistemas de Información, o CISA) es reconocida en forma global y ha sido obtenida por más de 50.000 profesionales. Su nueva certificación *Certified Information Security Manager* (Gerente Certificado de Seguridad de Información,

o CISM) se concentra exclusivamente en el sector de gerencia de seguridad de la información.

ISACA propone la metodología COBIT, la cual es una herramienta realizada en el año de 1996 y revisado posteriormente, dirigido a auditores, administradores y usuarios de sistemas de información, que tiene como objetivos de control la efectividad y eficiencia de las operaciones; confidencialidad e integridad de la información financiera y el cumplimiento de las leyes y regulaciones.

COBIT ha sido desarrollado como un estándar generalmente aplicable y aceptado para la práctica del control de Tecnología Informática. COBIT está basado en los Objetivos de Control existentes de la Information Systems Audit and Control Foundation (ISACF) mejorados con los estándares internacionales existentes y emergentes técnicos, profesionales, regulatorios y específicos de la industria. Los Objetivos de Control resultantes, aplicables y aceptados en forma generalizada, han sido desarrollados para ser aplicados a los sistemas de información de toda la empresa.

1.4.2 DEFINICION

COBIT, es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los participantes. Este instrumento también permite el desarrollo de políticas claras y buenas prácticas para control de tecnologías de información a través de las empresas. COBIT constantemente se actualiza y armoniza con otros estándares. Por lo tanto, COBIT se ha convertido en el integrador de las mejores prácticas de TI y marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. La estructura de procesos de COBIT y su enfoque de alto nivel

orientado al negocio brinda una visión completa de TI y de las decisiones a tomar acerca de TI.

1.4.3 UTILIDAD

COBIT brinda buenas practicas a través de un marco de trabajo de dominios y procesos, y presentan las actividades en una estructura manejable y lógica las buenas practicas de COBIT representa el consenso de los expertos. Estas enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudaran a optimizar las inversiones facilitadas por las TI, aseguraran la entrega del servicio y brindara una medida contra la cual juzgar cuando las cosas no vayan bien.
COBIT, se enfoca en que se requiere para lograr una administración y control adecuado de TI, y se posiciona en un alto nivel. COBIT ha sido alineado y armonizado con otros estándares y mejores prácticas mas detallados de TI. COBIT actúa como integrador de todos los materiales guías, resumiendo los objetivos claves bajo un mismo marco de trabajo integral que también se vincula con los requerimientos de gobierno y de negocio.

1.4.4 BENEFICIOS

Los beneficios al implementar COBIT como marco de referencia de gobierno sobre la TI, incluyen:

- Mejor alineación, con base en su enfoque de negocios
- Una visión, entendible para la gerencia de lo que hace TI
- Propiedad y responsabilidades claras, con base en su orientación a procesos.
- Aceptación general de terceros y reguladores
- Entendimiento compartido entre todos los participantes, con base en un lenguaje común.

- Cumplimiento de los requerimientos COSO para el ambiente de control de TI

1.4.5 ÁREAS FOCALES DEL GOBIERNO DE TI

La medición del desempeño es esencial para el gobierno de TI. COBIT le da soporte e incluye el establecimiento y el monitoreo de objetivos que se puedan medir, referentes a los proceso de TI requieren generar (resultados del proceso) y como lo generan (capacidad y desempeño del proceso). Muchos estudios han identificado que la falta de transparencia en los costos, valor y riesgos de TI, es uno de los más importantes impulsores para el gobierno de TI. Mientras las otras áreas consideradas contribuyen, la transparencia se logra de forma principal por medio de medición del desempeño.

Figura 1 Áreas focales del gobierno de TI

Definición de áreas focales

- **Alineación estratégica**
  Se enfoca en garantizar el vínculo entre los planes de negocio y de TI; en definir, mantener y validar la propuesta de valor de TI; y en alinear las operaciones de TI con las operaciones de la empresa.

- **Entrega de valor**

  Se refiere a ejecutar la propuesta de valor a todo lo largo del ciclo de entrega, asegurando que TI genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costos y en brindar el valor intrínseco de la TI.

- **Administración de riesgos**

  Requiere conciencia de los riesgos por parte de los altos ejecutivos de la empresa, un claro entendimiento del deseo de riesgo que tiene la empresa, comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos para la empresa, y la inclusión de las responsabilidades de administración de riesgos dentro de la organización.

- **Administración de recursos**

  Se trata de la inversión óptima, así como la administración adecuada de los recursos críticos de TI: aplicaciones, información, infraestructura y personas.

  Los temas claves se refieren a la optimización de conocimiento y de infraestructura.

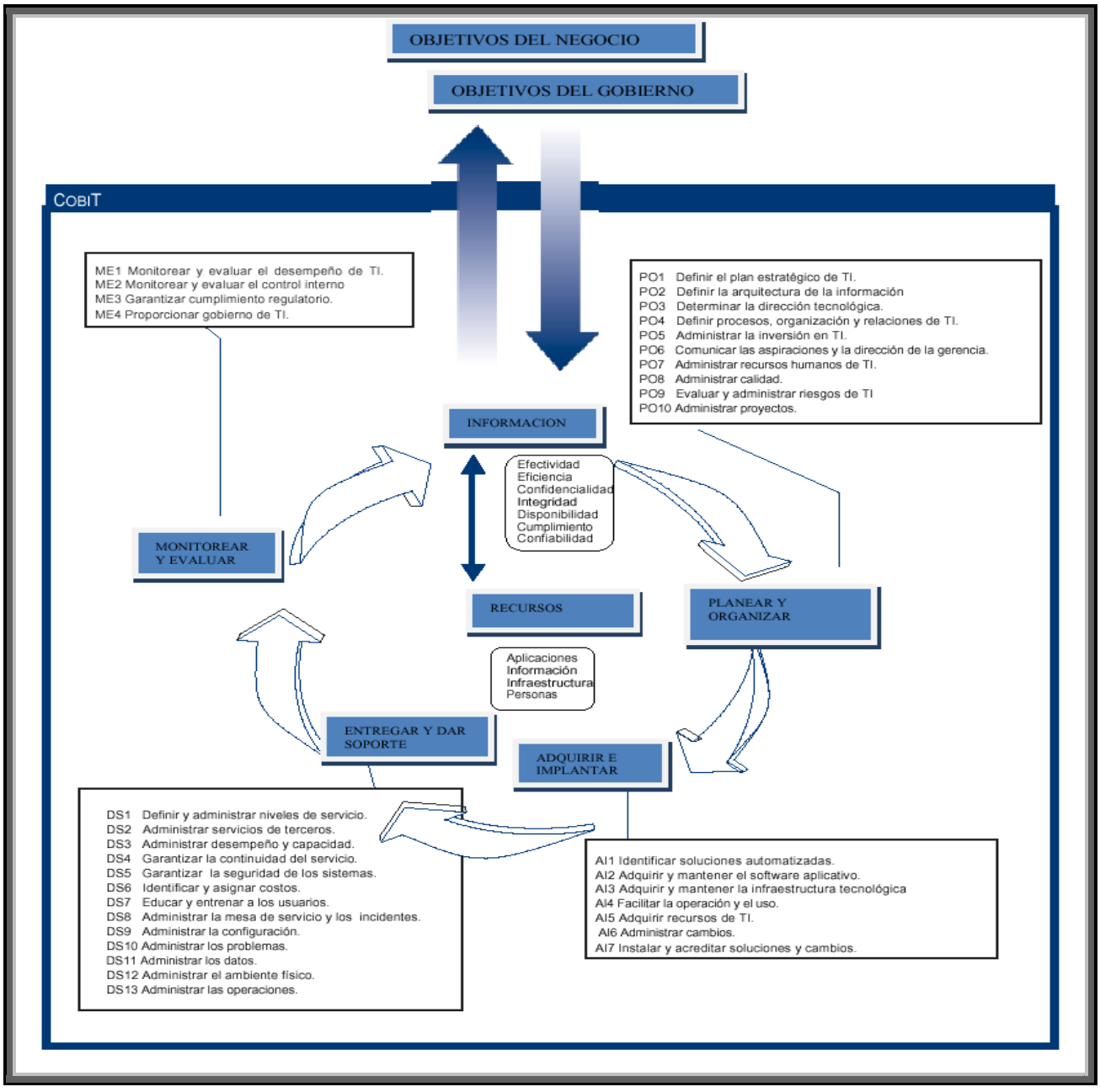
- **Medición del desempeño**

  Rastrea y monitorea la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio, con el uso, por ejemplo, de balanced scorecards que traducen la estrategia en acción para lograr las metas que se puedan medir más allá del registro convencional.

1.4.6 MARCO DE TRABAJO

El marco de trabajo de COBIT se creo con características principales de ser orientado a negocios, orientado a procesos, basados en controles e impulsado por mediciones.

Figura 2 Marco de Trabajo General de COBIT



1.4.8.1 ORIENTADO AL NEGOCIO

Este es el tema principal de COBIT, esta diseñado para ser utilizado no solo por proveedores de servicios, usuarios y auditores de TI, sino también y principalmente como guía integral para la gerencia y para los propietarios de los procesos de negocios.

Figura 3 Principio básico COBIT

El marco de trabajo COBIT ofrece herramientas para garantizar la alineación con los requerimientos del negocio a través de:

- **CRITERIOS DE INFORMACIÓN DE COBIT**

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. Con base en los requerimientos de calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

- **La efectividad:**
  Tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.
- **La eficiencia:**
  Consiste en que la información sea generada optimizando los recursos (más productivo y económico)
- **La confidencialidad**:
  Se refiere a la protección de información sensitiva contra revelación no autorizada.
- **La integridad:**
  Esta relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.
- **La disponibilidad:**
  Se refiere a que la información este disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne con la protección de los recursos y las capacidades necesarias asociadas.
- **El cumplimiento:**
  Tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales esta sujeto el proceso de negocio, es decir, criterios de negocios impuestos externamente, así como políticas internas.
- **La confiabilidad:**
  Significa proporcionar la información apropiada para que la gerencia administre la entidad y ejercite sus responsabilidades fiduciarias y de gobierno.

Gráficamente los criterios de TI se presentan en cada dominio de la siguiente forma, y su nivel de aplicabilidad cuando es Primario se denota mediante una “P”, y cuando su aplicabilidad es secundaria se denota mediante una “S”, así:

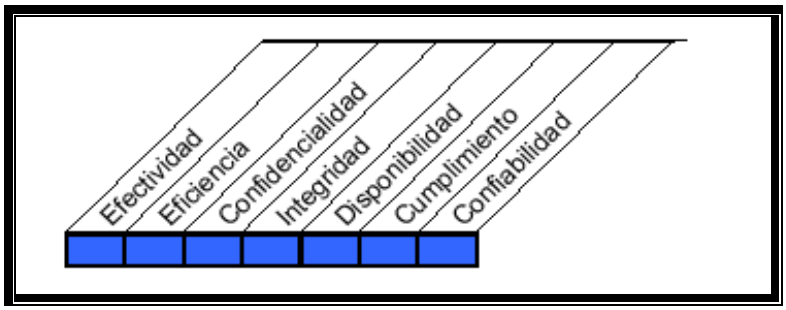


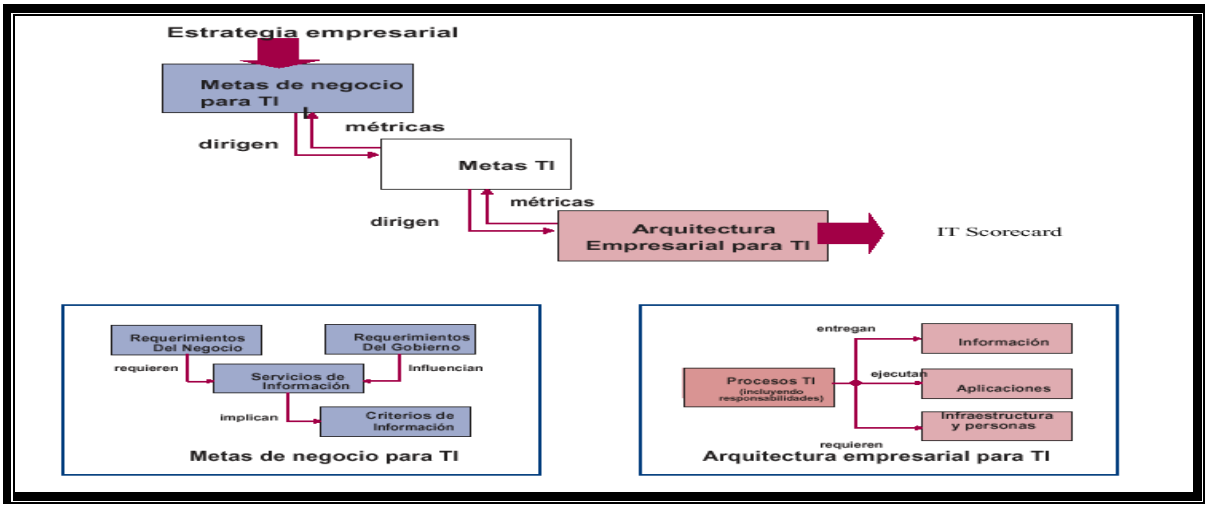
Figura 4 Criterios de TI

- **METAS DE NEGOCIO Y DE TI**

Mientras que los criterios de información proporcionan un método genérico para definir los requerimientos del negocio, la definición de un conjunto de metas genéricas de negocio y de TI ofrece una base mas refinada y relacionada con el negocio para el establecimiento de requerimientos de negocio y para el desarrollo de métricas que permitan la medición con respecto a estas metas.

La figura 5 proporciona una matriz de metas genéricas de negocios y metas de TI y como se asocian con los criterios de la información. Estos ejemplos genéricos se pueden utilizar como guía para determinar los requerimientos, metas y métricas específicas del negocio para la empresa.

Figura 5 Definición de metas de TI y Arquitectura Empresarial



- **RECURSOS DE TI**

Los recursos de TI identificados en COBIT se pueden definir como sigue:

- Aplicaciones

  Incluyen tanto sistemas de usuarios automatizados como procedimientos manuales que procesan información.

- Información

  Son los datos en todas sus formas de entrada, procesados y generados por los sistemas de información, en cualquier forma en que son utilizados por el negocio.

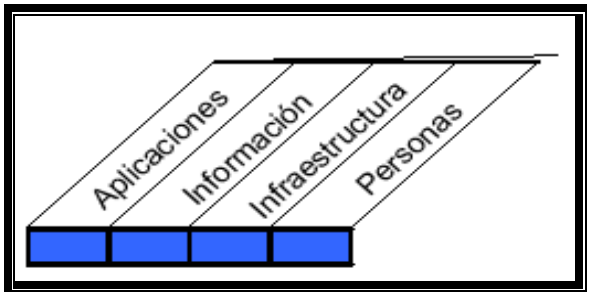
- Infraestructura

  Es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.

- Personas

  Son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas los servicios de información.

Gráficamente los recursos de TI, se representan de la forma siguiente y su aplicabilidad se denota marcando el espacio en blanco de la parte inferior una “X” así:



1.4.6.2 PROCESOS ORIENTADOS

COBIT define las actividades de TI en un modelo genérico de procesos en cuatro dominios, estos dominios son planear y organizar, adquirir e implementar, entregar y dar soporte y monitorear y evaluar. Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear.
Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Estos se pueden resumir como sigue:

- **PLANEAR Y ORGANIZAR**

  Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio. Además la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente se debe implementar una estructura organizacional y una estructura tecnológica apropiada.

Los objetivos de alto nivel que lo comprenden son los siguientes:

PO1	Definir el plan estratégico de TI
PO2	Definir la arquitectura de la información
PO3	Determinar la dirección tecnológica
PO4	Definir procesos, organización y relaciones de TI
PO5	Administrar la inversión en TI
PO6	Comunicar las aspiraciones y la dirección de la gerencia.
PO7	Administrar recursos humanos de TI
PO8	Administrar calidad
PO9	Evaluar y administrar riesgos de TI
PO10	Administrar proyectos

- **ADQUIRIR E IMPLEMENTAR**

  Para llevar a cabo las estrategias de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como la implementación e integración en los procesos de los negocios. Además el cambio y el mantenimiento de los sistemas existentes esta cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio.

Los objetivos de alto nivel que lo comprenden son los siguientes:

AI1	Identificar soluciones automatizadas
AI2	Adquirir y mantener el software aplicativo
AI3	Adquirir y mantener la infraestructura tecnológica
AI4	Facilitar la operación y el uso
AI5	Adquirir recursos de TI
AI6	Administrar cambios
AI7	Instalar y acreditar soluciones y cambios

- **ENTREGAR Y DAR SOPORTE**

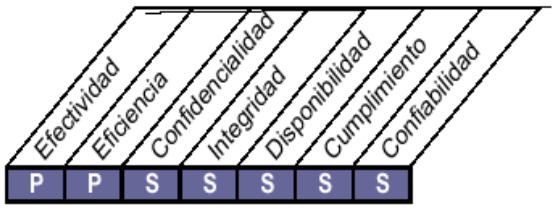
  Este dominio cubre la entrega en si de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales.

El dominio de Entrega de Servicios y soporte comprende trece objetivos de alto nivel los cuales se detallan a continuación:

DS1 Definir y Administrar los niveles de servicio.

Contar con una definición documentada y un acuerdo de servicios de TI y de niveles de servicio, hace posible una comunicación efectiva entre la gerencia de TI y los clientes de negocio respecto de los servicios requeridos, también incluye el monitoreo y la notificación oportuna a los participantes sobre el cumplimiento de los niveles de servicio y permite la alineación entre los servicios de TI y los requerimientos de negocio relacionados.

Criterio de TI aplicables:



Este proceso satisface el requisito de negocio de TI de asegurar la alineación de los servicios claves de TI con la estrategia del negocio, enfocándose en la identificación de requerimientos de servicio, el acuerdo de niveles de servicio y el monitoreo del cumplimiento de los niveles de servicio.

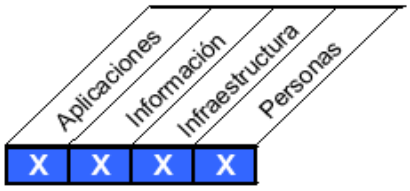
Lograr este objetivo de control solo es posible mediante:

- La formalización de acuerdos internos y externos en línea con los requerimientos y las capacidades de entrega
- La notificación del cumplimiento de los niveles de servicio (reportes y reuniones)
- La identificación y comunicación de requerimientos de servicios actualizados y nuevos para planeación estratégica.

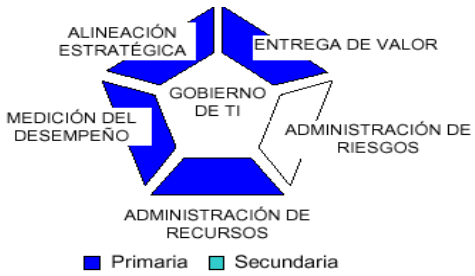
Es posible su medición a través de:

- El porcentaje de participantes satisfechos de que la entrega del servicio cumple con los niveles previamente acordados.
- El número de servicios entregados que no están en el catálogo.
- El número de reuniones formales de revisión del Acuerdo de niveles de Servicio (SLA) con las personas de negocio por año.

Recursos de TI aplicables:



Áreas focales aplicables:



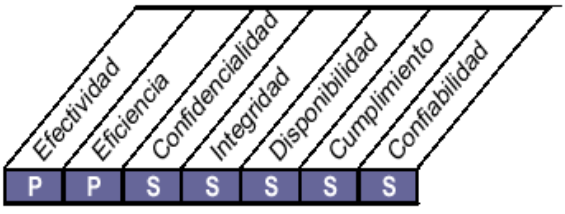
OBJETIVOS DE CONTROL DETALLADOS

DS1.1 Marco de trabajo de la administración de los niveles de servicio.
DS1.2 Definición de servicios.
DS1.3 Acuerdos de niveles de servicio.
DS1.4 Acuerdos de niveles de operación.
DS1.5 Monitoreo y reporte del cumplimento de los niveles de
DS1.6 Revisión de los acuerdos de niveles de servicio y de los contratos.

DS2 Administrar los Servicios de terceros.

La necesidad de asegurar que los servicios provistos por terceros cumplan con los requerimientos del negocio, requiere de un proceso efectivo de administración de terceros. Este proceso se logra por medio de una clara definición de roles, responsabilidades y expectativas en los acuerdos con los terceros, así como con la revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos. Una efectiva administración de los servicios de terceros minimiza los riesgos del negocio asociados con proveedores que no se desempeñan de forma adecuada.

Criterio de TI aplicables:



Este proceso satisface el requisito de negocio de TI para brindar servicios satisfactorios de terceros con transparencia acerca de los beneficios, riesgos y costos enfocándose en el establecimiento de relaciones y responsabilidades bilaterales con proveedores

calificados de servicios tercerizados y el monitoreo de la prestación del servicio para verificar y asegurar la adherencia a los convenios.

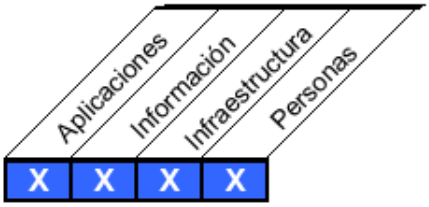
Se logra con:

- La identificación y categorización de los servicios del proveedor.
- La identificación y mitigación de riesgos del proveedor
- El monitoreo y la medición del desempeño del proveedor.

Es posible su medición a través de:

- El número de quejas de los usuarios debidas a los servicios contratados.
- El porcentaje de los principales proveedores que cumplen claramente los requerimientos definidos y los niveles de servicio.
- El porcentaje de los principales proveedores sujetos a monitoreo.

Recursos de TI aplicables:



Áreas focales aplicables:

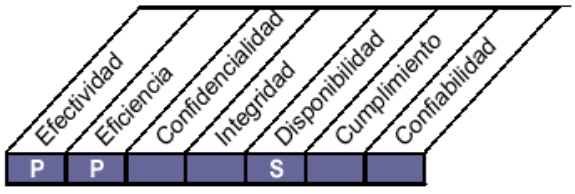
OBJETIVOS DE CONTROL DETALLADOS

DS2.1 Identificación de las relaciones con todos los proveedores
DS2.2 Administración de las relaciones con los proveedores
DS2.3 Administración de riesgos del proveedor
DS2.4 Monitoreo del desempeño del proveedor

DS3 Administrar el desempeño y la capacidad

La necesidad de administrar el desempeño y la capacidad de los recursos de TI requiere de un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI. Este proceso incluye el pronóstico de las necesidades futuras, basadas en los requerimientos de carga de trabajo, almacenamiento y contingencias. Este proceso brinda la seguridad de que los recursos de información que soportan los requerimientos del negocio están disponibles de manera continua.

Criterio de TI aplicables:



Este proceso satisface el requisito de negocio de TI para Optimizar el desempeño de la infraestructura, los recursos y las capacidades de TI en respuesta a las necesidades del negocio.

Se enfoca en cumplir con los requerimientos de tiempo de respuesta de los acuerdos de niveles de servicio, minimizando el tiempo sin servicio y haciendo mejoras continuas de desempeño y capacidad de TI a través del monitoreo y la medición.

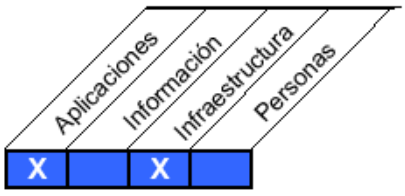
Se logra con:

- La planeación y la entrega de capacidad y disponibilidad del sistema
- Monitoreando y reportando el desempeño del sistema
- Modelando y pronosticando el desempeño del sistema.

Es posible su medición a través de:

- Número de horas perdidas por usuario por mes, debidas a la falta de planeación de la capacidad.
- Porcentaje de picos donde se excede la meta de utilización.
- Porcentaje de SLAs de tiempo de respuesta que no se satisfacen.

Recursos de TI aplicables:



Áreas focales aplicables:

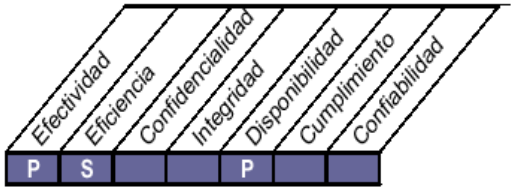
OBJETIVOS DE CONTROL DETALLADOS

DS3.1 Planeación del desempeño y la capacidad
DS3.2 Capacidad y desempeño actual
DS3.3 Capacidad y desempeño futuros
DS3.4 Disponibilidad de recursos de TI
DS3.5 Monitoreo y reporte

DS4 Garantizar la continuidad del servicio

La necesidad de brindar continuidad en los servicios de TI requiere desarrollar, mantener y probar planes de continuidad de TI, almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad. Un proceso efectivo de continuidad de servicios, minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio.

Criterio de TI aplicables:



Este proceso satisface el requisito de negocio de TI para asegurar el mínimo impacto al negocio en caso de una interrupción de servicios de TI.

Se enfoca en el desarrollo de resistencia en las soluciones automatizadas y desarrollando, manteniendo y probando los planes de continuidad de TI.

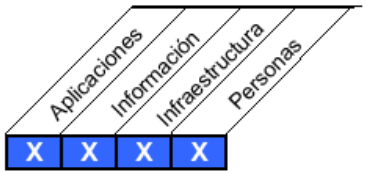
Se logra a través de:

- Desarrollando y manteniendo (mejorando) los planes de contingencia de TI.
- Con entrenamiento y pruebas de los planes de contingencia de TI.
- Guardando copias de los planes de contingencia y de los datos fuera de las instalaciones.

Es posible medirlo a través de:

- Número de horas perdidas por usuario por mes, debidas a interrupciones no planeadas.
- Número de procesos críticos de negocio que dependen de TI, que no están cubiertos por un plan de continuidad.

Recursos de TI aplicables:



Áreas focales aplicables:

OBJETIVOS DETALLADOS

DS4.1 IT Marco de trabajo de continuidad

DS4.2 Planes de continuidad de TI

DS4.3 Recursos críticos de TI

DS4.4 Mantenimiento del plan de continuidad de TI

DS4.5 Pruebas del plan de continuidad de TI

DS4.6 Entrenamiento del plan de continuidad de TI

DS4.7 Distribución del plan de continuidad de TI

DS4.8 Recuperación y reanudación de los servicios de TI

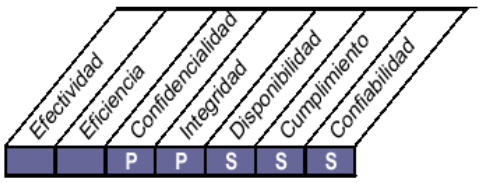
DS4.9 Almacenamiento de respaldos fuera de las instalaciones

DS4.10 Revisión post-reanudación

DS5 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS.

La necesidad de mantener la integridad de los sistemas de información y proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreos de seguridad y pruebas periódicas así como realizar acciones correctivas sobre debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad.

Criterio de TI aplicables:



Este objetivo de control se enfoca en la definición de políticas, procedimientos y estándares de seguridad de TI y en el monitoreo, detección, reporte y resolución de la vulnerabilidad o incidentes de seguridad.

Para lograrlo se debe de definir los siguientes puntos:

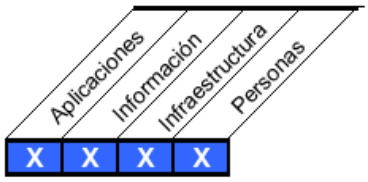
- El entendimiento de los requerimientos, vulnerabilidades y amenazas de seguridad.

- La administración entidades y autorizaciones de los usuarios de forma estandarizada.
- Probando la seguridad de forma regular.

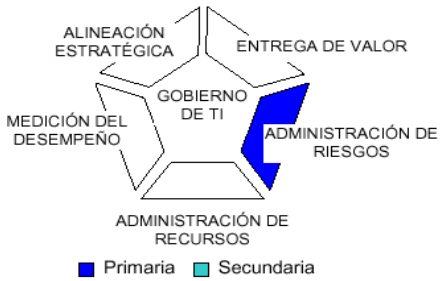
Y es medible a través de lo siguiente:

- El numero de incidentes que dañan con a reputación del público.
- El numero de sistemas donde no se cumplen los requerimientos de seguridad.
- El numero de violaciones de en la segregación de tareas.

Recursos de TI aplicables:



Áreas focales aplicables:



Para este objetivo de control de ato nivel también existen objetivos de control detallados y se mencionaran a continuación:

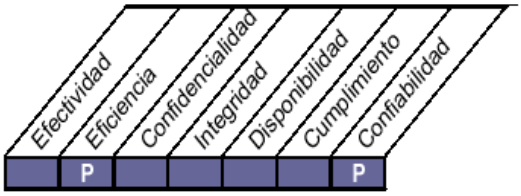
DS5.1 Administración de la seguridad de TI.
DS5.2 Plan de seguridad de TI.
DS5.3 Administración de identidad.
DS5.4 Administración de cuentas del usuario.
DS5.5 Pruebas, vigilancia y monitoreo de la seguridad
DS5.6 Definición de incidentes de seguridad.
DS5.7 Protección de la tecnología de seguridad
DS5.8 Administración de llaves criptográficas

DS5.9 Prevención, detección y corrección de software malicioso
DS5.10 Seguridad de la red
DS5.11 Intercambio de datos sensitivos

DS6 IDENTIFICAR Y ASIGNAR COSTOS

La necesidad de un sistema justo y equitativo para asignar costos de TI al negocio, requiere de una medición precisa y un acuerdo con los usuarios del negocio sobre una asignación justa. Este proceso incluye la construcción y operación y un sistema para capturar, distribuir y reportar costos de TI a los usuarios de los servicios. Un sistema equitativo de costos permite al negocio tomar decisiones mas informadas respecto a los usos de los servicios de TI.

Criterio de TI aplicables:



Este objetivo de control se enfoca en el registro completo y preciso de los costos de TI, un sistema equitativo para asignación acordado con los usuarios del negocio, y un sistema para reportar oportunamente el uso de TI y los costos asignados.

Para lograrlo se debe de definir los siguientes puntos:

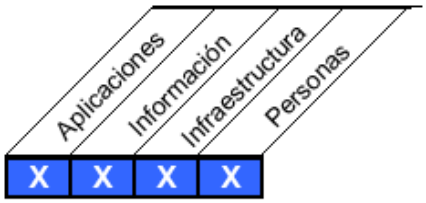
- La alineación de cargos con la calidad y cantidad de los servicios brindados.
- La construcción y aceptación de un modelo de costos completo.
- La aplicación de cargos con base en la política acordada.

Y es medible a través de lo siguiente:

- Porcentaje de facturas de servicio de TI aceptadas/pagadas por la gerencia del negocio.
- Porcentaje de variación entre los presupuestos, pronósticos y costos actuales.

- Porcentaje de costos totales de TI que son distribuidos de acuerdo con los modelos acordados

Recursos de TI aplicables:



Áreas focales aplicables:

Para este objetivo de control de ato nivel también existen objetivos de control detallados y se mencionaran a continuación:

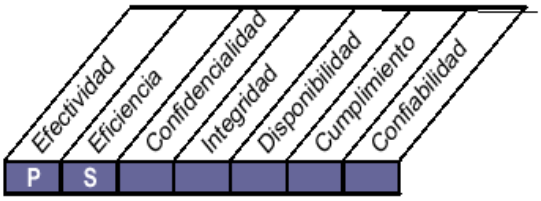
DS6.1 Definición de servicios
DS6.2 Contabilización de TI
DS6.3 Modelación de costos y cargos
DS6.4 Mantenimiento del modelo de costos

DS7 EDUCAR Y ENTRENAR A LOS USUARIOS

Para una adecuación efectiva de los usuarios de sistemas de TI, incluyendo aquellos dentro de TI, se requieren identificar las necesidades de entrenamiento de cada grupo de usuarios. Además de identificar las necesidades, este proceso incluye la definición y ejecución de una estrategia para llevar a cabo un entrenamiento efectivo y para medir los resultados. Un programa efectivo de entrenamiento incrementa el uso efectivo de la tecnología al

disminuir los errores, incrementando la productividad y el cumplimiento de los controles clave tales como las medidas de seguridad de los usuarios.

Criterio de TI aplicables:



Este objetivo de control se enfoca en un claro entendimiento de las necesidades de entrenamiento de los usuarios de TI, la ejecución de una efectiva estrategia de entrenamiento y la medición de resultados.

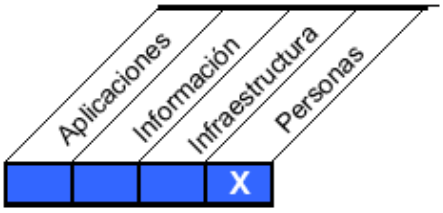
Para lograrlo se debe de definir los siguientes puntos:

- Establecer un programa de entrenamiento
- Organizar el entrenamiento
- Impartir el entrenamiento
- Monitorear y reportar la efectividad del entrenamiento

Y es medible a través de lo siguiente:

- Número de llamadas de soporte debido a problemas de entrenamiento
- Porcentaje de satisfacción de los participantes con el entrenamiento recibido
- Lapso de tiempo entre la identificación de la necesidad de entrenamiento y la impartición del mismo.

Recursos de TI aplicables:



Áreas focales aplicables:

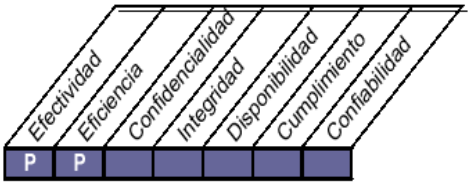
Para este objetivo de control de ato nivel también existen objetivos de control detallados y se mencionaran a continuación:

DS7.1 Identificar las necesidades de entrenamiento y educación
DS7.2 Impartición de entrenamiento y educación
DS7.3 Evaluación del entrenamiento recibido

DS8 ADMINISTRAR LA MESA DE SERVICIO Y LOS INCIDENTES

Responder de manera oportuna y efectiva a las consultas y problemas de los usuarios de TI, requiere de una mesa de servicio bien diseñada y bien ejecutada, y de administración de incidentes. Este proceso incluye la creación de una función de mesa de servicio con registro, escalamiento de incidentes, análisis de tendencia, análisis causa-raíz y resolución. Los beneficios del negocio incluyen el incremento en la productividad gracias a la resolución rápida de consultas. Además, el negocio puede identificar la causa-raíz (tales como pobre entrenamiento a los usuarios) a través de un proceso de reporte efectivo.

Criterio de TI aplicables:



Este objetivo de control se enfoca en una función profesional de mesa de servicio, con tiempo de respuesta rápida, procedimientos de escalamiento claros y análisis de tendencias y de resolución.

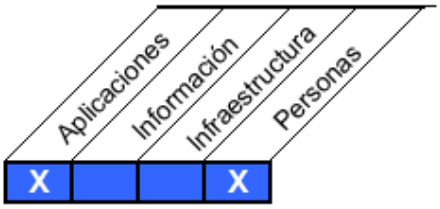
Para lograrlo se debe de definir los siguientes puntos:

- Instalación y operación de un servicio de una mesa de servicio
- Monitoreo y reporte de tendencias
- Definición de procedimientos y de criterios de escalamiento claros

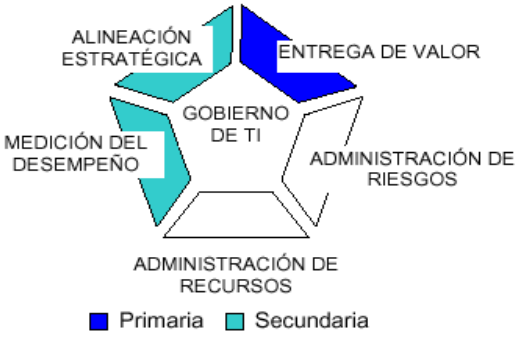
Y es medible a través de lo siguiente:

- Satisfacción del usuario con el soporte de primera línea
- Porcentaje de incidentes resueltos dentro de un lapso de tiempo aceptable acordado.
- Índice de abandono de llamadas

Recursos de TI aplicables:



Áreas focales aplicables:



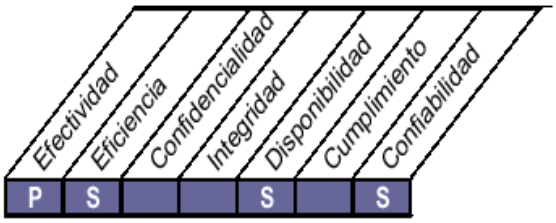
Para este objetivo de control de ato nivel también existen objetivos de control detallados y se mencionaran a continuación:

DS8.1 Mesa de servicios
DS8.2 Registro de consulta de clientes
DS8.3 Escalamiento de incidentes
DS8.4 Cierre de incidentes
DS8.5 Análisis de tendencias

DS9 ADMINISTRAR LA CONFIGURACION

Garantizar la integridad de las configuraciones de hardware y software requiere establecer y mantener un repositorio de configuraciones completo y preciso. Este proceso incluye la recolección de información de la configuración inicial, el establecimiento de normas, la verificación y auditoría de la información de la configuración y la actualización del repositorio de configuración conforme se necesite. Una efectiva administración de la configuración facilita una mayor disponibilidad, minimiza los problemas de producción y resuelve los problemas más rápido.

Criterio de TI aplicables:



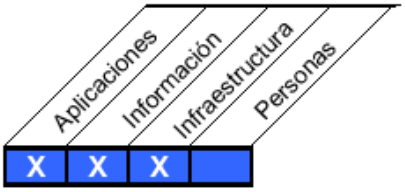
El proceso de administrar la configuración satisface el requisito de negocio de TI para optimizar la infraestructura, recursos y capacidades de TI, y llevar registro de los activos de TI.
Este proceso se enfoca en establecer y mantener un repositorio completo y preciso de atributos de la configuración de los activos y de las líneas base y compararlos contra la configuración actual.
Lograr este objetivo de control solo es posible mediante:

- El establecimiento de un repositorio central de todos los elementos de la configuración.
- La identificación de los elementos de configuración y su mantenimiento.
- La revisión de la integridad de los datos de configuración.

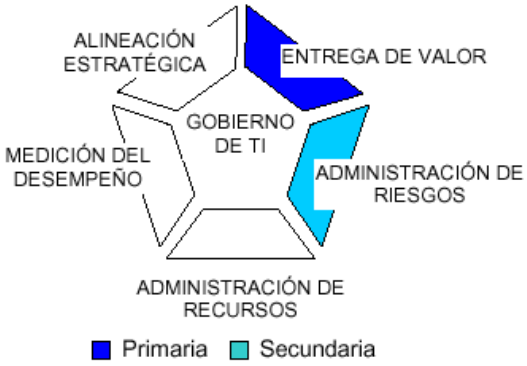
La medición del proceso administrar la configuración se hace por medio de:

- El número de problemas de cumplimiento del negocio debido a inadecuada configuración de los activos.
- El número de desviaciones identificadas entre el repositorio de configuración y la configuración actual de los activos.
- Porcentaje de licencias compradas y no registradas en el repositorio.

Recursos de TI aplicables:



Áreas focales aplicables:



Los objetivos de control detallados que se evalúan en este proceso son:

DS9.1 Repositorio de configuración y línea base

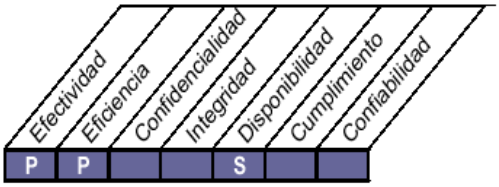
DS9.2 Identificación y mantenimiento de elementos de configuración

DS9.3 Revisión de integridad de la configuración

DS10 ADMINISTRACION DE PROBLEMAS

Una efectiva administración de problemas requiere la identificación y clasificación de problemas, el análisis de las causas desde su raíz, y la resolución de problemas. El proceso de administración de problemas también incluye la identificación de recomendaciones para la mejora, el mantenimiento de registros de problemas y la revisión del estatus de las acciones correctivas. Un efectivo proceso de administración de problemas mejora los niveles de servicio, reduce costos y mejora la conveniencia y satisfacción del usuario.

Criterio de TI aplicables:



El proceso de administración de problemas satisface el requisito de negocio de TI para garantizar la satisfacción de los usuarios finales con ofrecimientos de servicios y niveles de servicio, reducir el trabajo y los defectos en la prestación de los servicios y de las soluciones.

Este proceso se enfoca en registrar, rastrear y resolver problemas operativos; investigación de las causas raíz de todos los problemas relevantes y definir soluciones para los problemas operativos identificados.

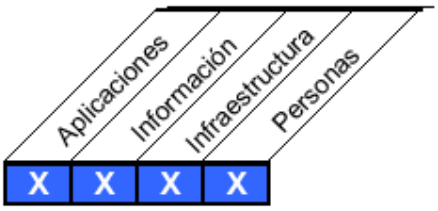
Lograr este objetivo de control solo es posible mediante:

- Realizando un análisis de causas de raíz de los problemas reportados
- Analizando las tendencias
- Tomando propiedad de los problemas y con una resolución de problemas progresiva.

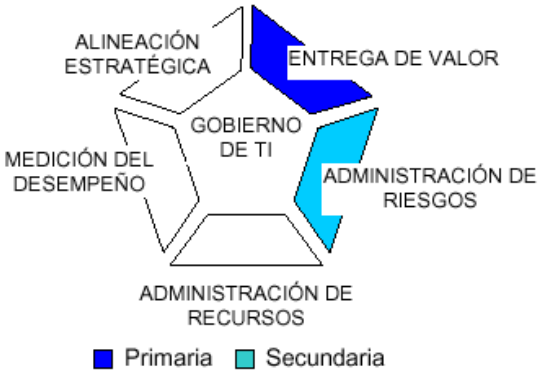
La medición del proceso administración de problemas se hace por medio de:Número de problemas recurrentes con impacto en el negocio

- Porcentaje de problemas resueltos dentro del periodo de tiempo solicitado
- Frecuencia de los reportes o actualizaciones sobre un problema en curso, con base en la severidad del problema.

Recursos de TI aplicables:



Áreas focales aplicables:



Los objetivos de control detallados que se evalúan en este proceso son:

DS10.1 Identificación y clasificación de problemas

DS10.2 Rastreo y resolución de problemas

DS10.3 Cierre de problemas

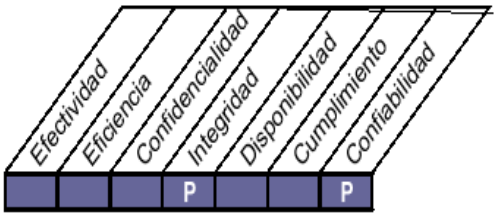
DS10.4 Integración de las administraciones de cambios, configuración y problemas

DS11 ADMINISTRACION DE DATOS

Una efectiva administración de datos requiere de la identificación de datos. El proceso de administración de información también incluye el establecimiento de procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios. Una efectiva administración de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de la información del negocio.

El proceso de administración de datos satisface el requerimiento de negocio de TI para optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera.

Criterio de TI aplicables:



Este proceso se enfoca en mantener la integridad, exactitud, disponibilidad y protección de los datos.

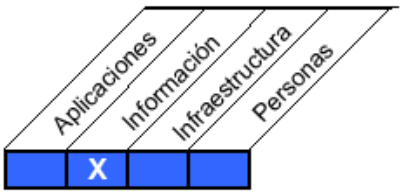
Lograr este objetivo de control solo es posible mediante:

- Respaldando los datos y probando la restauración
- Administrando almacenamiento de datos en sitio y fuera de sitio
- Desechando de manera segura los datos y el equipo.

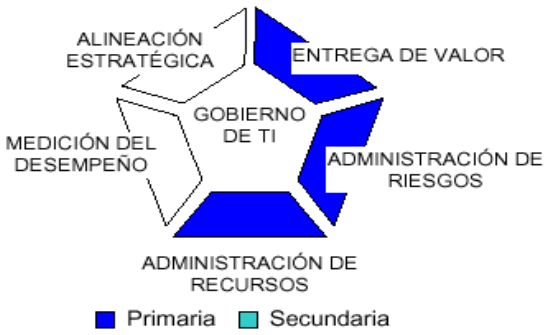
La medición del proceso administración de datos se hace por medio de:

- Satisfacción del usuario con la disponibilidad de los datos
- Porcentaje de restauraciones exitosas de datos
- Número de incidentes en los que tuvo que recuperarse datos sensitivos después que los medios habían sido desechados.

Recursos de TI aplicables:



Áreas focales aplicables:



Los objetivos de control detallados que se evalúan en este proceso son:

DS11.1 Requerimientos del negocio para administración de datos

DS11.2 Acuerdos de almacenamiento y conservación

DS11.3 Sistema de administración de librería de medios

DS11.4 Eliminación

DS11.5 Respaldo y restauración

DS11.6 Requerimientos de seguridad para la administración de datos

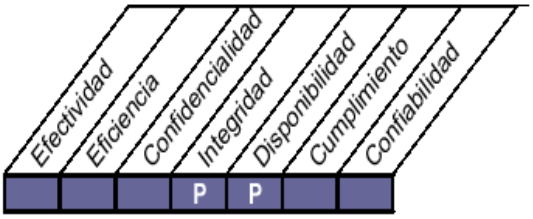
DS12 ADMINISTRACION DEL AMBIENTE FISICO

La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos (site), la selección de instalaciones apropiadas y el diseño de proceso efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal.

El proceso de administración del ambiente físico satisface el requisito de negocio de TI para proteger los activos de cómputo y

la información del negocio minimizando el riesgo de una interrupción del servicio.

Criterio de TI aplicables:



Este proceso se enfoca en proporcionar y mantener un ambiente físico adecuado para proteger los activos de TI contra acceso, daño o robo.

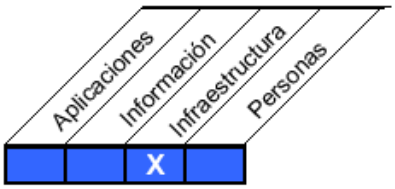
Lograr este objetivo de control solo es posible mediante:

- Implementando medidas de seguridad física
- Seleccionando y administrando las instalaciones

La medición del proceso administración del ambiente físico se hace por medio de:

- Tiempo sin servicio ocasionado por incidentes relacionados con el ambiente físico
- Número de incidentes ocasionados por fallas o brechas de seguridad física
- Frecuencia de revisión y evaluación de riesgos físicos

Recursos de TI aplicables:



Áreas focales aplicables:

Los objetivos de control detallados que se evalúan en este proceso son:

DS12.1 Selección y diseño del centro de datos

DS12.2 Medidas de seguridad física

DS12.3 Acceso físico

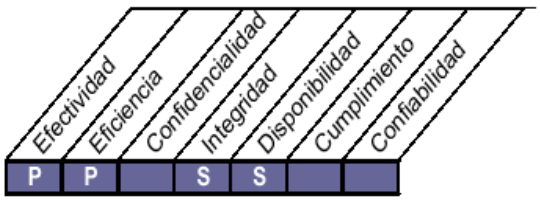
DS12.4 Protección contra factores ambientales

DS12.5 Administración de instalaciones físicas

DS13 ADMINISTRACIÓN DE OPERACIONES

Un procesamiento de información completo y apropiado requiere de una efectiva administración del procesamiento de datos y del mantenimiento del hardware. Este proceso incluye la definición de políticas y procedimientos de operación para una administración efectiva del procesamiento programado, protección de datos de salida sensitivos, monitoreo de infraestructura y mantenimiento preventivo de hardware. Una efectiva administración de operaciones ayuda a mantener la integridad de los datos y reduce los retrasos en el trabajo y los costos operativos de TI.

Criterio de TI aplicables:



Este proceso satisface el requisito de negocio de TI para mantener la integridad de los datos y garantizar que la infraestructura de TI puede resistir y recuperarse de errores y fallas.
Este proceso se enfoca en cumplir con los niveles operativos de servicio para procesamiento de datos programados, protección de datos de salida sensitivos y monitoreo y mantenimiento de la infraestructura.

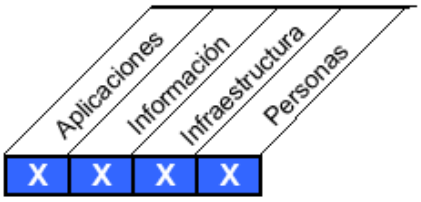
Lograr este objetivo de control solo es posible mediante:

- Operando el ambiente de TI en línea con los niveles de servicio acordados y con las instrucciones definidas.
- Manteniendo la infraestructura de TI.

La medición del proceso administración de operaciones se hace por medio de:

- Número de niveles de servicio afectados a causa de incidentes en la operación.
- Horas no planeadas de tiempo sin servicio a causa de incidentes en la operación.
- Porcentaje de activos de hardware incluidos en los programas de mantenimiento.

Recursos de TI aplicables:



Áreas focales aplicables:

Los objetivos de control detallados que se evalúan en este proceso son:

DS13.1 Procedimientos e instrucciones de operación
DS13.2 Programación de tareas
DS13.3 Monitoreo de la infraestructura de TI
DS13.4 Documentos sensitivos y dispositivos de salida
DS13.5 Mantenimiento preventivo de hardware

- **MONITOREAR Y EVALUAR**

  Todos lo procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y aplicación del gobierno.

Los objetivos de alto nivel que lo comprenden son los siguientes:

ME1 Monitorear y evaluar el desempeño de TI
ME2 Monitorear y evaluar el control interno
ME3 Garantizar cumplimiento regulatorio
ME4 Proporcionar gobierno de TI

2.4.6.3 BASADO EN CONTROLES

Control se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos del negocio se alcanzaran y los eventos no deseados serán prevenidos o detectados y corregidos.
Cada uno de los procesos de TI de COBIT tiene un objetivo de control de alto nivel y un número de objetivos de control detallados. Como un todo representan las características de un proceso bien administrado.

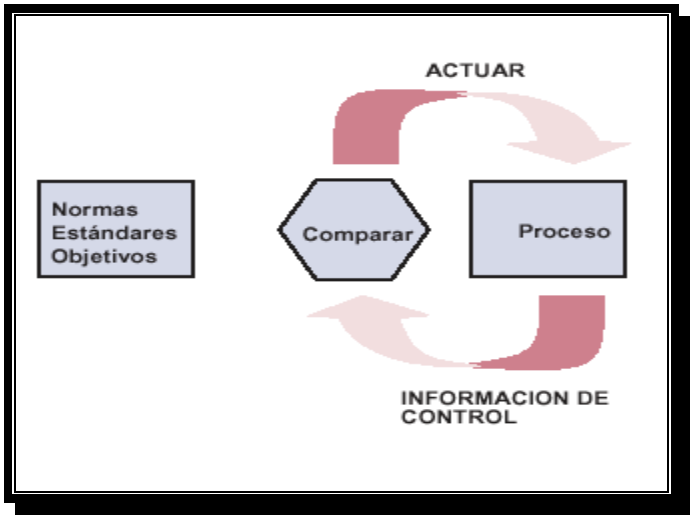


Figura 6 Modelo de Control

Se pueden establecer los siguientes tipos de controles:

- **CONTROLES DE NEGOCIO Y DE TI**
  En el sistema empresarial de controles internos impacta a TI en tres niveles:
  - Al nivel de dirección ejecutiva.
  - Al nivel de proceso de negocio.
  - Para soportar los procesos de negocio.

- **CONTOLES GENERALES DE TI Y CONTROLES DE APLICACIÓN**

  Los controles generales son aquellos que están inmersos en los procesos y servicios de TI.

  Los controles de aplicación son aquellos que están incluidos en las aplicaciones del proceso de negocio.

1.4.6.4 GENERADORES DE MEDICION

Una necesidad básica es entender el estado de sus propios sistemas de TI y decidir que nivel de administración y control debe proporcionar la empresa.

COBIT atiende estos temas por medio de:

- Modelos de madurez que facilitan la evaluación por medio de benchmarking y la identificación de las mejoras necesarias en la capacidad.
- Metas y mediciones de desempeño para los procesos de TI, que demuestren como los procesos satisfacen las necesidades del negocio y de TI, y como se usan para medir el desempeño de los procesos internos basados en los principios de un marcador de puntuación balanceada.
- Metas de actividades para facilitar el desempeño efectivo de los procesos.

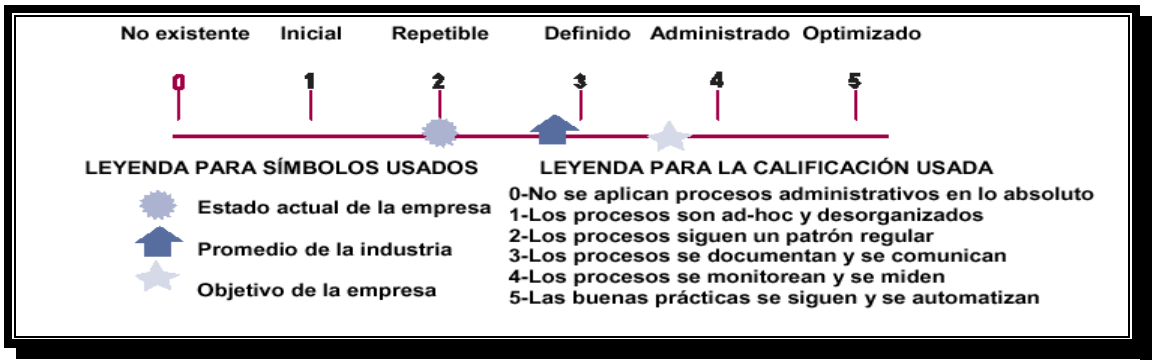


Figura 7 Representación Grafica de los modelos de madurez

1.4.9 FAMILIA DE PRODUCTOS COBIT

Los productos COBIT se han organizado en tres niveles, diseñados para dar soporte a:

- Administración y Consejos Ejecutivos
- Administración del negocio y de TI
- Profesionales en Gobierno, aseguramiento, control y seguridad.

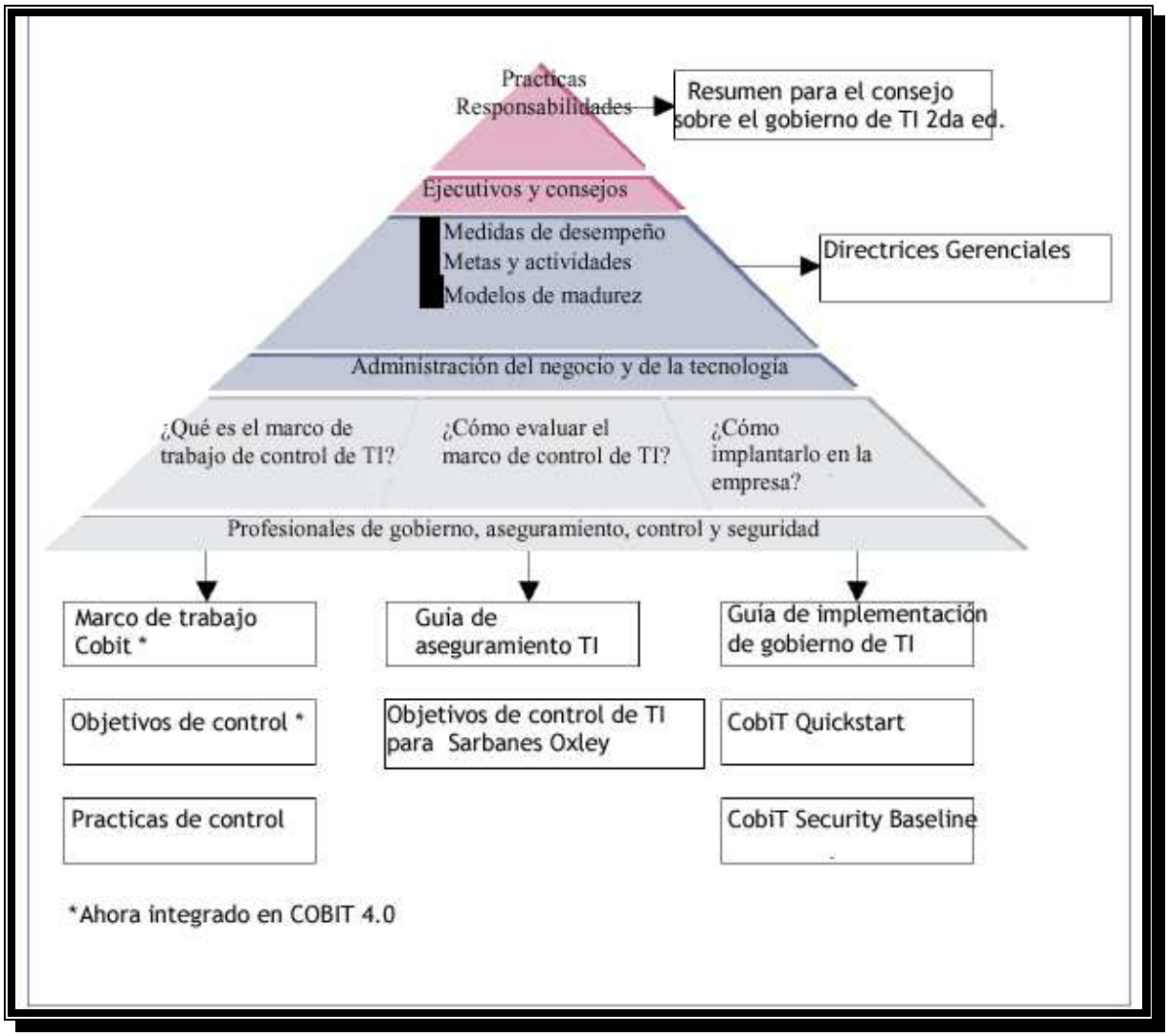


Figura 8 Productos COBIT

1.4.8 NUMERO DE CONTROL DE APLICACIÓN (ACN)

COBIT asume que el diseño e implementación de los controles de aplicación automatizados son responsabilidad de TI, y están cubiertos en el dominio de Adquirir e Implementar, con base en los requerimientos de negocio definidos, usando los criterios de información de COBIT. La responsabilidad operacional de administrar y controlar los controles de aplicación no es de TI, sino del propietario del proceso de negocio.

TI entrega y da soporte a los servicios de las aplicaciones y a las bases de datos e infraestructura de soporte. Por lo tanto, los procesos de TI de COBIT abarcan a los controles generales de TI, pero no los controles de las aplicaciones, debido a que son responsabilidad de los dueños de los procesos del negocio.

La siguiente lista sugiere un conjunto de objetivos de control de las aplicaciones identificados por ACn, número de Control de Aplicación (por sus siglas en inglés):

Controles de origen de datos/ autorización

AC1 Procedimientos de preparación de datos.
Los departamentos usuarios implementan y dan seguimiento a los procedimientos de preparación de datos. En este contexto, el diseño de los formatos de entrada asegura que los errores y las omisiones se minimicen. Los procedimientos de manejo de errores durante la generación de los datos aseguran de forma razonable que los errores y las irregularidades son detectadas, reportadas y corregidas.

AC2 Procedimientos de autorización de documentos fuente.

El personal autorizado, actuando dentro de su autoridad, prepara los documentos fuente de forma adecuada y existe una segregación de funciones apropiada con respecto a la generación y aprobación de los documentos fuente.

AC3 Recolección de datos de documentos fuente

Los procedimientos garantizan que todos los documentos fuente autorizados son completos y precisos, debidamente justificados y transmitidos de manera oportuna para su captura.

AC4 Manejo de errores en documentos fuente

Los procedimientos de manejo de errores durante la generación de los datos aseguran de forma razonable la detección, el reporte y la corrección de errores e irregularidades.

AC5 Retención de documentos fuente

Existen procedimientos para garantizar que los documentos fuente originales son retenidos o pueden ser reproducidos por la organización durante un lapso adecuado de tiempo para facilitar el acceso o reconstrucción de datos así como para satisfacer los requerimientos legales.

Controles de entrada de datos

AC6 Procedimientos de autorización de captura de datos.

Los procedimientos aseguran que solo el personal autorizado capture los datos de entrada.

AC7 Verificaciones de precisión, integridad y autorización

Los datos de transacciones, ingresados para ser procesados (generados por personas, por sistemas o entradas de interfases) están sujetos a una variedad de controles para verificar su precisión, integridad y validez. Los procedimientos también

garantizan que los datos de entrada son validados y editados tan cerca del punto de origen como sea posible.

AC8 Manejo de errores en la entrada de datos

Existen y se siguen procedimientos para la corrección y re-captura de datos que fueron ingresados de manera incorrecta.

Controles en el Procesamiento de datos

AC9 Integridad en el procesamiento de datos

Los procedimientos para el procesamiento de datos aseguran que la separación de funciones se mantiene y que el trabajo realizado de forma rutinaria se verifica. Los procedimientos garantizan que existen controles de actualización adecuados, tales como totales de control de corrida-a-corrida, y controles de actualización de archivos maestros.

AC10 Validación y edición del procesamiento de datos

Los procedimientos garantizan que la validación, la autenticación y la edición del procesamiento de datos se realizan tan cerca como sea posible del punto de generación. Los individuos aprueban decisiones vitales que se basan en sistemas de inteligencia artificial.

AC11 Manejo de errores en el procesamiento de datos

Los procedimientos de manejo de errores en el procesamiento de datos permiten que las transacciones erróneas sean identificadas sin ser procesadas y sin una indebida interrupción del procesamiento de otras transacciones válidas.

Controles de salida de datos

AC12 Manejo y retención de salidas

El manejo y la retención de salidas provenientes de aplicaciones de TI siguen procedimientos definidos y tienen en cuenta los requerimientos de privacidad y de seguridad.

AC13 Distribución de salidas

Los procedimientos para la distribución de las salidas de TI se definen, se comunican y se les da seguimiento.

AC14 Cuadre y conciliación de salidas

Las salidas cuadran rutinariamente con los totales de control relevantes. Las pistas de auditoría facilitan el rastreo del procesamiento de las transacciones y la conciliación de datos alterados.

AC15 Revisión de salidas y manejo de errores

Los procedimientos garantizan que tanto el proveedor como los usuarios relevantes revisan la precisión de los reportes de salida. También existen procedimientos para la identificación y el manejo de errores contenidos en las salidas.

AC16 Provisión de seguridad para reportes de salida

Existen procedimientos para garantizar que se mantiene la seguridad de los reportes de salida, tanto para aquellos que esperan ser distribuidos como para aquellos que ya están entregados a los usuarios.

Controles de límites

AC17 Autenticidad e integridad

Se verifica de forma apropiada la autenticidad e integridad de la información generada fuera de la organización, ya sea que haya sido recibida por teléfono, por correo de voz, como documento en papel, fax o correo electrónico, antes de que se tomen medidas potencialmente críticas.

AC18 Protección de información sensitiva durante su transmisión y transporte

Se proporciona una protección adecuada contra accesos no autorizados, modificaciones y envíos incorrectos de información sensitiva durante la transmisión y el transporte.

CAPITULO II

METODOLOGIA DE LA INVESTIGACIÓN Y DIAGNOSTICO

2. METODOLOGIA DE LA INVESTIGACIÓN

2.1 TIPO DE INVESTIGACIÓN

El problema relacionado a la inadecuada administración de los recursos informáticos y a la deficiente confiabilidad de la información, se investigó mediante el enfoque hipotético deductivo, analizando desde una perspectiva general los aspectos que podrían ser la causa fundamental en el surgimiento del fenómeno. Con el propósito de describir realidades o elementos específicos de comprobación que permitan plantear alternativas de solución o control.

2.2 TIPO DE ESTUDIO

La investigación se realizó bajo un estudio de tipo explicativo, analítico, correlacional, que pretende no solo describir el fenómeno relacionado con la inadecuada administración de los recursos informáticos y la deficiente confiabilidad de la información, analizar sus posibles causas, características, variables y elementos, estudiando la forma en que una variable ejerce influencia sobre la otra, la vinculación entre las variables y la causa principal que da origen al fenómeno en estudio

2.3 UNIDADES DE ANÁLISIS

Las unidades de análisis que se considerarón en la investigación están constituidas por los usuarios del sistema y la gerencia informática de las municipalidades en estudio.

2.8 UNIVERSO Y MUESTRA

La población para esta investigación está formada por la totalidad de alcaldías que utilizan el Sistema de Administración Financiera Integrada Municipal, entre ellas están Antiguo Cuscatlán, Sonsonate, San Antonio del Monte, Acajutla, San Martín y Juayua.
La población en estudio es de características homogéneas, por tratarse de instituciones que ocupan SAFIMU II, para los mismos fines.

2.9 INSTRUMENTOS Y TÉCNICAS A UTILIZADAS EN LA INVESTIGACIÓN

El instrumento de investigación que se utilizó para la recolección de datos fué, el cuestionario con preguntas cerradas, se elaboró un único cuestionario dirigido al personal de las áreas de tesorería, contabilidad, informática y presupuesto de las alcaldías de los municipios de Juayua, San Antonio del Monte, Ciudad Arce, Acajutla y Antiguo Cuscatlan. A través de su utilización se recolectó la información de campo necesaria para demostrar que la problemática planteada existe y que requiere de formas de solución o control.

Las técnicas utilizadas en el desarrollo de la investigación fueron:

a) Las sistematización bibliografica:
   Se efectuara una recopilación de la información bibliografica disponible para el área legal y técnica, mediante el uso de las distintas fuentes tanto primarias como secundarias.
b) Se diseñara un cuestionario dirigido a las unidades de análisis determinadas como la población en estudio.

2.10 PROCESAMIENTO DE LA INFORMACIÓN

El procesamiento de la información se efectuó por medio del paquete utilitario Excel, mediante un programa diseñado para la tabulacion de los datos, la elaboración de los gráficos y el cruce de variables. Las interpretaciones de los resultados se mostraron en términos absolutos y relativos.

2.11 ANÁLISIS E INTERPRETACION DE DATOS

La información obtenida mediante las encuestas realizadas al personal de las municipalidades en estudio específicamente en las áreas de Contabilidad, tesorería y presupuestos. Se proceso a través de hojas de cálculo que representan cantidades y porcentajes de los datos recopilados para cada una de las preguntas del cuestionario, además se elaboraron gráficos para ilustrar los resultados.

2.7.1 DIAGNOSTICO DE LA INVESTIGACION

De los análisis e interpretaciones de los resultados a las preguntas que se incluyeron en los cuestionarios, se procedió a realizar un análisis general respecto a los objetivos que se buscaban en las preguntas.

1. ¿Existe un departamento de informática establecido dentro de la institución?

RESPUESTAS	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
SI	17	65,38%
NO	9	34,62%
TOTAL	26	100,00%

Objetivo: Determinar si existe un departamento de informática formalmente establecido.

Análisis: El 63.38% afirmo que existe un departamento de informática en la institución y el resto de la población que representa el 34.62% afirma que no existe, de acuerdo al resultado se concluyo en más del 50% de las instituciones sujetas al estudio tienen establecido un departamento de informática en la institución.

2. ¿Cuál es la formación académica del personal encargado del mantenimiento tanto de hardware como de software de la institución?

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
BACHILLER EN INFORMÁTICA	5	17,24%
TECNICO EN MANTENIMIENTO DE REDES	7	24,14%
LICENCIATURA EN COMPUTACION	1	3,45%
INGENIRERIA EN SISTEMAS	5	17,24%
OTROS	11	37,93%
TOTAL	29	100,00%

Objetivo: Determinar si las personas encargadas del mantenimiento tienen la formación académica apropiada.

Análisis: En base al resultado obtenido se concluye que el 37.93% de la población encuestada posee una formación académica, la cual no está relacionada con el cargo que desempeña en el departamento de informática, mientras que un 24.14% posee una formación académica de Técnico en Mantenimiento de Redes.

3. ¿Cuál es el personal o área encargada de evaluar el desempeño del departamento de informática?

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
GERENCIA GENERAL	11	44,00%
AUDITORIA INTERNA	1	4,00%
USUARIOS	2	8,00%
JEFE DE DEPARTAMENTO	11	44,00%
TOTAL	25	100,00%

Objetivo: Determinar si existe un responsable de evaluar el desempeño del departamento de informática.

Análisis: De acuerdo a los resultados obtenidos se determinó que el área encargada de evaluar el desempeño del departamento de informática se realiza en forma conjunta por la gerencia general y el jefe del departamento de informática el cual esta representado por un 88% de la población.

4. ¿Existen políticas y procedimientos encaminados a mejorar la eficiencia y eficacia de los recursos informáticos de esta institución?

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
SI	11	42,31%
NO	15	57,69%
TOTAL	26	100,00%

Objetivo: Conocer si están establecidos en un documento formal las políticas y procedimientos a seguir para el uso eficiente y eficaz de los recursos informáticos.

Análisis: El 57.69% de la población considera que no existen políticas y procedimientos establecidos que vayan encaminados a la eficiencia y eficacia en el uso de los recursos informáticos, y el 42.31% de la población considera que si existen.

5. Si su respuesta fue a la pregunta anterior fue afirmativa ¿Qué tipo de políticas y procedimientos son aplicados a los recursos informáticos?

RESPÙESTAS	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
CONTROLES SOBRE EL ACCESODE USUARIOS AL SISTEMA	7	35,00%
CONTROLES EN LA ENTRADA, PROCESAMIENTO Y SALIDA DE DATOS	5	25,00%
CONTROLES PARA LA SEGURIDAD DEL EQUIPO DE COMPUTO Y MOBILIARIO DEL ÁREA INFORMÁTICA	5	25,00%
CONTROLES DE SEGURIDAD LOGICA	3	15,00%
TOTAL	20	100,00%

Objetivo: Comprobar que existen dichas políticas, y que estas realmente son dirigidas al área de informática.

Análisis: A través de los resultados se concluyó que las políticas encaminadas a mejorar la eficiencia y eficacia de los recursos informáticos, están basados en controles al acceso de usuarios al sistema con el 35% de afirmaciones, mientras el 25% asegura tener controles para la seguridad del equipo de cómputo y mobiliario del área informática y controles en la entrada, procesamiento y salida de datos y un 15% de la población dice tener políticas de control de seguridad lógica.

6. ¿Cuál es el grado de confiabilidad de la información procesada en el sistema?

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
ALTA	11	42,31%
MEDIA	14	53,85%
BAJA	1	3,85%
TOTAL	26	100,00%

Objetivo: Conocer el nivel de confianza que la información les proporciona a los usuarios de acuerdo a su criterio personal.

Análisis: El 53.85 de la población afirma que la confiabilidad de la información procesada es media, no obstante el 42.31% afirma que la confiabilidad es alta, mientras que un 3.85% afirma que es baja, en resumen se determinó que el nivel de confianza de la información procesada es media.

7. Si en la pregunta anterior contesto media o baja, ¿cuales de las siguientes razones considera como causa de la deficiente confiabilidad de la información procesada?

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
CAPACITACION DEL PERSONAL	11	45,83%
DEFICIENCIA EN EL PROCESAMIENTO DE LA INFORMACIÓN	7	29,17%
CAPACITACION EN LA INTERPRETACION DE LOS RESULTADOS	3	12,50%
MANIPULACION EN LA BASE DE DATOS	3	12,50%
TOTAL	24	100,00%

Objetivo: Conocer algunas de las razones por las cuales el usuario considera que la información no proporciona un alto nivel de confianza.

Análisis: De acuerdo a los resultados obtenidos, se determinó que la principal causa que genera un nivel de confiabilidad media es la falta de capacitación del personal.

8. ¿En cuales de las siguientes áreas considera que el sistema necesita mejorar?

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
CONTROLES DE ACCESO AL SISTEMA	6	22,22%
PERFILES DE USUARIO	2	7,41%
INTERFASES AMIGABLES	8	29,63%
FUNCIONAMIENTO DEL SISTEMA	11	40,74%
TOTAL	27	100,00%

Objetivo: conocer las áreas consideran que es necesario aplicar mejoras al sistema.

Análisis: De acuerdo a los resultados obtenidos el área que es considerada como la que necesita mejoras en su proceso es la de funcionamiento del sistema con un 40.74% de afirmaciones.

9. ¿Considera que los reportes que suministra el sistema son adecuados y suficientes para las necesidades de la institución y para la toma de decisiones?

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
SI	15	57,69%
NO	11	42,31%
TOTAL	26	100,00%

Objetivo: Determinar si los reportes que suministra el sistema son adecuados y suficientes a las necesidades de información, de acuerdo al criterio de los usuarios.

Análisis: De acuerdo a los resultados obtenidos el 57.69 % de la población considera que los reportes que suministra el sistema son adecuados y suficientes para las necesidades de la institución y para la toma de decisiones, mientras que el 42.31% restante considera que no cumplen con dichas características.

10. ¿Cuáles de las siguientes características reúnen los reportes suministrados por el sistema?

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
LA INFORMACIÓN GENERADA ES COMPLETA	12	19,67%
LOS REPORTES QUE GENERA EL SISTEMA SON ADECUADOS	3	4,92%
LOS REPORTES QUE GENERA EL SISTEMA SON SUFICIENTES	9	14,75%
LOS REPORTES SON ENTREGADOS EN EL TIEMPO OPORTUNO	11	18,03%
LA INFORMACIÓN GENERADA ES RAZONABLE Y CONFIABLE	10	16,39%
LOS REPORTESGENERADOS SON COMPRENSIBLES PARA LOS USUARIOS	16	26,23%
TOTAL	61	100,00%

Objetivo: Establecer que características cualitativas cumplen los reportes suministrados por el sistema.

Análisis: De acuerdo a los resultados obtenidos el 26.23% de la población en estudio considera que la principal característica que poseen los reportes que genera el sistema es la comprensibilidad para los usuarios; un 19.67% afirma que es información completa, es decir que no necesita ser reprocesada; otro 18.03% de los encuestados valora que es el tiempo oportuno en la entrega de los reportes; un 16.39% considera que es la razonabilidad y la confianza de la información generada.

11. ¿Anteriormente, le han realizado auditoria al área informática de esta entidad?

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
SI	6	23,08%
NO	20	76,92%
TOTAL	26	100,00%

Objetivo: Conocer si el área o departamento ha sido auditado alguna vez.

Análisis: De acuerdo a los resultados obtenidos, se determinó que no se han realizado con anterioridad auditoría de sistemas al área de Informática de la entidad con un el 76.92% de afirmaciones.

12. ¿En base a cual de las siguientes normativas técnicas ha sido realizada la Auditoría de Sistemas?

RESPUESTA	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
COBIT	0	0,00%
ISO 17799	0	0,00%
NIA`S	4	100,00%
TOTAL	4	100,00%

Objetivo: Conocer la normativa técnica que se utilizo en la realización de la auditoria de sistemas.

Análisis: El 100% de la población encuestada contesto que al momento de realizarles una auditoria esta se realizo en base a Normas Internacionales de Auditoría.

13. ¿Cuál es la formación académica de el personal que realizo la auditoría al departamento de informática?

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
BACHILLER TECNICO	0	0,00%
LIC. EN CONTADURIA PUBLICA	5	62,50%
INGENIEROS EN SISTEMAS	3	37,50%
OTROS	0	0,00%
TOTAL	8	100,00%

Objetivo: Determinar si el personal que realizo la auditoria tiene la formación académica apropiada para llevar a cabo dicha actividad.

Análisis: En base a los resultados obtenidos se determinó que el 62% de la población que realizó la auditoría de sistemas posee el grado académico de Licenciatura en Contaduría Pública, mientras que un 37.50% posee el titulo de Ingeniería en Sistemas.

14. Si su respuesta en la pregunta once fue negativa ¿Considera necesaria una auditoria al área o departamento de informática de esta entidad?

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
SI	16	76,19%
NO	5	23,81%
TOTAL	21	100,00%

Objetivo: Conocer si los usuarios consideran que es necesario realizar una auditoría al departamento de informática.

Análisis: En base a los resultados obtenidos, se concluyo que los que la gran mayoría de usuarios encuestados consideran que si existe la necesidad de realizar una Auditoria de Sistemas al departamento de Informática de la entidad.

15. ¿Considera que una auditoria de sistemas mejoraría la administración de los recursos informáticos y por ende los resultados de la información procesada por la institución?

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
SI	22	84,62%
NO	4	15,38%
TOTAL	26	100,00%

Objetivo: Determinar la necesidad de realizar una auditoría de sistemas.

Análisis: Se determinó que al realizar una Auditoría de Sistemas se mejoraría la administración en los recursos informáticos de las instituciones con un 84.62% de afirmaciones de los encuestados.

16. ¿Considera necesario contar con un documento que proporcione una guía para poder realizar una Auditoría de Sistemas?

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
SI	22	84,62%
NO	4	15,38%
TOTAL	**26**	100,00%

Objetivo: Conocer si los usuarios consideran necesario la elaboración de un documento guía para la evaluación de sistemas.

Análisis: En base a los resultados obtenidos se determinó que para una adecuada evaluación del sistema en una Auditoría es necesario contar con un documentos guía para la realización de la misma.

2.7.2 COMPROBACION DE HIPOTESIS

Con base a la información obtenida, del estudio de las unidades de análisis de la problemática planteada: "La inadecuada administración de los recursos informáticos y la deficiente confiabilidad de la información" se pudo comprobar que realmente existe el problema, y como parte del análisis de dichos resultados se concluye al respecto de la siguiente forma:

Relación de Preguntas 1, 4 y 15.

Conforme a los resultados obtenidos se comprueba que con un 65% de afirmaciones , las entidades en estudio poseen un departamento de informática, el cual no cuenta con políticas y procedimientos que contribuyan al uso eficiente y eficaz de los recursos informáticos de la institución, ya que un 58% de los encuestados confirman dicha ausencia de políticas, por lo anterior con el 85% de la población de acuerdo, se concluye que existe la necesidad de realizar una auditoría de sistemas para mejorar el uso de los recursos informáticos.

Relación de las preguntas 6, 7

Con los resultados obtenidos se establece que un 54% de la población coincide en que el grado de confiabilidad que ofrece la información procesada es media, 44% unas de las causas que fueron consideradas como de las principales son la falta de capacitación y las deficiencias en el procesamiento de la información. Dichas causas son problemas que son controlables al establecer políticas y procedimientos adecuados, los cuales al no estar claramente definidos en un documento por escrito, que sea del conocimiento de

todos los usuarios, permiten que se cometan los mismos errores en repetidas ocasiones. Pero es por medio de la auditoria de sistemas que las entidades obtienen un análisis de la situación actual y del desempeño del sistema, a su vez obtienen recomendaciones para corregir dichas observaciones.

CAPITULO III

“PROCESO DE AUDITORÍA DE SISTEMAS BASADO EN EL DOMINIO DE ENTREGAR Y DAR SOPORTE DEL MODELO COBIT APLICADO AL SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADA MUNICIPAL”

METODOLOGIA PROPUESTA

La propuesta sugerida para el proceso de Auditoría de Sistemas, se ha elaborado de conformidad con las Normas de Auditoría de Sistemas (NAS) emitidas por la Asociación de Control y Auditoría de Sistemas de Información (ISACA), los Controles de Alto Nivel y Detallados del Dominio Entregar y Dar Soporte (DS) y los Controles de Aplicación (ACn), de los Objetivos de Control para la Información y Tecnologías Relacionas (COBIT), y las Normas Internacionales de Auditoría (NIA)emitidas por la federación Internacional de Contadores (IFAC).

Específicamente, las herramientas técnicas utilizadas en la propuesta, son:

1. NORMAS DE AUDITORÍA DE SISTEMAS (EMITIDAS POR ISACA)

- S5 Planeación
- S6 Ejecución de la Auditoría
- S7 Reporte
- S11 Uso de la evaluación de Riesgos en la Planeación de Auditoría
- S12 Materialidad de Auditoría
- S14 Evidencia de Auditoría

2. OBJETIVOS DE ALTO NIVEL DEL DOMINIO ENTREGAR Y DAR SPORTE (COBIT)

- DS4 Garantizar la continuidad del servicio.
- DS5 Garantizar la Seguridad de los Sistemas
- DS10 Administrar los problemas
- DS11 Administrar los Datos

3. CONTROLES DE APLICACIÓN (COBIT)

- Controles de Origen de Datos-Autorización
- Controles de Entrada de Datos
- Controles de Procesamiento de Datos
- Controles de Salida de Datos
- Controles de Límite de Datos

4. NORMAS INTERNACIONALES DE AUDITORÍA (EMITIDAS POR IFAC)

- NIA 300 Planeación de una Auditoría de Estados Financieros
- NIA 315 Entendimiento de la Entidad y su Entorno y Evolución de los Riesgos de Representación Errónea de Importancia Relativa
- NIA 700 Dictamen del Auditor Independiente sobre un Juego Completo de Estados Financieros de Propósito General

El abordaje para cada una de las fases del proceso de auditoría, se detalla a continuación:

I. FASE I PLANEACION

Para desarrollar esta fase, se hizo un análisis de las herramientas técnicas antes detalladas y se combinaron, haciendo uso del juicio de la mejor aplicación para definir y desarrollar el contenido del Memorando de Planeación, debido a que las Normas, tanto para la Auditoría Financiera como para la Auditoría de Sistemas, no definen elementos puntuales para realizar un proceso técnico completo, para una auditoría de esta naturaleza.
Esta fase se desarrolló en forma completa en la metodología propuesta en este documento.

II. FASE 2 EJECUCION

En la fase de ejecución del trabajo de auditoría, para efectos didácticos y de esta forma ejemplificar el proceso a seguir, se ejecutaron únicamente los procedimientos de la sección “Validación y Edición” del programa correspondiente al Procesamiento de Datos.
La organización de los papeles de trabajo se realizó elaborando una Hoja de Trabajo (HT) que comprende cada una de las etapas del ciclo de funcionamiento del sistema.
Las Cédulas Sumarias contienen un resumen de los “elementos” que componen cada una de las etapas del ciclo de funcionamiento del sistema, sobre las cuales se ejecutan los procedimientos de auditoría y en base a los resultados obtenidos se realizan las conclusiones pertinentes.
En el caso de las Cédulas de Detalle, se desarrollan los procedimientos establecidos en los Programas de Auditoría y los resultados obtenidos son remitidos a la Cédula Sumaria.

III. FASE 3 INFORME

Para la elaboración y presentación del Informe de Auditoría de Sistemas, se retoman los elementos contenidos en la NAS S7 “Reporte” y se han ordenado y desarrollado lógicamente para un entendimiento y aplicación adecuados.

La propuesta incluye esto únicamente; es decir, no se ha elaborado por completo el informe con todos sus elementos propiamente dichos, debido a que la finalidad es proponer la estructura y contenido del mismo, lo cual constituye el aporte de la propuesta, para esta fase del proceso.

5. PLANEACIÓN

5.1. OBJETIVOS DE AUDITORIA

5.1.1. OBJETIVO GENERAL

Evaluar la suficiencia de las medidas de control adoptadas por la entidad, con el propósito de verificar que la información que se procesa en el sistema sea confiable y útil para la correcta y oportuna toma de decisiones.

5.1.2. OBJETIVOS ESPECIFICOS

- Evaluar el adecuado funcionamiento del modulo de Tesorería de SAFIMU II.

- Verificar que el modulo de Tesorería de SAFIMU II cumplan con las normativas y requisitos legales como la ley AFI, Código Tributario, Ley de Impuesto sobre la Renta, Código Municipal, Manual de Control Interno de la Corte de Cuentas.

- Evaluar los controles de calidad en el ciclo de funcionamiento del sistema en el origen, entrada, procesamiento y salida de información orientado a verificar la integridad de los datos que ahí se almacena.

5.1.3. ENTENDIMIENTO DE LA ENTIDAD Y SU ENTORNO

5.1.3.1. NATURALEZA DE LA ENTIDAD

5.1.3.1.1. OPERACIONES DE LA ENTIDAD

Las operaciones básicas de la municipalidad de XXX consisten en la recaudación de tasas e impuestos, servicios de emisión de documentos de Registro del estado familiar, clínica municipal,

servicios de alumbrado público y aseo, mantenimiento y ornato de parques, mercados, cementerios y áreas verdes de la ciudad.

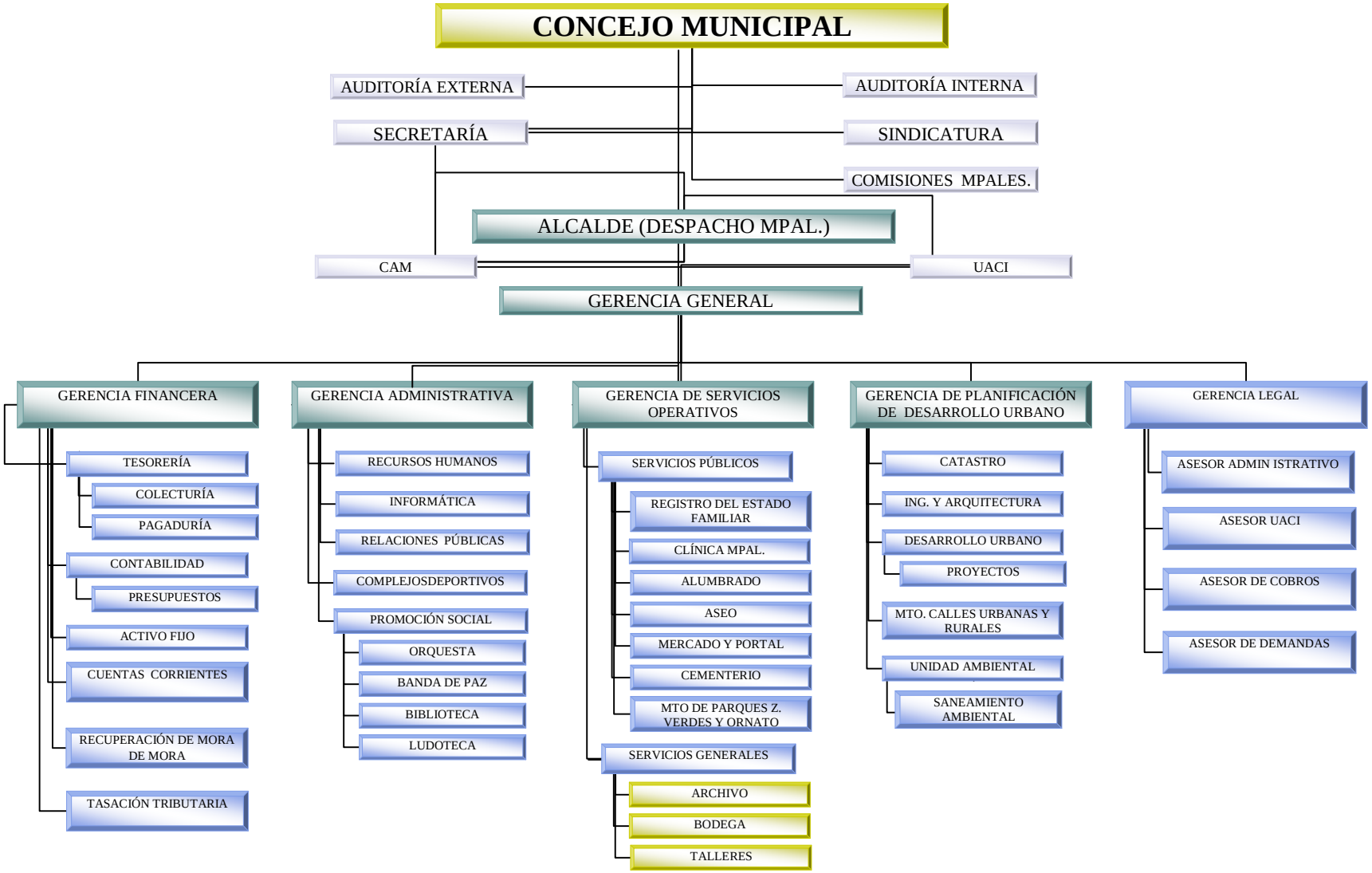
5.1.3.1.2. ESTRUCTURA ORGANIZATIVA

La Alcaldía de XXX está conformada por cuatro niveles gerenciales:

- Consejo Municipal
- Alcalde
- Gerencia General
- Gerencias Financiera, Administrativa, de Servicios Operativos, de Planificación de Desarrollo Urbano y Legal

A continuación se presenta la estructura organizativa de la institución:

FIGURA 9
ESTRUCTURA ORGANIZATIVA DE ALCALDIA MUNICIPAL DE XXX



5.1.3.1.3. REGULACIÓN APLICABLE AL SISTEMA

Las disposiciones legales que rigen el funcionamiento del sistema son:

- Código Municipal
- Ley de Administración Financiera del Estado
- Normas Técnicas de Control Interno Específicas para la Municipalidad de XXX
- Ley de Impuesto sobre la Renta
- Ley de Impuesto a la Transferencia de bienes muebles y a la Prestación de Servicios

A continuación se presenta una tabla con las disposiciones legales más relevantes aplicables al sistema.

TABLA 1

NORMATIVA LEGAL APLICADA A SAFIMU II

DISPOSICIÓN LEGAL	ÁRTICULO	APLICACIÓN
Código Municipal	**Art. 55** Deberes del secretario: En el siguiente literal expresa: 6- Expedir de conformidad con la ley, certificaciones de las actas del concejo o de cualquier otro documento que repose en los archivos, previa autorización del alcalde. **Art.86** Inciso 2 Para que sean de legitimo abono los pagos hechos por los tesoreros o por los que hagan sus veces, deberán estar recibidos firmados por los recipientes u otras personas a su ruego si no supieren o no pudieren firmar, y contendrán El Visto Bueno del Sindico Municipal y El Dese del Alcalde Municipal, con el sello correspondiente en su caso.	Como lo expresa la ley antes de hacer erogaciones en la municipalidad se debe emitir una acta y acuerdo esto de hace en las sesiones del concejo municipal y así establecer en el monto exacto de la erogación de acuerdo a la codificación presupuestaria, dentro del sistema al momento de haberse ya efectuado las cotizaciones y tener la orden de compra ingresada al sistema se crea un usuario al Sr. Secretario Municipal y este se encarga de asignar el numero de acta y acuerdo ya establecido a la cuenta presupuestaria que refleje la orden de compra. Al momento de ingresar la orden de compra o un justificante de pago de salarios estos deben de tener su codificación presupuestaria correspondiente. En el proceso que lleva la orden de compra una vez ingresara dentro del sistema esta debe tener el Dese del Alcalde y el Visto Bueno del Sindico con sus respectivos usuarios dentro del sistema.
Ley Administración Financiera del Estado	**Art. 99** Literal a) Establecer, poner en funcionamiento y mantener en cada identidad y organismos del sector público, un modelo especifico y único de contabilidad que integre las operaciones financieras, tanto presupuestarias como patrimoniales e incorpore los principios de contabilidad generalmente aceptables, aplicables al sector publico.	El sistema cumple con los lineamientos y principios establecidos por esta ley, a su vez es un sistema integrado con los módulos de Tesorería, Contabilidad y Presupuesto
Normas técnicas de control interno especificas de la Municipalidad de Antiguo Cuscatlán	**Art. 29** El Gerente General, Jefaturas, serán los responsables de implementar los sistemas de información y comunicación actualizados, acorde al plan estratégico de la municipalidad. **Art. 31** El Gerente General, Jefaturas, deberán asegurar que la información que procese sea confiable, oportuna, suficiente y pertinente para la toma de decisiones	El sistema de información con que cuenta esta municipalidad si cumple con los lineamientos de sistematizar el trabajo haciéndolo más eficiente y eficaz y cumpliendo con los requisitos de confiable, oportuno, suficiente y pertinente para la toma de decisiones
Ley de Impuesto sobre la renta	**Art. 58.-** Es agente de retención todo sujeto obligado por esta ley, a retener una parte de las rentas que pague o acredite a otro sujeto. **Art. 66.-** Las personas jurídicas, las personas naturales titulares de empresas, los fideicomisos, las Dependencias del Gobierno, las Municipalidades y las Instituciones Oficiales Autónomas que paguen o acrediten a las personas naturales que se encuentran dentro de los casos que a continuación se mencionan, sumas en concepto de pagos por prestación de servicios, asimismo, si se trata de anticipos por tales pagos en la ejecución de contratos o servicios convenidos, están obligadas a retener en concepto de este impuesto el porcentaje del 10% de dichas sumas, independientemente del monto de lo pagado.	La múnicipalidad cumple como agente de retención ya que retiene renta a proveedores y a personal que prestan sus servicios a la alcaldía. Además el sistema contempla la retención del 10% en el caso de personas naturales que prestan sus servicios a la institución

5.1.3.1.4. POLÍTICAS DE CONTROL INTERNO APLICABLES AL SISTEMA

Se deberán evaluar las políticas de control interno que son aplicadas al sistema, y la forma en que afectan al funcionamiento del mismo, específicamente para el Módulo de Tesorería, la administración no ha definido políticas ni normas de control interno.

5.1.4. EVALUACIÓN DE RIESGOS

5.1.4.1. TECNICA/ENFOQUE PARA EVALUACIÓN E IDENTIFICACION DE RIESGOS

El auditor de Sistemas de Información debe utilizar una técnica o enfoque apropiado de evaluación de riesgos, al desarrollar el plan general de auditoría y al determinar prioridades para la asignación eficaz de los recursos de auditoría conforme lo requiere la NAS S11 Párrafo 03, dicha elección queda a juicio profesional y la experiencia del auditor.

Para el análisis y evaluación del riesgo de auditoría y sus componentes se utilizó el enfoque que plantea el informe COSO, el cual evalúa sobre la base de los riesgos existentes.

El enfoque establece los siguientes pasos:

1. Identificar los procesos
2. Identificar las actividades que componen cada proceso
3. Identificar los objetivos de cada actividad
4. Identificar los riesgos asociados a tales objetivos
5. Identificar los controles actuantes a cada riesgo
6. Establecer la exposición al riesgo de cada actividad
7. Analizar lo adecuado de los controles sobre la base de los riesgos identificados

Los pasos 1), 2), y 3) fueron considerados durante el diseño de los instrumentos de recopilación de la información (cuestionario y observación), debido a que estos elementos permiten obtener un entendimiento de la organización y su entorno (NAS S9 párrafo 05).

Los pasos 4) y 5) se desarrollaron a partir de la información recopilada a través de los instrumentos de auditoría utilizados, los cuales se representan gráficamente en la matriz de riesgos para su evaluación.

La exposición al riesgo y el análisis de lo adecuado de los controles, paso 6) y 7) consiste en el análisis y ponderación de los resultados obtenidos, para lo cual el auditor debe considerar la materialidad del riesgo aplicando los criterios establecidos en la NAS S12.

Para la ponderación del riesgo inherente de cada actividad, se consideraron aspectos tales como:

- Susceptibilidad de la naturaleza de las actividades
- Segregación de funciones
- Tamaño del módulo de tesorería
- Volumen de operaciones
- Experiencia y conocimiento del personal encargado de dichas actividades
- Independencia a presiones por parte de otros departamento o áreas considerando estos criterios y la experiencia profesional del auditor, este último establece el grado de riesgo inherente que estime conveniente acorde a cada actividad evaluada.

Para la ponderación del riesgo de control se utilizaron los resultados del cuestionario, analizando las políticas y

procedimientos establecidos por la entidad para minimizar los errores u omisiones en el procesamiento de datos.

Los resultados se evaluaron en base al Modelo de Madurez de COBIT 4.0, el cual permite establecer el nivel de riesgo para cada actividad considerando una escala de medición de los controles que han sido implementados.

TABLA 2

RELACION DE LOS NIVELES DE RIESGO DE AUDITORIA Y EL MODELO DE MADUREZ DE COBIT 4.0

NIVEL DE RIESGO	CRITERIOS	ESCALA DE MEDICIÓN
ALTO	No se aplican procesos adminisrtrativos en lo absoluto	0- NO EXISTENTE
	Los procesos son desorganizados	1- INICIAL
MEDIO	Los procesos siguen un patrón regular	2- REPETIBLE
	Los procesos se documentan y se comunican	3- DEFINIDO
BAJO	Los procesos se monitorean y se miden	4- ADMINISTRADO
	Las buenas prácticas se siguen y se automatizan	5- OPTIMIZADO

Con dicho análisis se determina si las políticas y procedimientos de control implementadas al sistema son debilidades importantes o se clasifican como deficiencias materiales.

La NAS S12 considera que es una deficiencia material, si la ausencia de controles ocasiona que no exista garantía razonable de que se cumplan los objetivos de la entidad.

Por otra parte una debilidad es importante, cuando la probabilidad de que un evento indeseado no sea prevenido o detectado es remota.

Partiendo de estos principios, el riesgo de control será alto cuando la deficiencia sea “Material”, es decir que no existan controles o estos sean desorganizados; el riesgo de control será medio cuando los controles siguen patrones regulares en la aplicación y estos se documenten y comuniquen a los usuarios; y el riesgo de control será bajo cuando la debilidad sea “Importante”, es decir que existen controles los cuales son monitoreados, y las buenas prácticas se automatizan.

Para la ponderación del riesgo de detección, se utilizaron los resultados de los riesgos inherentes y de control en forma conjunta, haciendo un cruce de ambos se obtiene el de detección; tomando como base el siguiente cuadro que se propone a continuación.

TABLA 3

INTERRELACIÓN DE LOS RIESGOS DE AUDITORIA

RIESGO INHERENTE	RIESGO DE CONTROL		
	ALTA	MEDIA	BAJO
ALTO	LO MAS BAJA	MEDIA	BAJA
MEDIO	MAS BAJA	MAS BAJA	MEDIA
BAJO	MEDIA	MAS ALTA	LO MAS ALTA

RIESGO DE DETECCIÓN

Una vez establecidos los niveles de riesgo inherente, de control y de detección, estos se incorporan al cuerpo de la matriz de riesgos para representar en forma ordenada y gráfica el análisis de los mismos.

5.1.4.2. ACCIONES PARA ATENDER LOS RIESGOS

El ciclo de evaluación se cierra con la determinación de las acciones a seguir respecto al nivel de riesgo que el auditor está dispuesto a aceptar, estas acciones pueden ser:

- Controlar el riesgo: En este caso se fortalecen los controles existentes o se agregan nuevos.
- Eliminar el riesgo: Este consiste en eliminar el activo relacionado y por ende el riesgo.
- Compartir el riesgo: Estos se realizan mediante acuerdos contractuales en el cual se traspasa parte del riesgo o su totalidad a un tercero.
- Aceptar el riesgo: Este consiste en determinar el nivel de exposición al riesgo adecuado

5.1.4.3. MATRIZ DE RIESGOS

A continuación se presenta la matriz de riesgos para cada proceso y las actividades correspondientes incluidas en el Módulo de Tesorería.

TABLA 4
MATRIZ DE RIESGOS

No.	ACTIVIDADES/PROCEDIMIENTOS	EVALUACION DEL TIPO DE RIESGO			ACCIONES SUGERIDAS ANTE EL RIESGO
		RIESGO INHERENTE	RIESGO DE CONTROL	RIESGO DE DETECCION	
	ORIGEN DE DATOS				
1	Elaboración de Planillas de Sueldos	MEDIO	ALTO	MAS BAJA	CONTROLAR
2	Deteccion de errores u omisiones en Planillas	ALTO	ALTO	LO MAS ALTA	CONTROLAR
3	Elaboración de Ordenes de Compra	BAJO	MEDIO	MAS ALTA	CONTROLAR
4	Deteccion de errores u omisiones en Ordenes de Compra	ALTO	ALTO	LO MAS BAJO	CONTROLAR
	ENTRADA DE DATOS				
5	Registro de Justificantes de Pago de Salarios	MEDIO	MEDIO	MAS BAJA	CONTROLAR
6	Carga de Actas Y Acuerdos de Justificante de Pago	MEDIO	MEDIO	MAS BAJA	CONTROLAR
7	Registro de Ordenes de Compra	MEDIO	MEDIO	MAS BAJA	CONTROLAR
8	Registro del Devengado de Factura	MEDIO	MEDIO	MAS BAJA	CONTROLAR
9	Carga de Actas Y Acuerdos de Devengado de Facturas	MEDIO	MEDIO	MAS BAJA	CONTROLAR
	PROCESAMIENTO DE DATOS				
10	Visto Bueno (Aprobación del Sindico Municipal)	BAJO	MEDIO	MAS ALTA	CONTROLAR
11	DESE (Aprobación del Alcalde)	BAJO	MEDIO	MAS ALTA	CONTROLAR
12	Aprobación de Justificante de Pago	MEDIO	MEDIO	MAS BAJA	CONTROLAR
13	Anulación de Justificante de Pago	MEDIO	MEDIO	MAS BAJA	CONTROLAR
14	Aprobación de Ordenes de Compra	MEDIO	MEDIO	MAS BAJA	CONTROLAR
15	Anulación de Ordenes de Compra	MEDIO	MEDIO	MAS BAJA	CONTROLAR
16	Ingreso de facturación de Ordenes de Compra	MEDIO	MEDIO	MAS BAJA	CONTROLAR
17	Solicitud de Cheque	ALTO	MEDIO	MEDIA	CONTROLAR
18	Aprobación de cheque	ALTO	MEDIO	MEDIA	CONTROLAR
19	Anulación de Cheque	ALTO	MEDIO	MEDIA	CONTROLAR
	SALIDA DE DATOS				
20	Emisión de Cheque	ALTO	MEDIO	MEDIA	CONTROLAR
21	Reimpresión de Cheque	ALTO	MEDIO	MEDIA	CONTROLAR

5.1.5. ALCANCE

Las áreas de la Alcaldía a las que se orienta la auditoría son las siguientes:

1. Gerencia Financiera
2. Departamento de Tesorería
3. Departamento de Informática

La auditoría consiste en evaluar el funcionamiento y seguridad del Sistema de Administración Financiera Integrada Municipal verificando los mecanismos de control de acceso a objetos del sistema, archivos con permisos especiales, mecanismos de identificación y autenticación, administración de usuarios, grupos y cuentas (creación, modificación, bloqueo y eliminación) aplicado a los criterios de información de COBIT el grado de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información contra posibles violaciones sufridas en el pasado y posibles en el futuro.

5.1.5.1. EVALUACIÓN DEL SISTEMA

5.1.5.1.1. MODULO DE TESORERÍA

Para la ejecución del trabajo se han diseñado cinco programas de auditoría a la medida, y se enfocaron al ciclo de funcionamiento del sistema, desarrollándose conforme al Dominio Entregar y Dar Soporte de COBIT y organizados por los Controles de Aplicación (ACn), los cuales incluyen el origen, entrada, procesamiento, salida y límites de datos.

5.1.5.1.2. ORIGEN DE DATOS

Se identificará cual es el origen de datos y la secuencia seguida para el ingreso de los mismos al sistema.
En esta etapa se analizarán cuales son los distintos tipos de datos que se procesan, su origen y seguimiento dentro del sistema.
Para ello se tomarán muestras de las actividades que se ejecutan y su interacción con el módulo evaluado.

5.1.5.1.3. ENTRADA DE DATOS

Se evaluará el ingreso de datos en las diferentes opciones de menú del modulo de tesorería, determinando qué validaciones existen en las pantallas de captura y verificando que cada elemento esté configurado adecuadamente.
Se verificará la actividad de entrada de datos al sistema, haciendo pruebas de integridad y validación en la captura de los mismos, considerando los tipos de datos: tipo fecha, numéricos, valores predefinidos, alfanuméricos, tipo moneda, tipo texto.

5.1.5.1.4. PROCESAMIENTO DE DATOS

Se verificarán los procesos que se realizan en el sistema y fuera de las pantallas de captura, a fin de determinar si se le da seguimiento a los procedimientos de carga, actualización y cierre de datos.
En este caso se retomarán los datos que se ingresen al sistema, realizando las pruebas respectivas, si es posible darle seguimiento de forma manual, tomando en cuenta los parámetros necesarios establecidos en los procedimientos y normas aplicables.

5.1.5.1.5. SALIDA DE INFORMACIÓN

Se evaluarán los controles establecidos por la entidad, para la distribución de los reportes a los usuarios.
Esta es la etapa final del ciclo operativo del sistema en la que se determina cuál es el producto final obtenido del mismo, verificando la calidad de las salidas, su destino, responsables de la distribución y recepción de las mismas y las políticas relativas al buen uso de la información, confidencialidad, resguardo y destrucción de información generada por el sistema que ya no será utilizada.

5.1.5.2. PRUEBAS ASISTIDAS POR COMPUTADORA

Se procederá a realizar pruebas detalladas con datos almacenados en el sistema. Estas pruebas se efectuarán en base a una muestra de datos obtenidos del sistema con el objeto de poder efectuar validaciones de integridad, dichas validaciones pueden ser la revisión de fechas congruentes, operaciones de devengo y pago de proveedores; en este caso se verificará que toda factura esté justificada con previo acuerdo de Secretaría Municipal y que todo pago esté justificado con factura. Se verificará la integridad de los montos originalmente ingresados en facturas, es decir que estos no superen los valores descargados con dicho documento.

5.1.6. ADMINISTRACIÓN DEL TRABAJO

5.1.6.1. PERSONAL DE AUDITORIA

La auditoria será realizada por el siguiente personal:

TABLA 5
PERSONAL ASIGNADO

NOMBRE	CARGO
Mercedes Guadalupe Galdámez Canales	Encargado
Ana María Constanza Rodríguez	Supervisor
Isabel Cristina Avalos Chávez	Asistente
Ing. Samuel Hernández	Asistente

El personal de auditoría asignado al desarrollo del trabajo debe realizará sus tareas en forma objetiva e independiente, y rechazar la realización de actividades que amenacen o parezcan amenazar su independencia.

5.1.6.2. PERSONAL AUDITADO

El personal clave que será entrevistado y contactado para suministrar información, es el siguiente:

TABLA 6

PERSONAL AUDITADO

NOMBRE	CARGO	INFORMACION
Luis Escamilla Rogel	Jefe de departamento de Informática	Base de datos Consultas sobre base datos
Carlos Miguel Sibrian	Analista Programador	Apoyo para comprension del sistema
Omar Ely Escobar	Analista Programador	
Franklin Rodríguez	Técnico en mantenimiento	
John Patrick Dale Escalón	Técnico en mantenimiento	
Carmen Marisela Mejía	Tesorera Municipal	Consulta sobre procedimientos administrativos, requerimiento de documentacion para el desarrollo del trabajo
Marta Alicia Avendaño	Cajera	
Francisca de Rios	Encargada de Especies Municipales	
Mercedes Cortés	Encargada de pago a proveedores	
Yency Carolina Chicas	Encargada de Nominas de salarios	

5.1.6.3. FECHAS CLAVES Y ACTIVIDADES PRINCIPALES

TABLA 7

FECHAS CLAVE Y ACTIVIDADES PRICIPALES

No	ACTIVIDADES A REALIZAR	INICIO DE ACTIVIDADES	FINALIZACION DE ACTIVIDADES
1	Evaluación y Diagnóstico del modulo de tesorería	28 de Enero 2008	01 de Febrero 2008
2	Evaluación de las políticas de Control Interno para el funcionamiento del módulo de tesorería	04 de Febrero 2008	08 de Febrero 2008
3	Entrevistas con el personal clave sobre las políticas de control interno para el funcionamiento del sistema	11 de Febrero 2008	22 de Febrero 2008
4	Ejecución de los programas de Auditoria	10 de Marzo 2008	21 de Marzo 2008
5	Ejecución de las pruebas asistidas por computadora.	10 de Marzo 2008	21 de Marzo 2008

5.1.6.4. PERSONAL ASIGNADO, TIEMPO Y COSTOS

Resumen de Costos para la Evaluación y Diagnóstico para el Módulo de Tesorería del Sistema de Administración Financiera Integrado Municipal. (8 semanas, (40 días) del 28 de enero al 21 de marzo 2008)

TABLA 8

PERSONAL ASIGNADO, TIEMPO Y COSTOS

ACTIVIDAD/PERSONAL	HORAS EFECTIVAS	COSTO POR HORA HOMBRE	COSTO TOTAL
Evaluación y Diagnostico del modulo de tesorería	40	$ 6.00	240.00
Evaluación de las políticas de Control Interno para el funcionamiento del sistema en el modulo de tesorería	40	$ 6.00	240.00
Entrevistas con el personal clave sobre las políticas de control interno para el funcionamiento del sistema	80	$ 6.00	480.00
Ejecución de los programas de Auditoria	80	$ 6.00	480.00
Ejecución de las pruebas asistidas por computadora	80	$ 6.00	480.00
TOTAL	320 Hrs.		$ 1,920

3.2. EJECUCION

En esta parte de la auditoría se ejecutó únicamente la sección Validación y Edición del Procesamiento de datos por considerarse una de las áreas más importantes en el ciclo de funcionamiento de los Sistemas de Información, a continuación se presenta el programas de auditoría y los procedimientos que se ejecutarón para ejemplificar el proceso:

No.	Descripcion	Hecho por	Revisado por	P/T	Ref. DS
AC10 VALIDACION Y EDICION DEL PROCESAMIENTO DE DATOS					
10	Determinar si existe mas de un código asignado a un mismo proveedor.	I.C.A.C	M.G.G	PD2.10	5.7
11	Verificando si existen números de factura asignados con proveedores que no se encuentran registrados.	I.C.A.C	A.M.C	PD2.11	11.1
15	Verificar que el acuerdo de Egreso sea procesado antes que la factura.	M.G.G	A.M.C	PD2.15	5.2
18	Verificar que no existan pagos que sobrepasen el monto original de orden de compra.	M.G.G	A.M.C	PD2.18	11.1
22	Verificar que los campos numericos para el ingreso en el numero de facturas de proveedores, no acepte caracteres tales como guiones, flecas, asteriscos.	M.G.G	A.M.C	PD2.22	5.4

3.2.1. PAPELES DE TRABAJO (PRUEBAS ASISTIDAS POR COMPUTADORA)

A continuación se presenta la ejecución de los procedimientos de auditoría mencionados anteriormente en los papeles de trabajo debidamente referenciados.

CANALES AVALOS Y ASOCIADOS
AUDITORIA Y CONSULTORIA DE SISTEMAS

CLIENTE: ALCALDIA MUNICIPAL DE XXX
PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)

INDICE DE MARCAS DE AUDITORIA

SIMBOLO	SIGNIFICADO
AA	Datos obtenidos de base de datos SAFIMU II
CR	Condición Reportable
¥	Verificado físicamente
r	Cumple con atributo clave de control
W	Comprobante de cheque examinado
@	Cotejado contra fuente externa
»	Cálculos matemáticos verificados

CANALES AVALOS Y ASOCIADOS
AUDITORIA Y CONSULTORIA DE SISTEMAS

CLIENTE: ALCALDIA MUNICIPAL DE XXX
PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)

HOJA DE TRABAJO
ÁREAS A EXAMINAR:

OD **ORIGEN DE DATOS**

ED **ENTRADA DE DATOS**

PD **PROCESAMIENTO DE DATOS**

SD **SALIDA DE DATOS**

LD **LÍMITE DE DATOS**

CLIENTE: ALCALDIA MUNICIPAL DE XXX
PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)

CEDULA SUMARIA DE ORIGEN DE DATOS

OD1 **Procedimientos de Preparación**

OD2 **Procedimientos de Autorización de Documentos Fuente**

OD3 **Recolección de Datos de Documentos Fuente**

OD4 **Manejo de Errores en Documentos Fuente**

OD5 **Retención de Documentos Fuente**

Conclusión:

CLIENTE: ALCALDIA MUNICIPAL DE XXX
PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)

CEDULA SUMARIA DE ENTRADA DE DATOS

ED1 **Procedimientos de Autorización de Captura de Datos**

ED2 **Verificaciones de Precisión, Integridad y Autorización**

ED3 **Manejo de Errores en la Entrada de Datos**

Conclusión:

CLIENTE: ALCALDIA MUNICIPAL DE XXX
PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)

CEDULA SUMARIA DE PROCESAMIENTO DE DATOS

PD1 Integridad en el Procesamiento de Datos

PD2 Validación y Edición del Procesamiento de Datos

PD3 Manejo de Errores en el Procesamiento de Datos

Conclusión: En base a las pruebas realizadas al módulo de tesorería, se determinaron deficiencias que afectan la seguridad del sistema y por ende la confiabilidad de la información de la entidad, debido a que los errores en el procesamiento de datos no son detectados por la ausencia de políticas y mecanismos de control en el sistema que prevengan, detecten y corrijan dichos errores.

CLIENTE: ALCALDIA MUNICIPAL DE XXX
PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)

CEDULA SUMARIA DE SALIDA DE DATOS

SD1 **Manejo y Retención de Salidas**

SD2 **Distribución de Salidas**

SD3 **Cuadre y Conciliación de Salidas**

SD4 **Revisión de Salidas y Manejo de Errores**

SD5 **Provisión de Seguridad para Reportes de Salida**

Conclusión:

CANALES AVALOS Y ASOCIADOS
AUDITORIA Y CONSULTORIA DE SISTEMAS

CLIENTE: ALCALDIA MUNICIPAL DE XXX
PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)

CEDULA SUMARIA DE LÍMITE DE DATOS

LD1 **Controles de Límites**
LD2 **Protección de Información Sensitiva durante su Transmisión o Transporte**

Conclusión:

CLIENTE: ALCALDIA MUNICIPAL DE XXX
PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)

CEDULA DE DETALLE DE VALIDACIÓN Y EDICIÓN DEL PROCESAMIENTO DE DATOS

PD2.10	Prueba de Códigos de Proveedores
PD2.11	Prueba de Facturas a Proveedores no registrados
PD2.15	Prueba de congruencia de fecha de acuerdos con Acuerdos de factura
PD2.18	Prueba de Órdenes de Compra
PD2.22	Prueba de Parametrización de Campos

Conclusión: En base a las pruebas realizadas al módulo de tesorería, se determinaron deficiencias que afectan la seguridad del sistema y por ende la confiabilidad de la información de la entidad, debido a que los errores en el procesamiento de datos no son detectados por la ausencia de políticas y mecanismos de control en el sistema que prevengan, detecten y corrijan dichos errores.

CLIENTE: ALCALDIA MUNICIPAL DE XXX
PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)

VALIDACION Y EDICION DEL PROCESAMIENTO DE DATOS
PRUEBA DE CÓDIGOS DE PROVEEDORES

Para verificar la existencia de códigos repetidos asignados a diferente proveedor se realizó una consulta SQL, la cual se detalla a continuación:

PD2.10.A

```
SELECT    Num_Proveedor, COUNT(Num_Proveedor)AS
          mas_prove
FROM      FITE_Catalogo_Proveedor
GROUP BY  Num_Proveedor
ORDER BY  mas_prove
```

Esta consulta permite visualizar si se repite un número de proveedor en la tabla FITE_Catalogo_Proveedor. A continuación se presenta una muestra del resultado obtenido:

H: ICAC
R: MGG

CLIENTE: ALCALDIA MUNICIPAL DE XXX
PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)

VALIDACION Y EDICION DEL PROCESAMIENTO DE DATOS
PRUEBA DE CÓDIGOS DE PROVEEDORES

PD2.10.1.1

# PROVEEDOR	# FACTURA	FECHA DE FACTURA
12955	03062	2007-03-07 00:00:00.000
2667	1842	2007-02-27 00:00:00.000
13072	59934	2007-03-31 00:00:00.000
10569	25481	2007-02-27 00:00:00.000
10569	25438	2007-02-23 00:00:00.000
13811	00126	2007-03-06 00:00:00.000
3580	184552	2007-03-13 00:00:00.000
3494	4-1-209184	2007-03-01 00:00:00.000
8026	1157	2007-03-13 00:00:00.000
14676	00200	2007-03-26 00:00:00.000
2392	08968	2007-03-24 00:00:00.000
6256	681/2007	2007-03-26 00:00:00.000
11491	14379	2007-03-26 00:00:00.000
15902	06SD00F0246	2007-06-21 00:00:00.000
15631	0702--	2007-07-02 00:00:00.000
15902	06SD00F0235	2007-06-11 00:00:00.000
15631	0709-	2007-07-02 00:00:00.000

AA

Conclusión: Al realizar las pruebas se determinó que no existen códigos repetidos para ningún proveedor

AA= Datos obtenidos de la base de datos de SAFIMU II

CLIENTE: ALCALDIA MUNICIPAL DE XXX
PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)

VALIDACION Y EDICION DEL PROCESAMIENTO DE DATOS
PRUEBA DE FACTURAS A PROVEEDORES NO REGISTRADOS

Para verificar la existencia de números de facturas asignados a proveedores no registrados en el sistema se realizo una consulta en SQL la cual se detalla a continuación:

PD2.11.A

```
SELECT    FITE_Factura_Orden.Num_Proveedor,
          FITE_Catalogo_Proveedor.Num_Proveedor
FROM      FITE_Factura_Orden left join
          FITE_Catalogo_Proveedor
on        FITE_Factura_Orden.Num_Proveedor =
          FITE_Catalogo_Proveedor.Num_Proveedor
order by  FITE_Catalogo_Proveedor.Num_Proveedor
```

Esta consulta permite determinar todos aquellos numeros de factura que se encuentran en la tabla FITE_Factura_Orden que no se encuentran asigandos a uno de los proveedores de la tabla FITE_Catalogo_Proveedor.

A continuacion se presenta una muestra de los resultados obtenidos:

H: ICAC
R: AMC

CLIENTE: ALCALDIA MUNICIPAL DE XXX
PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)

VALIDACION Y EDICION DEL PROCESAMIENTO DE DATOS
PRUEBA DE FACTURAS A PROVEEDORES NO REGISTRADOS

PD2.11.1.1

# PROVEEDOR	# FACTURA	FECHA DE FACTURA
10569	31825	2007-06-09 00:00:00.000
10569	31832	2007-06-13 00:00:00.000
10569	31836	2007-06-13 00:00:00.000
10569	32256	2007-06-15 00:00:00.000
4673	0000577403	2007-06-04 00:00:00.000
4673	0000578534	2007-06-12 00:00:00.000
4673	0002101623	2007-06-06 00:00:00.000
13936	07MS000F0013	2007-07-06 00:00:00.000
15631	0698	2007-07-02 00:00:00.000
15631	0699	2007-07-02 00:00:00.000
2392	01047	2007-07-09 00:00:00.000
2392	01334-	2007-07-14 00:00:00.000
2392	01153	2007-07-07 00:00:00.000
13934	00221	2007-07-06 00:00:00.000
13934	00220	2007-07-06 00:00:00.000
5761	005350	2007-07-10 00:00:00.000
44	06MZ000F067	2007-06-29 00:00:00.000
10569	32255	2007-06-15 00:00:00.000
7320	1030-	2007-07-04 00:00:00.000
7320	1078	2007-07-09 00:00:00.000
16055	758/2007	2007-07-11 00:00:00.000

AA

Conclusión: Al realizar las pruebas se determinó que no existen facturas asignadas a proveedores no registrados en el catalogo de proveedores.

AA= Datos obtenidos de la base de datos de SAFIMU II

H: ICAC
R: AMC

CLIENTE: ALCALDIA MUNICIPAL DE XXX
PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)

VALIDACION Y EDICION DEL PROCESAMIENTO DE DATOS

PRUEBA DE CONGRUENCIA DE FECHAS DE ACUERDO DE EGRESO CON FACTURA

Para verificar la existencia de acuerdos de egreso procesados antes de la fecha de la factura, se realizó una consulta en SQL la cual se detalla a continuación:

PD2.15.1

```
SELECT      ID_ORGANIZACION, NUM_PROVEEDOR, NUM_FACTURA,
            FEC_ACUERDO, FEC_FACTURA
FROM        FITE_Factura_Orden
WHERE       FEC_ACUE
```

H: MGG
R: AMCR

CLIENTE: ALCALDIA MUNICIPAL DE XXX
PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)

VALIDACION Y EDICION DEL PROCESAMIENTO DE DATOS PRUEBA DE CONGRUENCIA DE FECHAS DE ACUERDO CON FACTURA

Esta consulta permite identificar aquellos registros de la tabla FITE_Factura_Orden en donde la fecha de factura es mayor que la fecha en que surgió el Acuerdo. A continuación se presenta una pequeña muestra de los resultados obtenidos:

PD2.15.2

PROVEEDOR	FACTURA	FECHA DE ACUERDO	FECHA DE FACTURA
14887	0797	2007-06-20	2005-02-28
12955	03062	2007-03-20	2007-03-07
2667	1842	2007-03-20	2007-02-27
13072	59934	2007-04-03	2007-03-31
10569	25481	2007-03-13	2007-02-27
10569	25438	2007-03-13	2007-02-23
13811	00126	2007-03-20	2007-03-06
3580	184552	2007-03-28	2007-03-13
3494	4-1-209184	2007-03-28	2007-03-01

AA

Conclusión: Al realizar las pruebas de auditoría se determinó que existen facturas que fueron procesadas antes de la fecha del acuerdo de egreso. **(CR)**

AA= Datos obtenidos de la base de datos de SAFIMU II
CR= Condición reportable

CANALES AVALOS Y ASOCIADOS
AUDITORIA Y CONSULTORIA DE SISTEMAS

H: MGG
R: AMC

CLIENTE: ALCALDIA MUNICIPAL DE XXX
PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)

VALIDACION Y EDICION DEL PROCESAMIENTO DE DATOS
PRUEBA DE PAGO DE ORDENES DE COMPRA

Para la verificación de pagos de órdenes de compra para el año 20X1, se utilizarón las técnicas de auditoría con la ayuda de computadora (TAAC), desarrollando una consulta en el lenguaje SQL, la cual se presenta a continuación:

PD2.18.A

```
select *
from        fite_orden_compra
where       mto_pagos_orden > mto_original_orden
```

Esta consulta permite identificar aquellos registros en la tabla fite_orden_compra en donde los pagos efectuados para la orden no coinciden con el monto original de la misma. Los resultados obtenidos son:

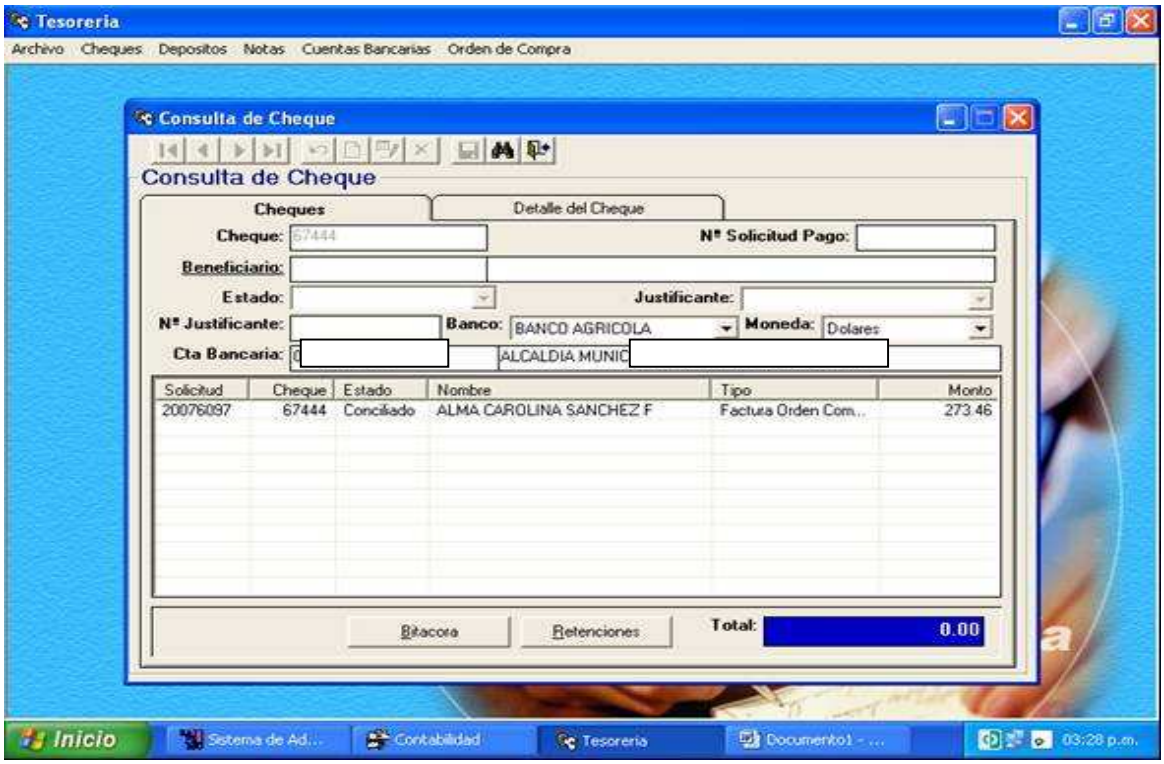
CANALES AVALOS Y ASOCIADOS
AUDITORIA Y CONSULTORIA DE SISTEMAS

H: MGG
R: AMC

CLIENTE: ALCALDIA MUNICIPAL DE XXX
PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)

PRUEBA DE PAGO DE ORDENES DE COMPRA

PD2.18.B



AA

Como se puede apreciar en la captura de consulta de cheque, existe para el periodo auditado la orden de compra # 4730 cuyo monto original de $ 0.00 y se efectuó un pago por $ 300.00 con cheque # 6744,**(CR)**

AA= Datos obtenidos de la base de datos de SAFIMU II
CR= Condición reportable

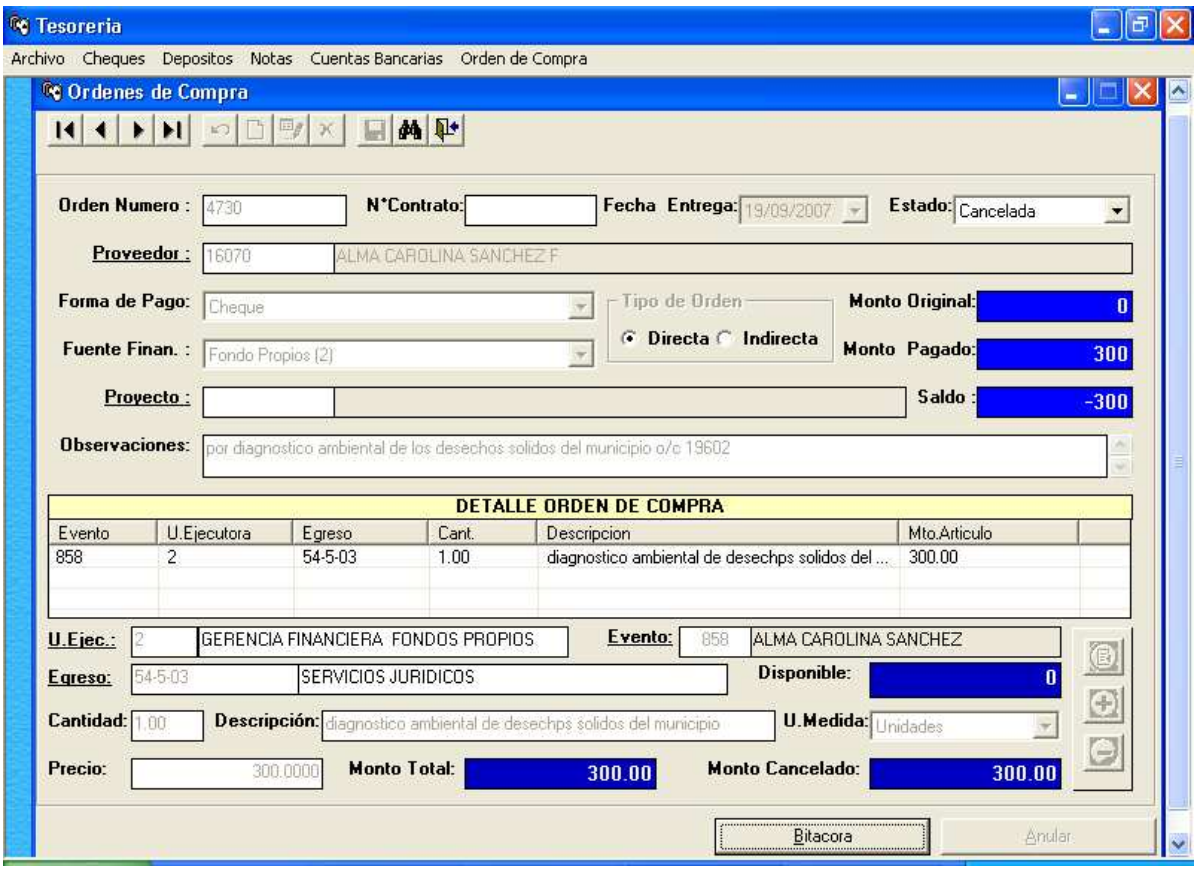
CANALES AVALOS Y ASOCIADOS
AUDITORIA Y CONSULTORIA DE SISTEMAS

H: MGG
R: AMC

CLIENTE: ALCALDIA MUNICIPAL DE XXX
PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)

CAPTURA DE PANTALLA ORDENES DE COMPRA

PD2.18.1.1



AA

Se genero la captura de pantalla de la orden de compra donde se pueden observar los detalles y condiciones de la compra.

AA= Datos obtenidos de la base de datos de SAFIMU II

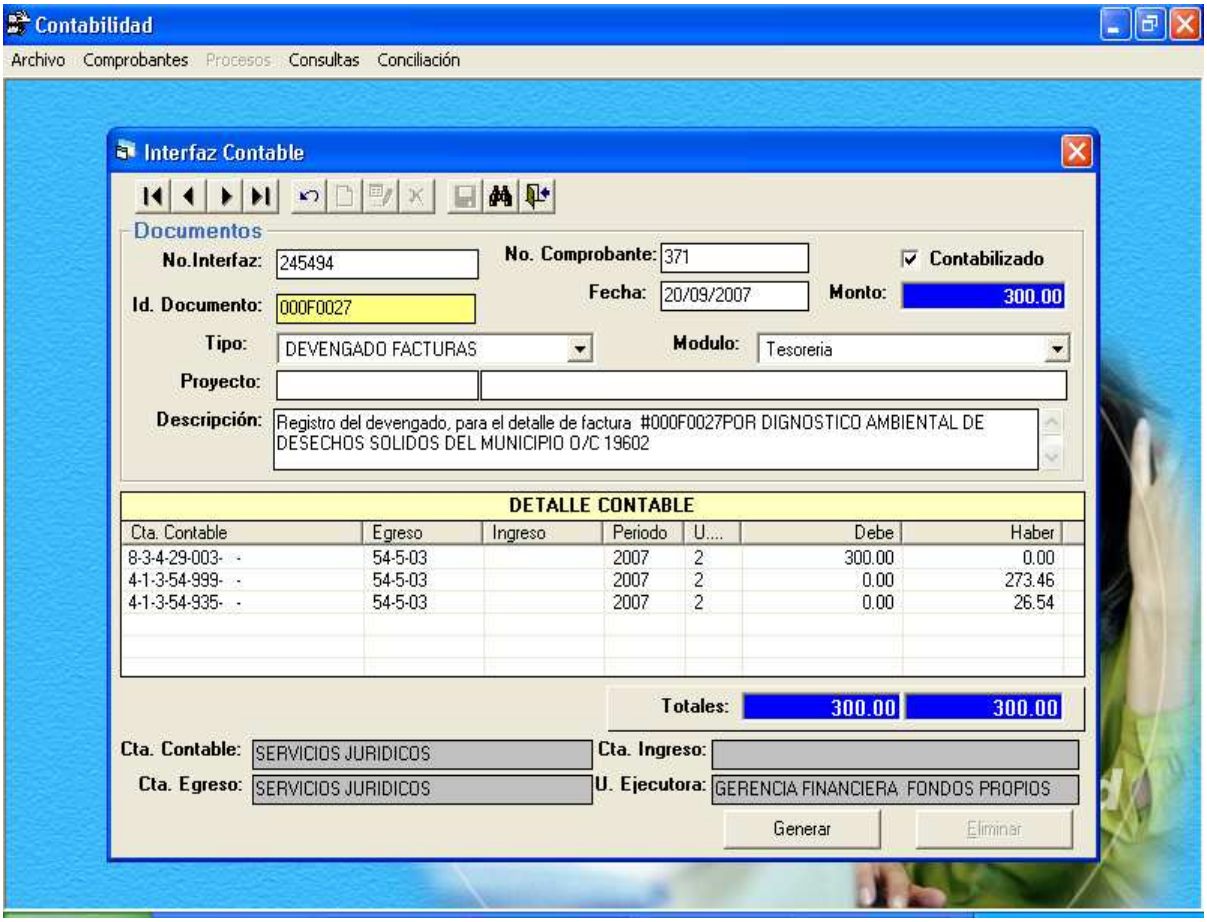
CANALES AVALOS Y ASOCIADOS
AUDITORIA Y CONSULTORIA DE SISTEMAS_____

H: MGG
R: AMC

CLIENTE: ALCALDIA MUNICIPAL DE XXX
PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)

CAPTURA DE PANTALLA DE DEVENGADO DE FACTURAS

PD2.18.1.2



AA

Se genero la captura de pantalla de la partida de devengado o provision del gasto, para verificar la contabilizacion del mismo.

AA= Datos obtenidos de la base de datos de SAFIMU II

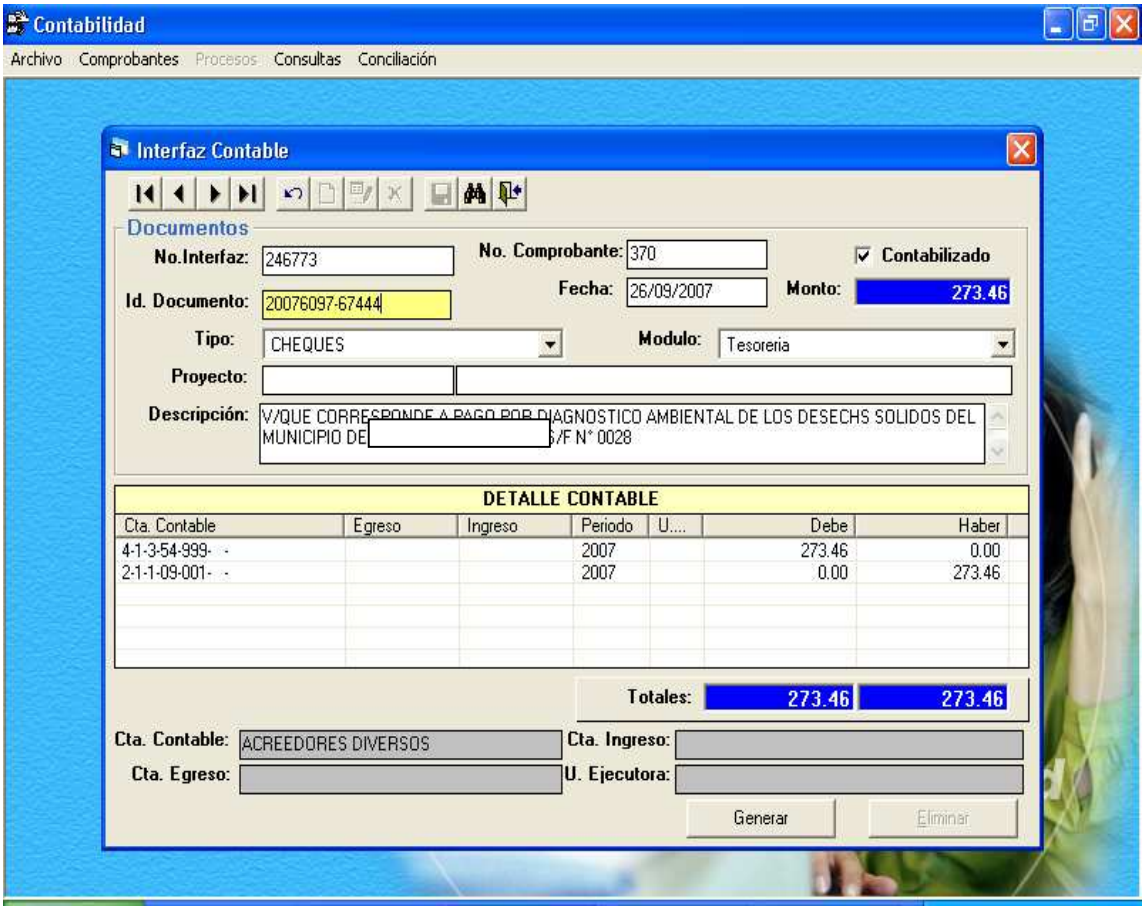
CANALES AVALOS Y ASOCIADOS
AUDITORIA Y CONSULTORIA DE SISTEMAS

H: MGG
R: AMC

CLIENTE: ALCALDIA MUNICIPAL DE XXX
PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)

CAPTURA DE PANTALLA DE PARTIDA DE PAGO DE FACTURA

PD2.18.1.3



AA

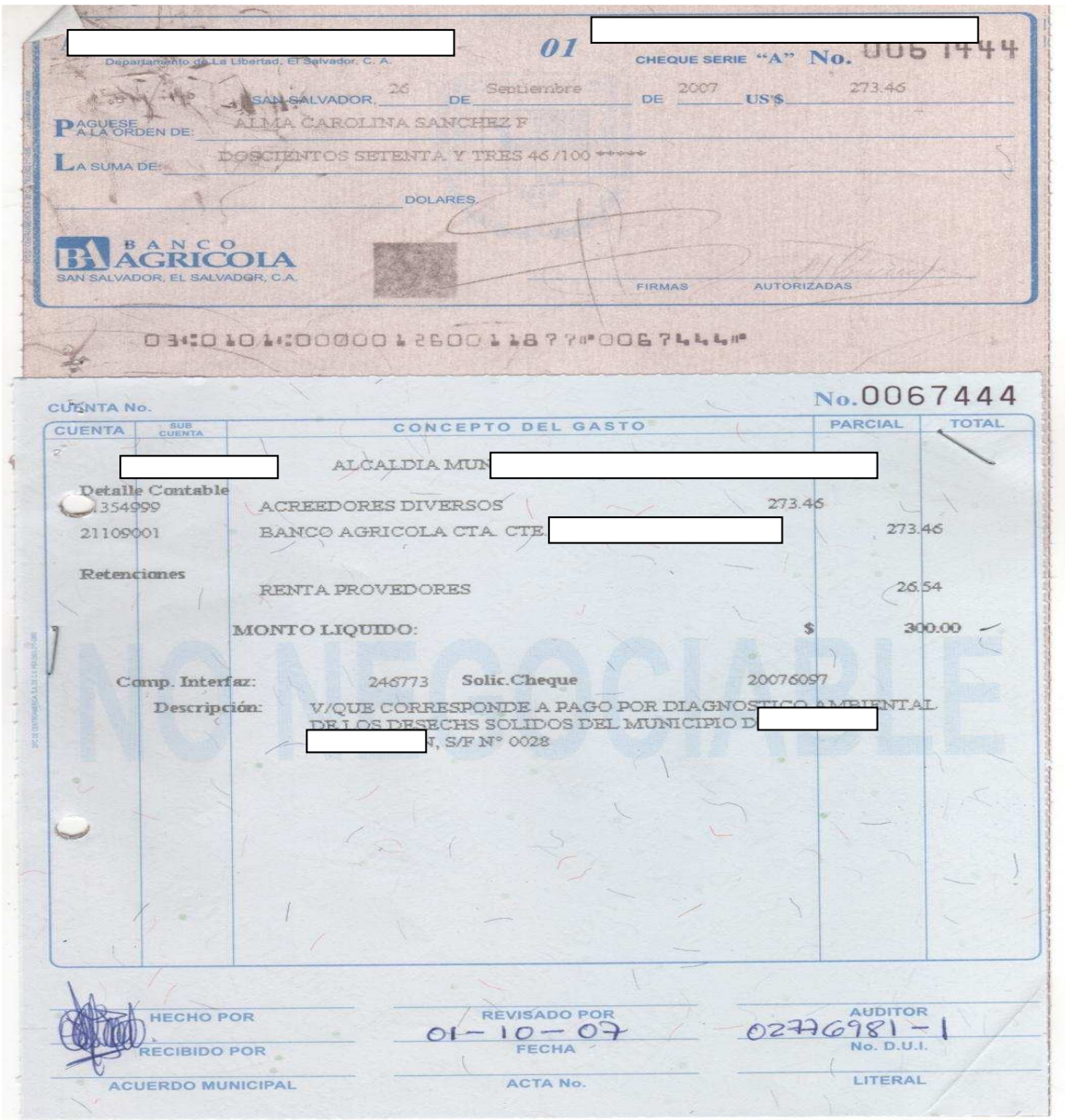
Se genero la captura de pantalla de la partida de pago del proveedor, para verificar la contabilización de la salida de los fondos.

AA= Datos obtenidos de la base de datos de SAFIMU II

CANALES AVALOS Y ASOCIADOS
AUDITORIA Y CONSULTORIA DE SISTEMAS

H: MGG
R: AMC

CLIENTE: ALCALDIA MUNICIPAL XXX
PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)



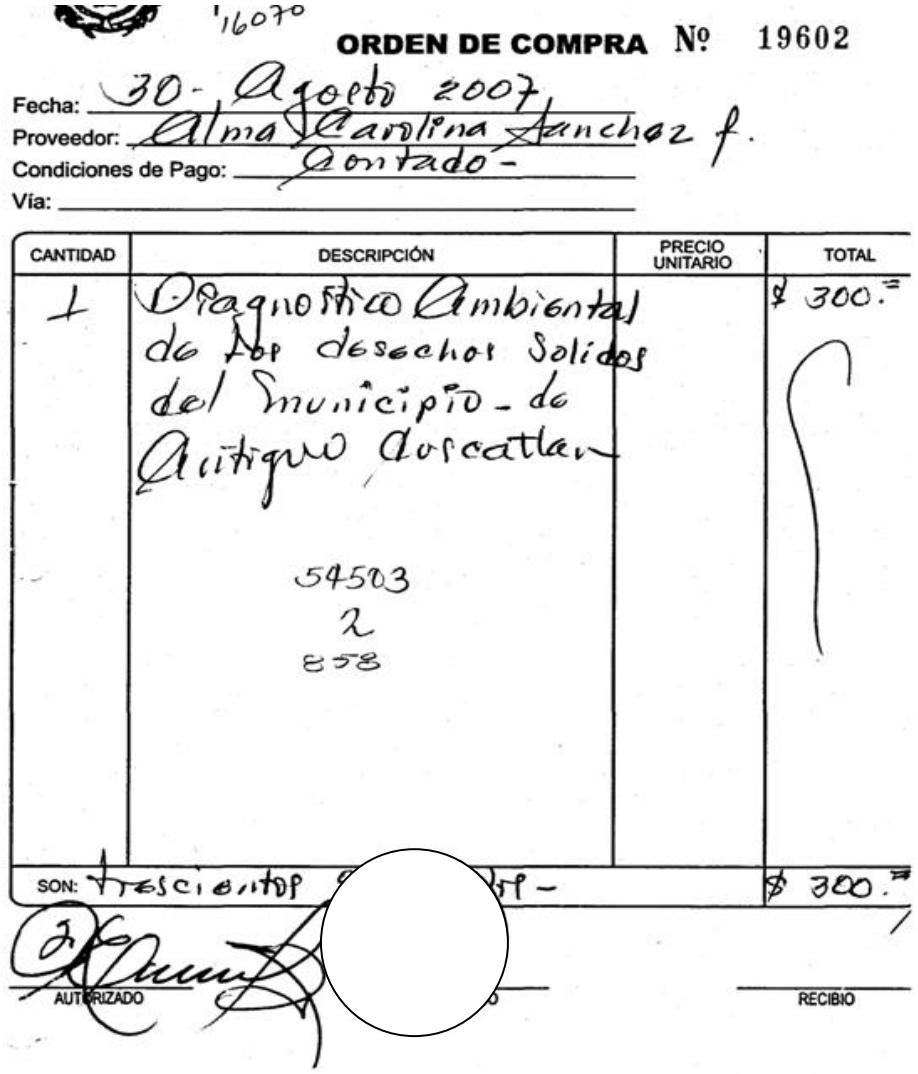
¥

¥ = Comprobante de Cheque verificado físicamente

CANALES AVALOS Y ASOCIADOS
AUDITORIA Y CONSULTORIA DE SISTEMAS

H: MGG
R: AMC

CLIENTE: ALCALDIA MUNICIPAL DE XXX
PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)



'16070

ORDEN DE COMPRA Nº 19602

Fecha: 30- Agosto 2007
Proveedor: Alma Carolina Sanchez f.
Condiciones de Pago: Contado -
Vía:

CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	TOTAL
1	Diagnostico Ambiental de los desechos Solidos del Municipio - de Acitiguo Moscatlan		$ 300.=
	54503 2 858		
SON: Trescientos			$ 300.=

AUTORIZADO

RECIBIO

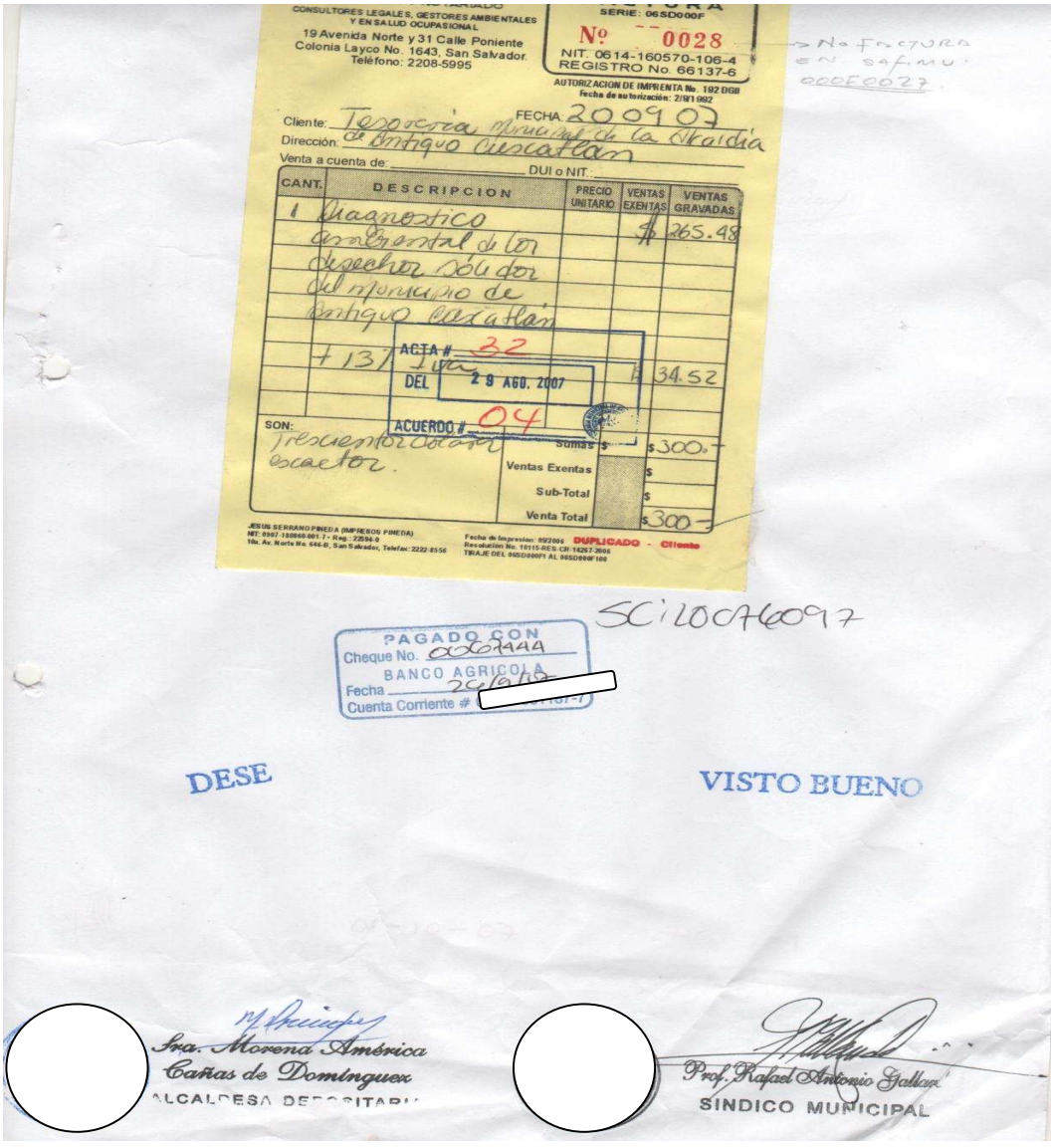
¥

¥ = Orden de Compra verificado físicamente

CANALES AVALOS Y ASOCIADOS
AUDITORIA Y CONSULTORIA DE SISTEMAS

H: MGG
R: AMC

CLIENTE: ALCALDIA MUNICIPAL DE XXX
PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)



¥

¥ = Factura de Compra del servicio con DESE y visto Bueno verificado físicamente

CANALES AVALOS Y ASOCIADOS
AUDITORIA Y CONSULTORIA DE SISTEMAS

H: MGG
R: AMC

CLIENTE: ALCALDIA MUNICIPAL DE XXX
PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)

VALIDACION Y EDICION DEL PROCESAMIENTO DE DATOS

PRUEBA DE PARAMETRIZACIÓN DE CAMPOS

Para verificar que los campos numéricos para el ingreso del número de facturas de proveedores no acepte caracteres tales como guiones(-), flecas(/), asteriscos(*) se realizó la siguiente consulta en SQL:

PD2.22.

```
SELECT *
FROM          FITE_Factura_Orden
WHERE         (YEAR(FEC_FACTURA) = 2007)
ORDER BY      NUM_FACTURA
```

Esta consulta permite visualizar todos los registros en la tabla FITE_Factura_Orden que posean fecha del año 2007. A continuación se presenta una pequeña muestra del resultado de la consulta:

CANALES AVALOS Y ASOCIADOS
AUDITORIA Y CONSULTORIA DE SISTEMAS

H: MGG
R: AMC

CLIENTE: ALCALDIA MUNICIPAL DE XXX

PERIODO AUDITORÍA: DEL 01 AL 31 DE DICIEMBRE DE 20X1
SISTEMA AUDITADO: SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL (SAFIMU II)

VALIDACION Y EDICION DEL PROCESAMIENTO DE DATOS

PRUEBA DE PARAMETRIZACIÓN DE CAMPOS

PD2.22.2

AA

Num_ Proveedor	Num_Factura	Fec_Factura	Mto_Factura	Est_Factu	Num_Orden Compra
15965	000003-1	26/03/2007 00:00	369.52	CA	3763
16059	120	14/11/2007 00:00	219824.56	AP	5136
4673	143780	11/01/2007 00:00	84.9	CA	3478
4673	144449	24/01/2007 00:00	26.26	CA	3599
44	000028--	22/01/2007 00:00	941	CA	3482
44	000029-	24/01/2007 00:00	1003	CA	3482
16100	000030-	22/10/2007 00:00	178.5	CA	5057
9017	000040--	18/05/2007 00:00	3.95	CA	4266
13936	0001------	11/05/2007 00:00	292.2	CA	4062
14949	000104-	13/03/2007 00:00	3454.28	CA	3718
16059	000114-	17/08/2007 00:00	709732.43	AP	4561

Conclusión: Al realizar las pruebas se determinó que en el campo numero de factura, NUM_FACTURA, este permite caracteres tales como, guiones, flecas, asteriscos debido a que la mascara de entrada no se diseñó adecuadamente. (CR)

AA= Datos obtenidos de la base de datos de SAFIMU II
CR= Condición reportable

3.3. INFORME

3.3.1. ELEMENTOS Y DESCRIPCION BASICA DEL INFORME DE AUDITORIA DE SISTEMAS

De conformidad con la Norma de Auditoría de Sistemas “S7 Reporte”, emitida por ISACA, el Auditor de Sistemas de Información debe suministrar un informe, en un formato apropiado, al finalizar la auditoría.

Al emitirse, el informe del Auditor de Sistemas de Información debe ser firmado, fechado y distribuido de acuerdo con los términos del estatuto de auditoría o carta compromiso.

El auditor de Sistemas de Información debe tener evidencia de auditoría suficiente y apropiada para respaldar los resultados reportados.

El informe debe identificar:

1. La organización
2. Los destinatarios previstos y respetar cualquier restricción con respecto a su circulación.

El informe de auditoría debe indicar:

1. El alcance
2. Objetivos
3. El periodo de cobertura
4. La naturaleza, plazo y extensión de las labores de auditoría realizadas
5. Los hallazgos
6. Conclusiones
7. Recomendaciones
8. Cualquier reserva, calificación o limitación que el auditor tuviese en cuanto al alcance de la auditoría.

3.3.2. PROPUESTA DE LA ESTRUCTURA DEL INFORME

A continuación se representa el modelo de informe de auditoría de sistemas aplicado a la Alcaldía Municipal de Antiguo Cuscatlán.

INFORME DE AUDITORIA DE SISTEMAS

Antiguo Cuscatlán, Día, Mes, Año

Gerencia General
Alcaldía Municipal de Antiguo Cuscatlán
Presente

Párrafo introductorio:
(Este apartado deberá contener, el sistema auditado, área auditada, periodo a evaluar y se revelara una declaración de la responsabilidad de la entidad y la responsabilidad del auditor)

OBJETIVOS DE LAS PRUEBAS REALIZADAS
(En este apartado se colocará el propósito de las evaluaciones realizadas al Modulo de Tesorería.)

ALCANCE DE LAS PRUEBAS
(En este apartado se describen las áreas en las que fueron aplicadas las pruebas de auditoría, plazo y extensión de las labores de auditoría)

HALLAZGOS (DEBILIDADES)

1) ORIGEN DE DATOS
2) ENTRADA DE DATOS
3) PROCESAMIENTO DE DATOS
4) SALIDA DE DATOS

CONCLUSIONES

1) ORIGEN DE DATOS
2) ENTRADA DE DATOS
3) PROCESAMIENTO DE DATOS
4) SALIDAD DE DATOS

RECOMENDACIONES

1) ORIGEN DE DATOS
2) ENTRADA DE DATOS
3) PROCESAMIENTO DE DATOS
4) SALIDAD DE DATOS

F._____ F._____

Encargado de la Auditoría Supervisor de la Auditoría

Cc.

Consejo Municipal

Gerencia Financiera

Gerencia Informática

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

1. En base a la investigación se determinó que para una efectiva administración en los Sistemas de Información se deben definir medidas de control interno, con el objetivo de salvaguardar los recursos informáticos, ya que dichas medidas disminuyen el riesgo informático al que están expuestas las entidades; la ausencia de políticas de control interno en la entrada, procesamiento y salida de datos incrementa la probabilidad de errores potenciales que afectan la información presentada en los estados financieros de una entidad, y por ende conllevan a una inadecuada toma de decisiones.

2. Se concluyó que el Dominio Entregar y Dar Soporte del modelo COBIT, constituye una de las herramientas más apropiadas para evaluar el ciclo de funcionamiento de los sistemas de información ya que proporcionan una guía idónea y lineamientos adecuados para la evaluación de controles en los sistemas de información, para mejorar los niveles de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información.

3. La Auditoría a los Sistemas de Información permite tener una visión clara, sobre las vulnerabilidades de un Sistema de información y de que forma afecta la información presentada en los Estados Financieros de una entidad.

4.2 RECOMENDACIONES

1. Se deben implementar políticas de control interno encaminadas a mejorar la administración del sistema y por ende a proporcionar un grado de confiabilidad de la información aceptable con la finalidad de tomar decisiones adecuadas que afecten positivamente a las entidades.

2. Para mejorar la calidad en el trabajo de auditoría de sistemas se recomienda a los profesionales en el área, utilizar la metodología COBIT como una herramienta de soporte a través de un marco de trabajo de dominios y procesos que presenta las actividades de una manera manejable y lógica.

3. Realizar periódicamente Auditoría al Sistemas para monitorear si las políticas y medidas de controles establecidas por la administración funcionan adecuadamente y si estos están orientados a los objetivos de la entidad.

BIBLIOGRAFIA.

LIBROS

- HERNANDEZ Hernández, Enrique. Auditoria en informática, un enfoque metodológico y practico. México: Compañía Editorial Continental, S.A. de C.V, 1995. Primera Edición.
- MUNOZ Razo, Carlos. Auditoria en Sistemas Computacionales. México: Editorial Pearson Prentice Hall, 2002. Primera Edición.
- Diccionario de Sinónimos y Antónimos. Océano Grupo Editorial, S.A. España.

REVISTAS

- THIERAUF, Robert J. El contador Público gerencial especializado del colegio de contadores públicos. Lima, Perú. Año 2, Revista 9 Junio de 1997.

TRABAJOS DE INVESTIGACION

- GOMEZ Girón, José Alfredo. Diseño de un modelo de evaluación de los niveles de riesgos en la auditoria informática. Tesis para optar al grado de Licenciatura en Contaduría Publica. San Salvador, El Salvador. Universidad de El Salvador. Facultad de Ciencias Económicas. Escuela de Contaduría Pública.
- CLAROS Cruz, Evelyn Marlene. Auditoría en Informática basada en las NIA´s aplicables a un ambiente de CIS. Tesis para optar al grado de Licenciatura en Contaduría Publica. San Salvador, El Salvador. Universidad de El Salvador. Facultad de Ciencias Económicas. Escuela de Contaduría Pública.

NORMAS TÉCNICAS Y LEGALES

- Instituto Mexicano de Contadores Públicos, A.C. Normas Internacionales de Auditoria. México Edición 2006.

- Information Systems Audit and Control Association (ISACA). Objetivos de Control para la Información y Tecnologías Afines (COBIT 4.0). Edición 2005

- Ley de Administración Financiera del Estado, Decreto Legislativo No. 584, 14 de Abril de 2008.
- Normas Técnicas de Control Interno específicas para la Municipalidad de Antiguo Cuscatlán, dado en el salón de Sesiones del Consejo Municipal, Antiguo Cuscatlán, 27 de Febrero de 2004.
- Ley de Impuesto sobre la Renta, Decreto 134 del 18 de Diciembre de 1991.

DIRECCIONES ELECTRONICAS

- QUINTERO, Oscar. Auditoría. Monografías.com. Disponible en <http://www.monografias.com/trabajos3/concepaudit/concepaudit.shtml> [Consulta: 27 de Mayo 2007]

- ROJAS Corsico, Ivana Soledad. Auditoria de sistemas de información. Disponible:<http://www.monografias.com/trabajos14/auditoriasistemas/auditoriasistemas.shtml> [Consulta: 27 de Mayo 2007]

- Control Interno, Seguridad y Auditoria Informática. Disponible en:<http://auditi.com/cobit1.htm> [Consulta: 15 de Junio 2007]

- Normas Generales para la Auditoria de Sistemas de Información.

- Disponible en:<http://www.adacsi.org.ar/es/content.php?id=79> [Consulta: 08 de Agosto 2007]

❖ Código de Ética Profesional.
Disponible en: http://www.adacsi.org.ar/es/content.php?id=42>
[Consulta: 08 de Agosto 2007]

❖ Normas de Auditoría de Sistemas de Información.
Disponible en: <http://www.isaca.org>
[Consulta: 20 de Febrero 2008]

ANEXO 1
CUESTIONARIO DE CONTROL INTERNO

CANALES AVALOS Y ASOCIADOS
AUDITORIA Y CONSULTORIA DE SISTEMAS
CUESTIONARIO DE CONTROL INTERNO PARA EVALUAR EL MODULO DE TESORERIA

CUESTIONARIO DE CONTROL INTERNO PARA EVALUAR EL MODULO DE TESORERIA
SISTEMA DE ADMINISTRACIÓN FINANCIERA INTEGRADO MUNICIPAL II

OBJETIVO: Evaluar las políticas y procedimientos establecidos para la administración y el control del ciclo de operaciones de la información (Origen, Entrada, Proceso, Salida y Límites)

No	DESCRIPCION	SI	NO	N/A
1	Para la información que será procesada en el modulo de tesorería ¿Existe una guía o flujograma de procedimientos para ordenarla y clasificarla previo a su ingreso al sistema?		✔	
2	¿Para la elaboración de planillas y ordenes de compra, se verifica que en ellos se encuentre claramente consignada toda la información que será necesaria para el llenado de los campos en los formularios de captura?	✔		
3	¿Se realizan evaluaciones constantes al personal responsable de la elaboración de planillas y ordenes de compra?		✔	
4	¿Existen procedimientos para la detección y control de errores u omisiones en la elaboración de planillas y ordenes de compra?		✔	
5	Para toda orden de compra ¿Existe por lo menos tres cotizaciones diferentes, del bien o servicio a ser adquirido?	✔		
6	¿Existe un responsable de la evaluación de los errores u omisiones en dichos documentos?		✔	
7	¿Se deja como referencia en estos documentos, las iníciales o firma de la persona que lo elaboró?	✔		
8	¿Existe una persona responsable de autorizar y aprobar los documentos antes de ser ingresadas al sistema?	✔		
9	¿Existe autorización restringida para la reproducción de dichos documentos?		✔	
10	¿Para el acceso al modulo de tesorería y a los diferentes niveles del sistema, cada usuario poseen una clave de acceso única?	✔		
11	¿Existe una persona responsable de la administración de las cuentas de usuarios y la asignación de accesos al sistema de los mismos?	✔		
12	¿Existe un manual de usuario para el manejo del sistema que sea del conocimiento de los mismos?	✔		
13	¿Permite el sistema dejar campos vacíos en los formularios de captura de datos?		✔	
No	**DESCRIPCION**	**SI**	**NO**	**N/A**

CANALES AVALOS Y ASOCIADOS
AUDITORIA Y CONSULTORIA DE SISTEMAS
CUESTIONARIO DE CONTROL INTERNO PARA EVALUAR EL MODULO DE TESORERIA

14	¿Los cálculos de tasas, intereses y retenciones son realizados por el sistema de forma automática o realizados por el usuario fuera del sistema?		✔	
15	¿Existe un procedimiento formal y documentado para el registro de las retenciones? 1)Proveedores 2)Servicios Eventuales	✔		
16	¿Para el ingreso de las órdenes de compra y justificantes de pago y devengado de facturas, los campos en los formularios de captura están parametrizados o son llenados manualmente por el usuario?	✔		
17	¿Se verifica que la carga del acta y acuerdo sean realizados únicamente por la persona autorizada?	✔		
18	¿Existe un proceso para la autorización de las órdenes de compra y cuál es?		✔	
19	Dentro del Sistema ¿Existe la posibilidad de realizar movimientos con fechas correspondientes a periodos Anteriores, posteriores o Ya cerrados?	✔		
20	¿En los campos tipo moneda existen límites para los valores máximos a ingresar?		✔	
21	¿Existen procedimientos de revisión posteriores al ingreso de los datos al modulo de tesorería?		✔	
22	¿Las correcciones de errores en la entrada de datos son realizadas en el momento en que se identifican, con previa autorización?		✔	
23	¿Existe una bitácora de registro de las operaciones realizadas dentro del modulo de Tesorería, que permita determinar fecha, hora, tipo de movimiento y usuario que realizo el ingreso de datos?	✔		
24	¿Se verifica que todo justificante de pago posea un acta y un acuerdo vinculado a la operación del gasto?	✔		
25	¿Se verifica que para la aprobación de los justificantes de pago, estos cuenten obligatoriamente con Visto Bueno y DESE?	✔		
26	¿Existen medidas de control para los justificantes de pago anulados?		✔	
27	¿Se verifica que toda solicitud de cheques se vincule a un justificante de pago?	✔		
28	Para la selección del tipo de cheque, ¿Existe un mecanismo dentro del sistema que verifique que la selección sea correcta de acuerdo al tipo de operación a cancelar?		✔	

CANALES AVALOS Y ASOCIADOS
AUDITORIA Y CONSULTORIA DE SISTEMAS
CUESTIONARIO DE CONTROL INTERNO PARA EVALUAR EL MODULO DE TESORERIA

No	DESCRIPCION	SI	NO	N/A
29	¿Existen políticas y procedimientos de control para la aprobación de cheques?		✔	
30	¿Existe una persona responsable de la aprobación de cheques?	✔		
31	¿Cuál es el proceso para la aprobación de cheques?			✔
32	¿Existen controles de los cheques anulados y las causas de dichas anulaciones?		✔	
33	¿Cuál es el proceso para la aprobación de las retenciones de proveedores y personal eventual?			✔
34	¿Existe una persona responsable de la aprobación de las retenciones?	✔		
35	¿Existen procedimientos para la prevención, detección y corrección de errores en el procesamiento de datos?		✔	
36	¿Existen rutinas de detección de errores u omisiones que permitan la identificación de valores duplicados?		✔	
37	¿Los errores son corregidos en el momento en que son detectados y quien es el encargado de autorizar su corrección?	✔		
38	¿Existen documentación soporte de las correcciones realizadas al sistema por errores en el procesamiento?	✔		
39	¿Son interrumpidas otras operaciones del sistema durante la corrección de los errores y omisiones?		✔	
40	¿Existen una bitácora que registre las operaciones realizadas dentro del modulo, que permita determinar fecha, hora, tipo de movimiento, equipo utilizado y usuario que realizo la aprobación del documento procesado?	✔		
41	¿Se verifica que la fecha de la factura del proveedor sea posterior a la fecha del DESE?		✔	
42	¿Existen montos de facturas que difieren con el valor de la orden de compra?		✔	
43	¿Existen facturas emitidas por proveedores no registrados en la entidad?		✔	
44	¿Existe personal asignado para la impresión de los diferentes reportes de salida?	✔		
45	Una vez suministrados los reportes por el sistema ¿Existe la necesidad de reprocesar la información en una aplicación adicional (Excel)?	✔		
46	¿Existe una lista de distribución de los reportes generados por el sistema de acuerdo a	✔		

CANALES AVALOS Y ASOCIADOS
AUDITORIA Y CONSULTORIA DE SISTEMAS
CUESTIONARIO DE CONTROL INTERNO PARA EVALUAR EL MODULO DE TESORERIA

	las necesidades de información del usuario.			
No	**DESCRIPCION**	**SI**	**NO**	**N/A**
47	¿Existe personal autorizado para el acceso a los reportes de salida de información?	✔		
48	¿Existen revisiones continuas para determinar las necesidades de información de los usuarios en los reportes de salida y quien es el encargado de realizarlas?		✔	
49	¿Existen procedimientos en el sistema permitan controlar el momento en que el pago de un justificante queda formalizado con la entrega del cheque?		✔	
50	¿Existen procedimientos de control para la opción de reimpresión de cheques?		✔	
51	¿Que tipo de atributos se identifican en los reportes generados por el sistema? a)Nombre del Reporte b)Periodo que Comprende c)Modulo al que corresponde d)fecha y hora de la impresión e)numero de paginas	✔		
52	¿Existen procedimientos de destrucción y almacenamiento de los reportes con información restrictiva o confidencial?	✔		
53	¿Se realizan procedimientos de corrección, cuando al conciliar las salidas se detectan errores, alteraciones u omisiones?	✔		
54	¿Existen procedimientos establecidos para detectar los errores u omisiones en los reportes de salida?		✔	
55	¿Existen procedimientos establecidos para proporcionar seguridad y privacidad para los reportes impresos?	✔		
56	¿Que tipo de procedimientos se realizan para verificar la autenticidad e integridad de la información originada fuera de la entidad? a)Confirmaciones telefónicas b)Vía fax c)Correo electrónico d)Correo de voz e)otras	✔		
57	¿Bajo cuales de las siguientes circunstancias se realizan confirmaciones externas? a)Por inconsistencia en la documentación recibida. b)otras	✔		

CANALES AVALOS Y ASOCIADOS
AUDITORIA Y CONSULTORIA DE SISTEMAS
CUESTIONARIO DE CONTROL INTERNO PARA EVALUAR EL MODULO DE TESORERIA

No	DESCRIPCION	SI	NO	N/A
58	¿Se realiza documentación de dichas confirmaciones?	✔		
59	¿Se posee una clasificación de la información de acuerdo a la sensibilidad que representa para la entidad?	✔		
60	¿Se implementan políticas o procedimientos para proteger la información sensitiva durante el proceso de transmisión de esta?		✔	

ANEXO 2
PROGRAMAS DE AUDITORÍA

CANALES AVALOS Y ASOCIADOS
PROGRAMAS DE AUDITORÍA DE SISTEMAS
SISTEMA DE ADMINISTRACION FINANCIERA INTEGRADA MUNICIPAL SAFIMU II
MODULO DE TESORERIA
ORIGEN DE DATOS
EJERCICIO A DICTAMINARSE: AÑO 20X1

OBJETIVO: Evaluar la suficiencia y el cumplimiento de los procedimientos establecidos por la administracion para la preparación, autorización, recolección y manejo de errores en los documentos fuente.

No.	Descripcion	Hecho por	Revisado por	P/T	Ref. DS
ACN CONTROL DE ORIGEN DE DATOS/AUTORIZACION AC1 PROCEDIMIENTOS DE PREPARACION DE DATOS					
1	Obtener un flujograma del ciclo de operaciones de la información para identificar los puntos más importantes en esta para una efectiva administración de datos.				11.1
2	Obtener políticas y procedimientos para la administración de los datos en caso existiese.				11.1
3	Identificar los puntos en los que la institución origina los datos y detalle cuales son las áreas de donde proviene la información ingresada al sistema.				11.1 1.6
4	Identificar el tipo de origen de datos ya sea documental, directo e hibrido.				11.1
5	Una vez identificado el tipo de origen realizar las siguientes pruebas: - Identificar qué tipo de documentos son utilizados para alimentar al sistema - Revisar que tipo de procedimientos son utilizados para la preparación de datos				11.1
6	Verificar si los documentos para alimentar al sistemas cumplen con los siguientes atributos: 1) Si son elaborados de acuerdo a una secuencia de ingreso. 2) Si presentan títulos y encabezados descriptivos. 3) Con espacios suficientes para correcciones y firmas de responsables.				11.1
7	Verifique que los formularios de captura de datos en el sistema, estén elaborados de acuerdo a la secuencia que tiene el formato del documento fuente, de donde se extrae la información que será introducida a este. (Realizar capturas de pantalla de los formularios).				11.1
8	Indagar si los errores e irregularidades en la preparación de datos son detectados, reportados y corregidos.				11.1

CANALES AVALOS Y ASOCIADOS
PROGRAMAS DE AUDITORÍA DE SISTEMAS
SISTEMA DE ADMINISTRACION FINANCIERA INTEGRADA MUNICIPAL SAFIMU II
MODULO DE TESORERIA
ORIGEN DE DATOS
EJERCICIO A DICTAMINARSE: AÑO 20X1

No.	Descripcion	Hecho por	Revisado por	P/T	Ref. DS
AC2 PROCEDIMIENTOS DE AUTORIZACION DE DOCUMENTOS FUENTES					
9	Verificar si existe un manual de funciones donde estén segregadas la asignación de actividades y que sea del conocimiento de los interesados.				7.1
10	Comprobar que en los documentos fuente se especifique: 1) La persona que elaboro el documento. 2) La persona que autorizo la operación.				11.1
11	Verificar que los documentos fuente se preparan adecuadamente cumpliendo con las necesidades de información de los usuarios				11.1
12	Indagar si los documentos son revisados antes de ser autorizados y verificar si ambas funciones son realizadas por la misma persona.				11.1
13	Verificar que exista un responsable asignado, para la autorización de los documentos fuente.				11.1
AC3 RECOLECCION DE DATOS DE DOCUMENTOS FUENTE					
No.	**Descripcion**	**Hecho por**	**Revisado por**	**P/T**	Ref. DS
14	Verificar que los documentos fuente autorizados, son completos y precisos que no existen omisiones en el llenado del formulario.				11.1
15	Verificar que para cada documento fuente, existe una justificación del porque la necesidad de dicha operación.				11.1
16	Determinar si los documentos fuente son transmitidos de manera oportuna para su captura en el sistema.				11.1
17	Verificar si existe una persona responsable de monitorear que los documentos fuente en el momento adecuado.				11.1
AC4 MANEJO DE ERRORES EN DOCUMENTOS FUENTE.					
18	Indagar como se detectan los errores u omisiones en los documentos fuente.				11.1 11.6
19	Verificar si existe un responsable de evaluar los errores en los documentos fuente.				11.1 11.6
20	Verificar que los errores u omisiones son corregidos en el momento oportuno.				11.1 11.6
21	Determinar si existen procedimientos establecidos formalmente para las correcciones al sistema.				11.1 11.6
22	Determinar si los errores u omisiones son reportados y discutidos con la autoridad responsable.				11.1 11.6
AC5 RETENCION DE DOCUMENTOS FUENTE					
23	Indagar si existe autorización restringida para la reproducción de documentos fuente.				11.1 11.2
24	Determinar si los procedimientos para el control en el acceso de los documentos fuente asegura la integridad de los datos.				11.1
25	Identifique las condiciones reportables a la administración o de la entidad, detalle con una cedula de hallazgos				

CANALES AVALOS Y ASOCIADOS
PROGRAMAS DE AUDITORÍA DE SISTEMAS
SISTEMA DE ADMINISTRACION FINANCIERA INTEGRADA MUNICIPAL SAFIMU II
MODULO DE TESORERIA
ENTRADA DE DATOS
EJERCICIO A DICTAMINARSE: AÑO 20X1

OBJETIVO: Evaluar el proceso de ingreso de datos en el sistema para determinar la suficiencia y el cumplimiento de los procedimientos de validación existentes en las pantallas de captura.

No.	Descripcion	Hecho por	Revisado por	P/T	Ref. DS
ACN CONTROL DE ENTRADA DE DATOS AC6 PROCEDIMIENTOS DE AUTORIZACION DE CAPTURA DE DATOS					
1	Obtener una lista identificando los campos más importantes en donde se realizan la entrada de datos para cada uno de los formularios de entrada.				11.1
2	Una vez obtenida la lista de campos realizar las siguientes validaciones a dichos campos: a) Identificar los tipos de campos y clasificarlos ya sea como campos de texto, numéricos, de moneda, alfanumericos. b) Verificar que la captura de datos al sistema sea procesada exclusivamente por el personal autorizado.				11.1 5.3
3	Indagar si el sistema genera una bitácora que permita determinar: a) Quien realizo la captura de datos b) En qué fecha lo realizo (Cuando) c) El numero de documento fuente que lo ampara d) Movimientos de captura anulados e) Movimientos de captura modificados f) Equipo utilizado para el acceso				5.4 11.1 11.6
4	Verificar que los campos de los formularios para el registro de depósitos bancarios sean Parametrizados				11.1 5.3
5	Verificar si existe un administrador del sistema que establece y asigna el ID y el password a los usuarios.				5.3 5.4

CANALES AVALOS Y ASOCIADOS
PROGRAMAS DE AUDITORÍA DE SISTEMAS
SISTEMA DE ADMINISTRACION FINANCIERA INTEGRADA MUNICIPAL SAFIMU II
MODULO DE TESORERIA
ENTRADA DE DATOS
EJERCICIO A DICTAMINARSE: AÑO 20X1

No.	Descripcion	Hecho por	Revisado por	P/T	Ref. DS
7	Verificar si se cuenta con reportes de violaciones a la seguridad y procedimientos formales de solución de problemas.				5.6 11.6 10.1 10.2
8	Verificar que los perfiles de usuarios esten adecuados a los cargos y responsabilidades del personal.				5.3 5.4
9	Verificar que para ingresar al sistema este requiere el ID de usuario y el password para el acceso.				5.3 5.4
10	Verificar que para ingresar al modulo de Tesorería el sistema requiere nuevamente el ID de usuario y password.				5.3 5.4
11	Corroborar ingresando un ID y password de usuario con perfil de consulta e intentar ingresar y modificar datos.				5.3 5.4
AC7 VERIFICACIONES DE PRECISION, INTEGRIDAD Y AUTORIZACION					
12	Obtener los parámetros establecidos en la realización de los campos para cada uno de estos y conforme a estos parámetros realizar las siguientes validaciones: ▪ Probar que en los campos numéricos no se puedan ingresar valores negativos donde no corresp				11.1 5.2 5.7
13	Verifique que no exista la necesidad de un reproceso en los procedimientos y cálculos que realiza el sistema, es decir que los usuarios no realicen procedimientos extras para el ingreso de datos al sistema.				11.1
14	Investigue y Compruebe si el sistema permite dejar campos vacíos, siendo dichos campos de gran importancia para controles o cálculos en esa misma pantalla o en otras de esa aplicación.				11.1

PROGRAMAS DE AUDITORÍA DE SISTEMAS
SISTEMA DE ADMINISTRACION FINANCIERA INTEGRADA MUNICIPAL SAFIMU II
MODULO DE TESORERIA
ENTRADA DE DATOS
EJERCICIO A DICTAMINARSE: AÑO 20X1

No.	Descripcion	Hecho por	Revisado por	P/T	Ref. DS
15	Revise las máscaras de entrada para códigos o números que tienen un formato establecido desde el origen de su emisión.				11.1
16	Indagar sobre la existencia de controles que permitan verificar la: a) La precisión b) Integridad c) Autorización				5.2 11.6
17	Determinar si los controles aplicados a los datos son ejecutados por el personal distinto al que lo genera y procesa.				5.2
18	Verificar el cumplimiento del proceso de autorización de las órdenes de compra.				11.1
19	Determinar que tan próximos al punto de origen son editados y actualizados los datos.				11.1
20	Verificar que los datos sean editados en el periodo que les corresponde, y no en fechas posteriores.				11.1
21	Verificar que los datos hayan sido procesados de acuerdo al documento fuente.				11.1
22	Indagar si existen verificaciones de datos, posteriores al ingreso de estos al sistema.				11.1
	AC8 MANEJO DE ERRORES EN LA ENTRADA DE DATOS				
23	Verificar si existen módulos que lleven a cabo revisiones de precisión, suficiencia y autorización de captura.				5.2
24	Verificar la existencia de funciones que lleven a cabo rutinas de corrección de errores en la entrada de datos.				5.9
25	Verificar que existen procedimientos que permiten corregir datos ingresados de manera incorrecta.				5.9
26	Indagar si existe una persona responsable de autorizar correcciones al sistema o si estas se hacen sin previa autorización.				5.3
27	Indagar si las correcciones son realizadas en el momento oportuno.				5.2
28	Verificar la existencia de controles de los depósitos bancarios anulados y la forma en que se documentan las circunstancias de su anulación.				11.2
29	Identifique las condiciones reportables a la administración o de la entidad, detalle con una cedula los hallazgos.				

CANALES AVALOS Y ASOCIADOS
PROGRAMAS DE AUDITORÍA DE SISTEMAS
SISTEMA DE ADMINISTRACION FINANCIERA INTEGRADA MUNICIPAL SAFIMU II
MODULO DE TESORERIA
PROCESAMIENTO DE DATOS
EJERCICIO A DICTAMINARSE: AÑO 20X1

OBJETIVOS: Evaluar los procesos de carga, cierre y actualizaciones de datos para determinar si se le da seguimiento al procedimiento establecido para ello.

No.	Descripcion	Hecho por	Revisado por	P/T	Ref. DS
ACN CONTROLES EN EL PROCESAMIENTO DE DATOS AC9 INTEGRIDAD EN EL PROCESAMIENTO DE DATOS					
1	Compruebe y Verifique que los campos del sistema sean paramétrizados y estos incluyan valores útiles para sus cálculos, y que no puedan ser modificados manualmente por cualquier usuario.				11.6 5.7
2	Compruebe y Verifique que los cálculos que automáticamente realiza el sistema, sean los correctos y ágiles a) Retenciones de Renta b) Retenciones de ISSS y AFP's				11.1 5.7
3	Verifique y Compruebe que los cálculos que automáticamente realiza en el sistema, estén de acuerdo a parámetros ya establecidos por el sistema.				11.6 5.2
4	Verifique y Compruebe que los campos paramétrizados, que incluyan valores útiles para cálculos, estén actualizados y de acuerdo a leyes o políticas vigentes según las leyes actuales por el gobierno.				11.1
5	Verificar que los datos sean procesados completos, sin modificaciones u omisiones.				11.6 5.7
6	Verificar que los datos sean actualizados oportunamente.				11.1 5.2
7	Determinar si existen procedimientos que garanticen las actualizaciones de los archivos maestros y verificar que esten actualizados.				5.2
8	Verificar que para la selección del tipo de cheque, existe un mecanismo dentro del sistema que verifique que la selección sea correcta de acuerdo al tipo de operación a cancelar.				11.6
9	Verificar la existencia de controles de los justificantes de pago anulados.				5.2
AC10 VALIDACION Y EDICION DEL PROCESAMIENTO DE DATOS					
10	Determinar si existe mas de un código asignado a un mismo proveedor.				5.7
11	Verificando si existen números de factura asignados con proveedores que no se encuentran registrados.				11.1
12	Verifique si el sistema es capaz de detectar datos o valores duplicados.				11.6

CANALES AVALOS Y ASOCIADOS
PROGRAMAS DE AUDITORÍA DE SISTEMAS
SISTEMA DE ADMINISTRACION FINANCIERA INTEGRADA MUNICIPAL SAFIMU II
MODULO DE TESORERIA
PROCESAMIENTO DE DATOS
EJERCICIO A DICTAMINARSE: AÑO 20X1

No.	Descripcion	Hecho por	Revisado por	P/T	Ref. DS
14	Verificar que todo justificante de pago posea un acta y un acuerdo vinculado a la operación del gasto.				5.2 5.7
15	Verificar que el acuerdo de Egreso sea procesado antes que la factura.				5.2
16	Verificar que para la aprobación de los justificantes de pago, estos cuenten obligatoriamente con: • Visto Bueno • DESE				11.1
17	Verificar que toda factura, tenga su respectiva orden de compra.				11.1
18	Verificar que no existan pagos que sobrepasen el monto original de orden de compra.				11.1
19	Verificar si el sistema posee mecanismos de control que permitan validar el estado de los cheques ya sea como emitidos u aprobados.				5.2
20	Indagar si existe una persona responsable de la aprobación de cheques.				5.5
21	Indagar cuál es el proceso para la aprobación de las retenciones.				5.3
22	Realizar una lista de los procesos dentro del menú de cuentas bancarias que permite realizar el sistema.				5.4
23	Indagar si los cálculos de tasa o porcentajes son realizados por el mismo sistema o fuera de este.				11.1
AC11 MANEJO DE ERRORES EN EL PROCESAMIENTO DE DATOS					
24	Investigar que tipo de problemas son más usuales al utilizar el sistema.				10.1
25	Verificar si existen políticas y procedimientos encaminados a la administración de problemas.				10.1
26	Verificar si los planes de contingencia utilizados para la administración de problemas, están clasificados por categoría, impacto, urgencia.				10.1
27	Investigar si existe personal encargado para solucionar los problemas del sistema.				10.1
28	Verificar la existencia de métodos o rutinas utilizados para prevenir, detectar y corregir errores ya sea por medios manuales o programados.				11.6
29	Verificar si existe una bitácora de registros que permita rastrear o detectar, analizar y determinar la causa raíz de todos los problemas.				10.2

CANALES AVALOS Y ASOCIADOS
PROGRAMAS DE AUDITORÍA DE SISTEMAS
SISTEMA DE ADMINISTRACION FINANCIERA INTEGRADA MUNICIPAL SAFIMU II
MODULO DE TESORERIA
PROCESAMIENTO DE DATOS
EJERCICIO A DICTAMINARSE: AÑO 20X1

No.	Descripcion	Hecho por	Revisado por	P/T	Ref. DS
30	Indagar si las transacciones erróneas son identificadas: a) Antes de ser procesadas b) Después de ser procesadas				10.1 11.6
31	Verificar si los errores se corrigen en el momento en que se detectan sin previa autorización o si estos necesitan ser autorizados por la persona responsable.				10.2
32	Indagar si son documentadas las correcciones realizadas al sistema por errores en el procesamiento.				11.2
33	Verificar la existencia de controles de los justificantes de pago anulados.				11.1
34	Determinar si se lleva control de los cheques anulados y las causas de dichas anulaciones.				11.1
35	Determinar si la corrección de los errores interrumpen las otras transacciones, mientras es solucionado el error.				10.2
36	Investigar el número y la frecuencia de interrupciones del negocio debido a problemas operativos del sistema.				10.2
37	Identificar el numero de problemas abiertos, nuevos o cerrados por severidad del problema.				10.2
38	Investigar si se emiten reportes sobre los problemas sobresalientes que tienen un alto impacto en las operaciones del sistema.				10.2
39	Investigar si a los reportes de incidentes emitidos por la gerencia informatica se les da un seguimiento adecuado, para solucionarlos y prevenir que se repitan.				10.2
40	Identifique las condiciones reportables a la administración de la sociedad, detalle con una cedula los hallazgos encontrados.				

CANALES AVALOS Y ASOCIADOS
PROGRAMAS DE AUDITORÍA DE SISTEMAS
SISTEMA DE ADMINISTRACION FINANCIERA INTEGRADA MUNICIPAL SAFIMU II
MODULO DE TESORERIA
SALIDA DE DATOS
EJERCICIO A DICTAMINARSE: AÑO 20X1

OBJETIVO: Evaluar los procedimientos para la administración y distribución de la salida de datos, y la forma en que la información es proporcionada por el sistema.

No.	Descripcion	Hecho por	Revisado por	P/T	Ref. DS
	CONTROLES DE SALIDA DE DATOS **AC12 MANEJO Y RETENCION DE SALIDAS**				
1	Verificar que el acceso a la salida de información sea física y lógicamente a personal autorizado.				11.1 5.4 5.5
2	Identificar si existe una adecuada asignación de perfiles de usuarios para la eliminación y salida de datos.				11.1 11.4 5.4
3	Verificar si se lleva a cabo una revisión continua de necesidades de salida.				11.1 1.6
4	Investigue quiénes están autorizados para imprimir reportes, y cuál es la forma o procedimientos que se siguen para la impresión.				11.1 5.3 5.4
5	Verificar si el sistema permitir imprimir únicamente los cheques que poseen el estado de aprobado.				11.1
6	Verificar si existen procedimientos de control para la opción de reimpresión de cheques.				11.6 11.1
7	Indagar si para la impresión de reportes, existen periodos específicos, como por ejemplo: A) Semanal B) Quincenal C) Mensual D) otros				11.1
8	Indagar si los reportes del sistema son distribuidos en base a criterios de necesidades de información.				11.1
9	Indagar si para la realización de consultas a los reportes, el sistema requiere de: a) Identificación de usuario b) Clave de acceso.				11.1 5.4
10	Verificar si existe una bitácora que permita identificar: a) Fecha de consulta b) Modulo consultado c) Usuario que realizo la consulta d) Equipo que fue utilizado para la consulta e) Reportes impresos durante la consulta				11.6 11.1 5.4 5.5
11	Indagar si existen reportes que están restringidos, para el uso exclusivo de usuarios específicos.				11.6 5.4 5.6

CANALES AVALOS Y ASOCIADOS
PROGRAMAS DE AUDITORÍA DE SISTEMAS
SISTEMA DE ADMINISTRACION FINANCIERA INTEGRADA MUNICIPAL SAFIMU II
MODULO DE TESORERIA
SALIDA DE DATOS
EJERCICIO A DICTAMINARSE: AÑO 20X1

No.	Descripcion	Hecho por	Revisado por	P/T	Ref. DS
12	Verificar que estos reportes no puedan ser accesados por otros usuarios, distintos a los que son los autorizados.				11.1 11.6 5.4 5.6
	AC13 DISTRIBUCION DE SALIDAS				
13	Indagar si están definidos los procedimientos para la distribución de reportes.				11.1 5.7
14	Investigue y Determine la forma en que los reportes generados por el sistema son distribuidos a los usuarios.				11.1 5.7
15	Indagar si para la distribución de reportes, a los usuarios de la información estos estampan firma de recibido y colocan la fecha en que le son entregados los reportes.				11.6 5.7 5.5
16	Verificar si existe una persona responsable de dar seguimiento a la correcta distribución de los reportes del sistema.				11.1 1.4 5.6 5.9
17	Determinar si el sistema posee una bitácora que permitan determinar el momento en el cual los pagos de los justificantes quedan formalizados con la entrega de los cheques.				11.6 5.9 8.3 5.5
18	Investigar a través de un listado de reportes generados e impresos en el sistema, si estos se distribuyen correctamente.				11.6 5.9 8.3
	AC14 CUADRE Y CONCILIACION DE SALIDAS				
19	Verificar que la información ingresada de los documentos fuente, y procesados en el sistema, sea la misma información en los reportes de salida.				11.1 11.6 5.11
20	Indagar si las conciliaciones de las salidas, permiten detectar errores, alteraciones y omisiones.				11.6
21	Indagar que procedimientos se realizan, cuando al conciliar las salidas se detectan errores, alteraciones u omisiones				11.6
22	Indagar si las conciliaciones y los resultados de estas son documentados y archivados.				11.2
23	Solicite el listado de distribución de reportes generados por el sistema.				11.1
24	Verifique que los reportes generados y guardados en archivos no puedan ser editados por el usuario o por otra persona.				11.6 5.3
	AC15 REVISION DE SALIDAS Y MANEJO DE ERRORES				
25	Corroborar si la precisión de los reportes de salida es revisada y los errores contenidos en la salida son revisados por personal capacitado.				11.6 10.2 5.5

CANALES AVALOS Y ASOCIADOS
PROGRAMAS DE AUDITORIA DE SISTEMAS
SISTEMA DE ADMINISTRACION FINANCIERA INTEGRADA MUNICIPAL SAFIMU II
MODULO DE TESORERIA
SALIDA DE DATOS
EJERCICIO A DICTAMINARSE: ANO 20X1

No.	Descripcion	Hecho por	Revisado por	P/T	Ref. DS
26	Determine si la información proporcionada por el sistema es suficiente para el usuario final o se ve en la necesidad de reprocesarla fuera del sistema.				11.1 1.2
27	Verifique que los reportes que se generan estén bien identificados con nombre del programa que lo genera, títulos, fechas, período cubierto, número de página.				11,1
28	Indagar que procedimientos están establecidos para detectar los errores en los reportes de salida.				11.6 10.1
29	Verificar que dichos procedimientos son adecuados para minimizar los errores.				10.4 11.6
30	Determinar si los usuarios llevan a cabo los procedimientos de detección de errores.				10.2 11.6
31	Indagar sobre los procedimientos establecidos para el manejo de errores.				11.6 10.1
32	Indagar si existe un responsable de autorizar las correcciones por errores u omisiones al sistema.				11.6 10.2 5.9
33	Verificar la incidencia en la determinación de errores en la información procesada.				10.2 8.3 5.9
34	Verificar que los errores detectados se corrijan en el momento de su reconocimiento con la autorización correspondiente.				10.2 10.3 5.9
AC16 PROVISION DE SEGURIDAD PARA REPORTES DE SALIDA					
35	Indagar la existencia de procedimientos que garantizan la seguridad y la privacidad para: a) reportes impresos por distribuir b) los reportes ya entregados a los usuarios				11.6 5.6
36	Indagar si existen asignacion de responsabilidades para los usuarios, con relación a la revelación de la información que les es proporcionada a través de los reportes .				11,1
37	Verificar si los reportes que se imprimen y no son utilizados por alguna razón, son destruidos.				11,4
38	Verificar que la información marcada como eliminada cambia de tal forma que no se pueda				11.4
39	Determine si existe algún procedimiento de destrucción o almacenamiento adecuado de los				11.2 11.4

PROGRAMAS DE AUDITORÍA DE SISTEMAS
SISTEMA DE ADMINISTRACION FINANCIERA INTEGRADA MUNICIPAL SAFIMU II
MODULO DE TESORERIA
SALIDA DE DATOS
EJERCICIO A DICTAMINARSE: AÑO 20X1

No.	Descripcion	Hecho por	Revisado por	P/T	Ref. DS
40	Realizar las siguientes validaciones por medio de capturas de pantallas y evaluar el nivel de riesgo de manipulación de datos.				11.1 5.6
41	Verificar la existencia de un plan de recuperacion de desastre/contingencia en la funcion en los servicios del modulo de tesorería .				4.2
42	Indagar si el plan de continuidad posee criterios de prioridad de informacion para la recuperación y reanudación de actividades.				4.3
43	Verificar si para el plan de continuidad existen periodos de revisión definidos.				4.4
44	Indagar si el plan de continuidad es puesto a prueba de forma regular, para determinar que este permite la recuperacion efectiva de la informacion del modulo.				4.5
45	Verificar que el personal es capacitado para la ejecución del plan de continuidad.				4.6
46	Indagar si existe una estrategia de distribución del plan de continuidad.				4.7
47	Verificar que el plan de continuidad comprenda acciones alternativas de procedimientos durante el periodo de recuperación y reanudacíon de los servicios.				4.8
48	Indagar el lugar donde es almacenado el plan de continuidad y los medios de respaldo utilizados para ello.				4.9
49	Verificar si los planes de continuidad estan actualizados.				4.4
50	Identifique las condiciones reportables a la administración de la sociedad, detalle con una cedula los hallazgos encontrados.				

CANALES AVALOS Y ASOCIADOS
PROGRAMAS DE AUDITORIA DE SISTEMAS
SISTEMA DE ADMINISTRACION FINANCIERA INTEGRADA MUNICIPAL SAFIMU II
MODULO DE TESORERIA
LIMITES DE DATOS
EJERCICIO A DICTAMINARSE: AÑO 20X1

OBJETIVOS: Evaluar los procedimientos de verificación de los documentos fuente que se generan fuera de la entidad y los métodos de protección de la información sensitiva.

No.	Descripcion	Hecho por	Revisado por	P/T	Ref. DS
	AC17 CONTROLES DE LIMITE				
1	Indagar si existen procedimientos para verificar la autenticidad e integridad de la información generada fuera de la entidad.				5.1 11.6
2	Indagar si para estos procedimientos existe una persona responsable de su ejecución.				5.2
3	Determinar si dichas verificaciones se realizan: a) Antes de introducir la datos b) Después de procesar la datos c) Después de la salida de información.				11.6
	AC18 PROTECCION DE INFORMACION SENSITIVA DURANTE SU TRANSMISION O TRANSPORTE.				
4	Verificar que existan procedimientos especiales para el tratamiento de la información sensitiva durante todo el ciclo de información.				11.6
5	Verificar que el traslado de la información sensitiva se realiza únicamente a través del sistema o si existen otros medios, analizar su confiabilidad y confidencialidad.				5.11
6	Determinar si para la información sensitiva existen procedimientos que permitan que esta sea modificada.				5.11
7	Indagar si existe una persona responsable asignada para la autorización de modificaciones de la información sensitiva.				5.11
8	Indagar si las modificaciones requieren autorización de la persona responsable y si estas son documentadas.				5.4
9	Verificar que estén definidos los usuarios que tienen acceso exclusivo a la información sensitiva.				5.11
10	Indagar si para el acceso a la información sensitiva se requiere de claves de acceso.				5.4
11	Identifique las condiciones reportables a la administración de la sociedad, detalle con una cedula los hallazgos encontrados.				

ANEXO 3

LISTADO DE ALCALDÍAS

Listado de Alcaldías Municipales que utilizan el Sistema de Administración Financiera Integrada Municipal SAFIMU II son las siguientes:

- Alcaldía Municipal de Antiguo Cuscatlán
- Alcaldía Municipal de Juayua
- Alcaldía Municipal de San Martin
- Alcaldía Municipal de San Antonio del Monte
- Alcaldía Municipal de Acajutla
- Alcaldía Municipal de Ciudad Arce

ANEXO 4

ENCUESTA

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURIA PÚBLICA

OBJETIVO

Conocer la opinión de administradores y usuarios del SAFIMU II acerca del desempeño, la aplicación en las municipalidades que lo utilizan.

INDICACIONES

Coloque una "X", según sea su respuesta, en cada una de las interrogantes presentadas.

Cargo: _____ Departamento _____

Fecha: _____

1. ¿Existe un departamento de informática establecido dentro de la institución?

   SI ☐ NO ☐

2. ¿Cuál es la formación académica del personal encargado del mantenimiento tanto de hardware como de software de la institución?

   Bachiller en Informática _____

   Técnico en mantenimiento de redes _____

   Licenciatura en Computación _____

   Ingeniería en Sistemas _____

   Otros _____

3. ¿Cuál es el personal o área encargada de evaluar el desempeño del departamento de informática?

   Gerencia General _____

   Auditoria Interna _____

   Usuarios _____

   Jefe de Departamento (especifique) _____

4. ¿Existen políticas y procedimientos encaminados a mejorar la eficiencia y eficacia de los recursos informáticos de esta institución?

   SI ☐ NO ☐

5. Si su respuesta fue a la pregunta anterior fue afirmativa ¿Qué tipo de políticas y procedimientos son aplicados a los recursos informáticos?

   a) Controles sobre el acceso de usuarios al sistema
   b) Controles en la entrada, procesamiento y salida de datos.
   c) Controles para la seguridad del equipo de cómputo y mobiliario del área informática.
   d) Controles de seguridad lógica

6. ¿Cuál es el grado de confiabilidad de la información procesada en el sistema?

   Alta ( ) Media ( ) Baja ( )

7. Si en la pregunta anterior contesto media o baja, ¿cuales de las siguientes razones considera como causa de la deficiente confiabilidad de la información procesada?

   Capacitación del personal ( )
   Deficiencias en el procesamiento de la información ( )
   Capacitación en interpretación de resultados ( )
   Manipulación en la base datos ( )

8. ¿En cuales de las siguientes áreas considera que el sistema necesita mejorar?

   Controles de acceso al sistema ( )
   Perfiles de usuario ( )
   Interfaces amigables ( )
   Funcionamiento del sistema ( )

9. ¿Considera que los reportes que suministra el sistema son adecuados y suficientes para las necesidades de la institución y para la toma de decisiones?

SI ☐ NO ☐

10. ¿Cuáles de las siguientes características reúnen los reportes suministrados por el sistema?

La información generada es completa (no es necesario reprocesarla por otros medios para hacer uso de ellos) ( )
Los reportes que genera el sistema son adecuados
Los reportes que genera el sistema son suficientes ( )
Los reportes son entregados en el tiempo oportuno ( )
La información generada es razonable y confiable ( )
Los reportes generados son comprensibles para los usuarios

11. ¿Anteriormente, le han realizado auditoria al área informática de esta entidad?

SI ☐ NO ☐

12. ¿En base a cual de las siguientes normativas técnicas ha sido realizada la Auditoría de Sistemas?

COBIT (Objetivos de Control de tecnologías de información y afines) ( )
ISO 17799 (Gestión de la Seguridad de la Información) ( )
NIA'S (Normas Internacionales de Auditoría) ( )

13. ¿Cuál es la formación académica de el personal que realizo la auditoría al departamento de informática?

Bachiller Técnico (opción contador)
Licenciatura en Contaduría Pública
Ingenieros en Sistemas
Otros

14. Si su respuesta en la pregunta once fue negativa ¿Considera necesaria una auditoria al área o departamento de informática de esta entidad?

SI ☐ NO ☐

15. ¿Considera que una auditoria de sistemas mejoraría la administración de los recursos informáticos y por ende los resultados de la información procesada por la institución?

SI ☐ NO ☐

16. ¿Considera necesario contar con un documento que proporcione una guía para poder realizar una Auditoría de Sistemas?

SI ☐ NO ☐

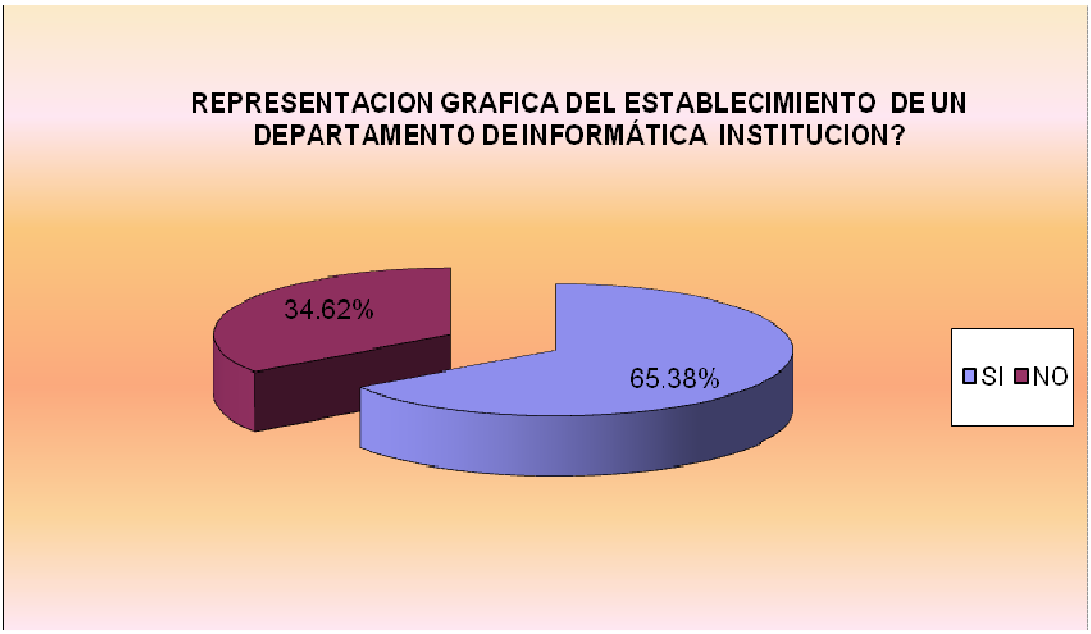
ANEXO 5
ANALISIS E INTERPRETACIÓN DE DATOS

1. ¿Existe un departamento de informática establecido en la institución?

Objetivo: Determinar si existe un departamento de informática formalmente establecido.

DISTRIBUCIÓN DE FRECUENCIAS

RESPUESTAS	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
SI	17	65.38%
NO	9	34.62%
TOTAL	26	100.00%



Análisis

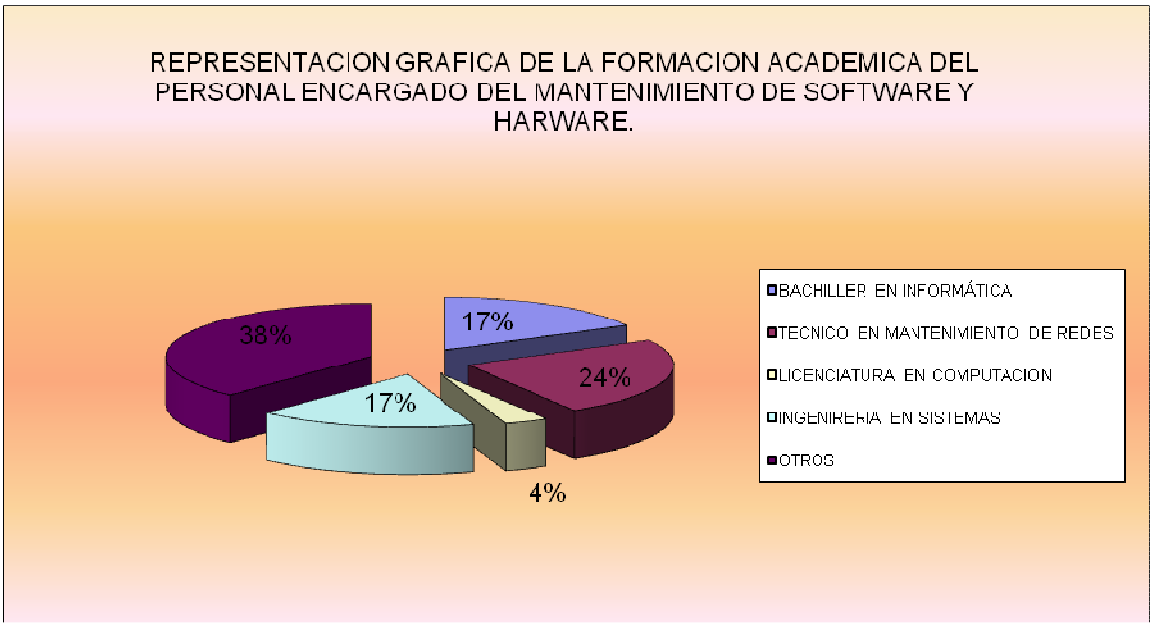
El 65.38 % afirmo que si existe departamento de informática en la institución y el resto de la población que representa el 34.62% afirma que no existe.

2. ¿Cuál es la formación académica del personal encargado del mantenimiento tanto de hardware como de software de la institución?

Objetivo: Determinar si las personas encargadas del mantenimiento tienen la formación académica apropiada.

DISTRIBUCIÓN DE FRECUENCIAS

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
BACHILLER EN INFORMÁTICA	5	17.24%
TECNICO EN MANTENIMIENTO DE REDES	7	24.14%
LICENCIATURA EN COMPUTACION	1	3.45%
INGENIRERIA EN SISTEMAS	5	17.24%
OTROS	11	37.93%
TOTAL	29	100.00%



Análisis

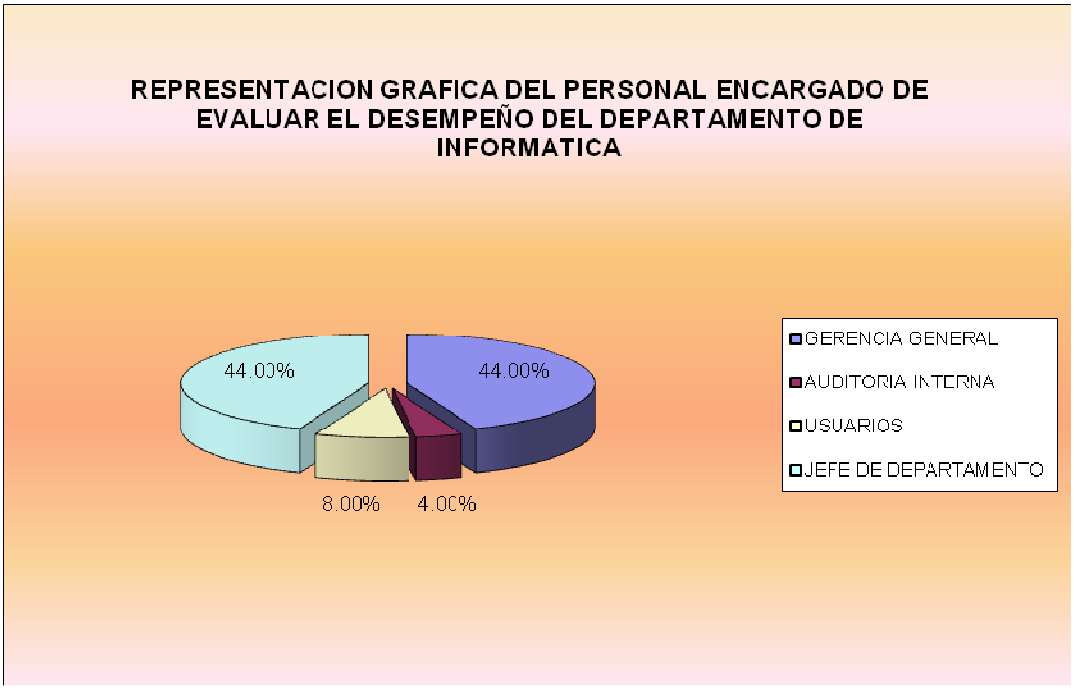
El 24.14 % de la población encuestada afirma que la formación académica es a nivel de técnico en mantenimiento de redes, mientras el 37.93% afirma que el nivel académico es otro, con lo cual se concluye que el grado académico del personal encargado del mantenimiento no es el más adecuado.

3. ¿Cuál es el personal o área encargada de evaluar el desempeño del departamento de informática?

Objetivo: Determinar si existe un responsable de evaluar el desempeño del departamento de informática.

DISTRIBUCIÓN DE FRECUENCIAS

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
GERENCIA GENERAL	11	44.00%
AUDITORIA INTERNA	1	4.00%
USUARIOS	2	8.00%
JEFE DE DEPARTAMENTO	11	44.00%
TOTAL	25	100.00%



Análisis

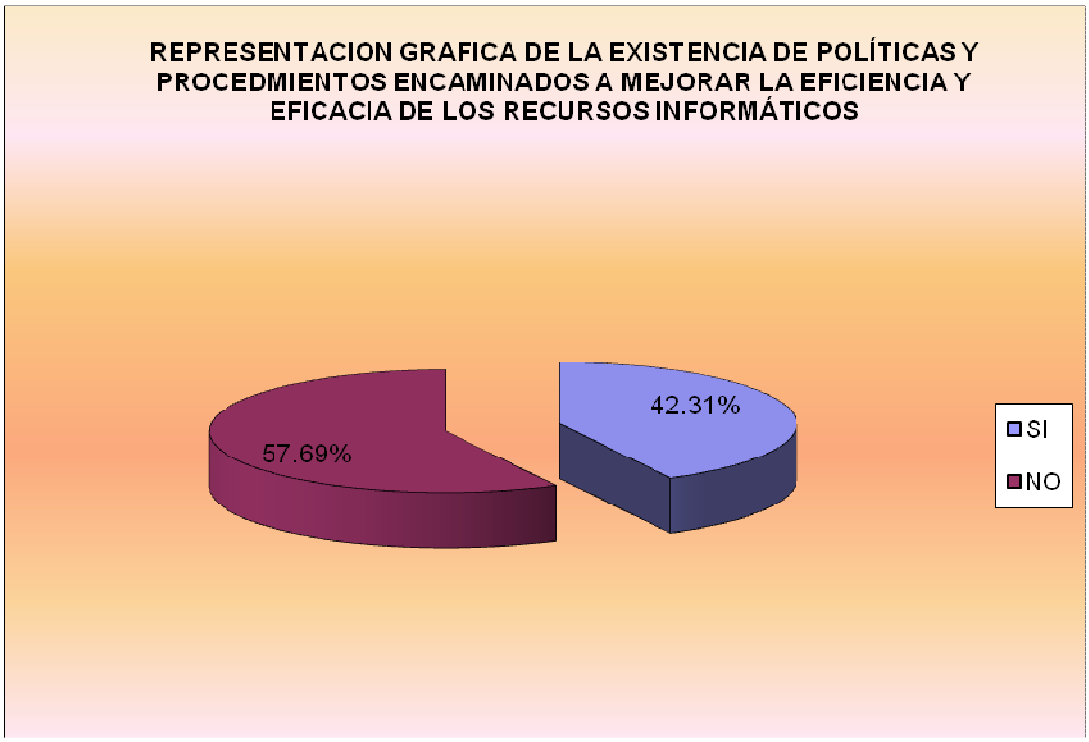
Mediante la encuesta realizada se determino que un 44% de la población afirma que la Gerencia General de la institución es la encargada de evaluar el desempeño del departamento de informática, de igual forma otro 44% afirma que el jefe del Departamento de Informática es el encargado de evaluar el mismo.

4. ¿Existen políticas y procedimientos encaminados a mejorar la eficiencia y eficacia de los recursos informáticos de esta institución?

Objetivo: Conocer si están establecidos en un documento formal las políticas y procedimientos a seguir para el uso eficiente y eficaz de los recursos informáticos.

DISTRIBUCIÓN DE FRECUENCIAS

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
SI	11	42.31%
NO	15	57.69%
TOTAL	26	100.00%



Análisis

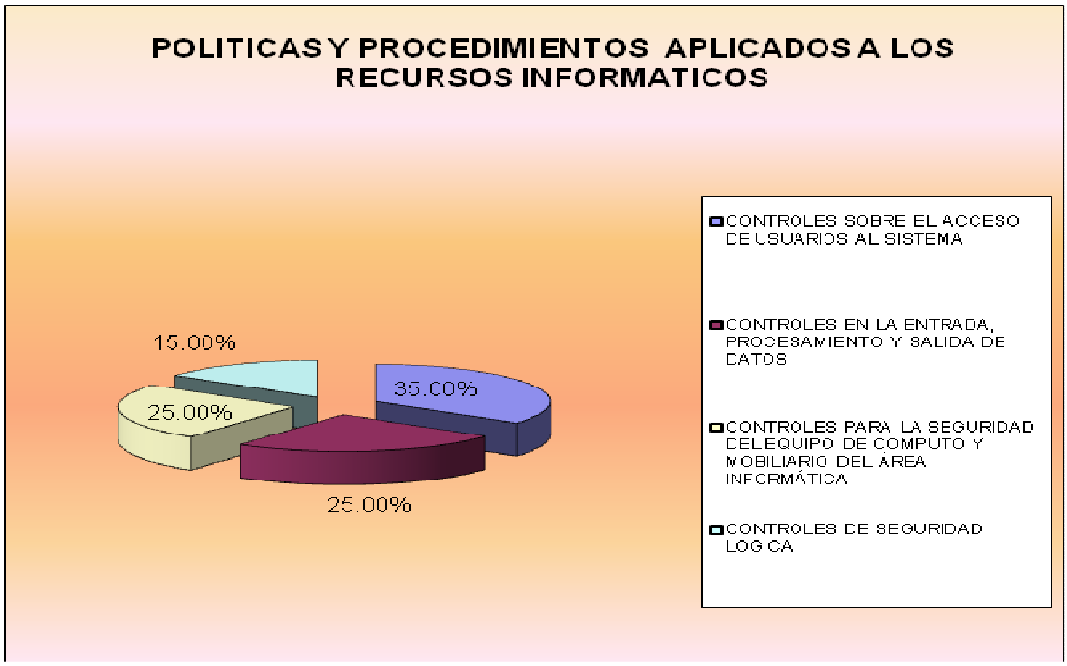
El 57.69% de la población encuestada considera que las funciones que realiza en su trabajo son las adecuadas según sus habilidades y capacidades, mientras el 42.31% afirma que no.

5. Si su respuesta a la pregunta anterior fue afirmativa ¿Qué tipo de políticas y procedimientos son aplicados a los recursos informáticos?

Objetivo: Comprobar que existen dichas políticas, y que estas realmente son dirigidas al área de informática.

DISTRIBUCIÓN DE FRECUENCIAS

RESPÙESTAS	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
CONTROLES SOBRE EL ACCESO DE USUARIOS AL SISTEMA	7	35.00%
CONTROLES EN LA ENTRADA, PROCESAMIENTO Y SALIDA DE DATOS	5	25.00%
CONTROLES PARA LA SEGURIDAD DEL EQUIPO DE COMPUTO Y MOBILIARIO DEL ÁREA INFORMÁTICA	5	25.00%
CONTROLES DE SEGURIDAD LOGICA	3	15.00%
TOTAL	20	100.00%



Análisis

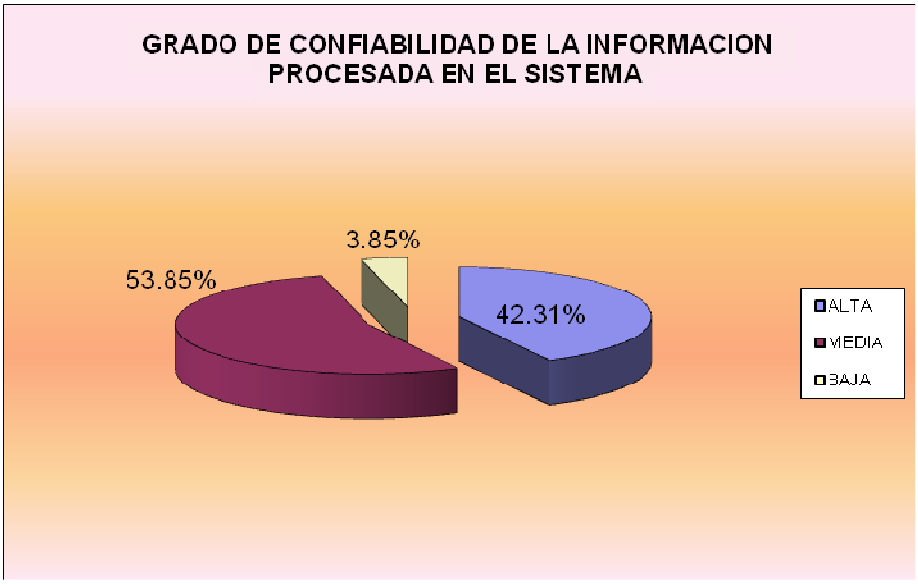
Las políticas y procedimientos aplicados al sistema SAFIMU son principalmente sobre el acceso de usuarios al sistema representado por un 35%, los controles en la entrada, procesamiento y salida de datos y los controles sobre la seguridad del equipo de computo y mobiliario de informática son aplicados en un 25% para cada tipo de control y un 15% de las políticas se aplican a la seguridad lógica del sistema.

6.¿Cuál es el grado de confiabilidad de la información procesada en el sistema?

Objetivo: Conocer el nivel de confianza que la información les proporciona a los usuarios de acuerdo a su criterio personal.

DISTRIBUCIÓN DE FRECUENCIAS

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
ALTA	11	42.31%
MEDIA	14	53.85%
BAJA	1	3.85%
TOTAL	26	100.00%



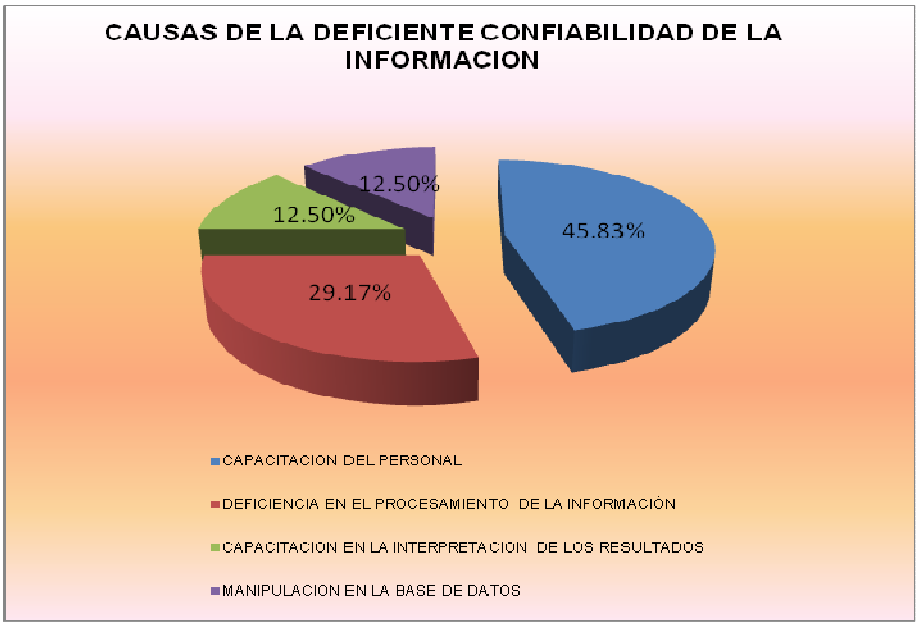
Análisis
El 53,85% de la población afirma que la confiabilidad de la información procesada es media, no obstante el 42,13% afirma que la confiabilidad es alta y el 3,85% afirma que es baja.

7. Si en la pregunta anterior contestó media o baja, ¿cuales de las siguientes razones considera como causa de la deficiente confiabilidad de la información procesada?

Objetivo: Conocer algunas de las razones por las cuales los usuarios consideran que la información no proporciona un alto nivel de confianza.

DISTRIBUCIÓN DE FRECUENCIAS

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
CAPACITACION DEL PERSONAL	11	45.83%
DEFICIENCIA EN EL PROCESAMIENTO DE LA INFORMACIÓN	7	29.17%
CAPACITACION EN LA INTERPRETACION DE LOS RESULTADOS	3	12.50%
MANIPULACION EN LA BASE DE DATOS	3	12.50%
TOTAL	24	100.00%



Análisis

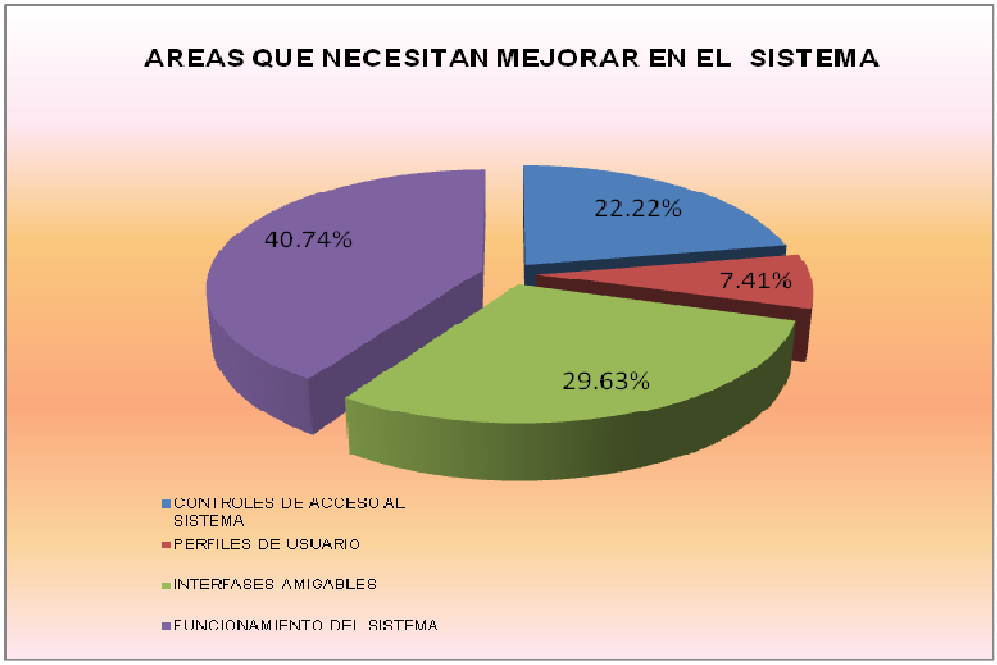
De acuerdo con los resultados el 45.83% de la población considera que una de las principales causas de la deficiente confiabilidad de la información procesada es la falta de capacitación del personal; un 29.17% considera que es la deficiencia en el procesamiento de la información.

8. ¿En cuáles de las siguientes áreas considera que el sistema necesita mejorar?

Objetivo: conocer las áreas en las que se consideran que es necesario aplicar mejoras al sistema.

DISTRIBUCIÓN DE FRECUENCIAS

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
CONTROLES DE ACCESO AL SISTEMA	6	22.22%
PERFILES DE USUARIO	2	7.41%
INTERFASES AMIGABLES	8	29.63%
FUNCIONAMIENTO DEL SISTEMA	11	40.74%
TOTAL	27	100.00%



Análisis

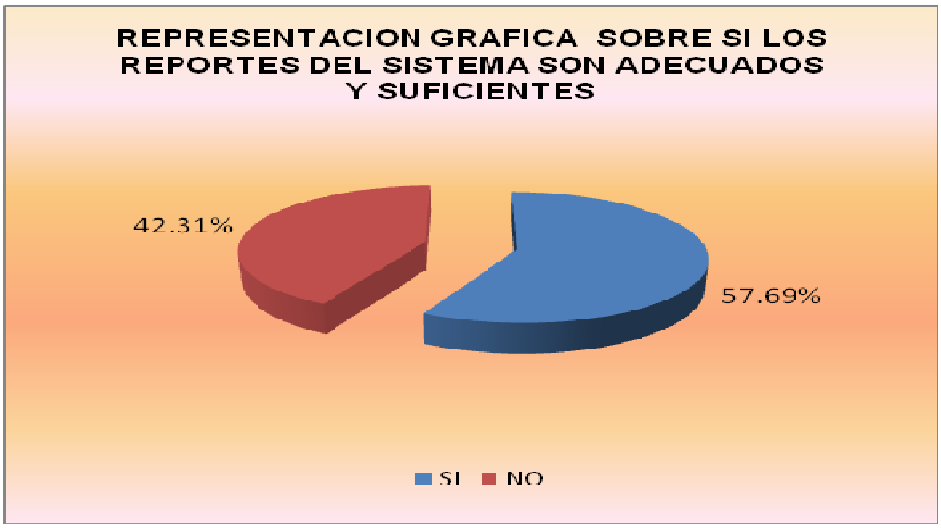
De acuerdo a los resultados obtenidos el área que es considerada como la principal, para realizar mejoras es el funcionamiento del sistema con un 40,74%; en segundo lugar se encuentran las interfaces amigables con un 29,63%: luego están los controles de acceso al sistema con un 22,22%, y por ultimo los perfiles de usuario con un 7,41%.

9. ¿Considera que los reportes que suministra el sistema son adecuados y suficientes para las necesidades de la institución y para la toma de decisiones?

Objetivo: Conocer si los reportes generados por el sistema son los adecuados y suficientes para los usuarios en la toma de decisiones.

DISTRIBUCIÓN DE FRECUENCIAS

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
SI	15	57.69%
NO	11	42.31%
TOTAL	26	100.00%



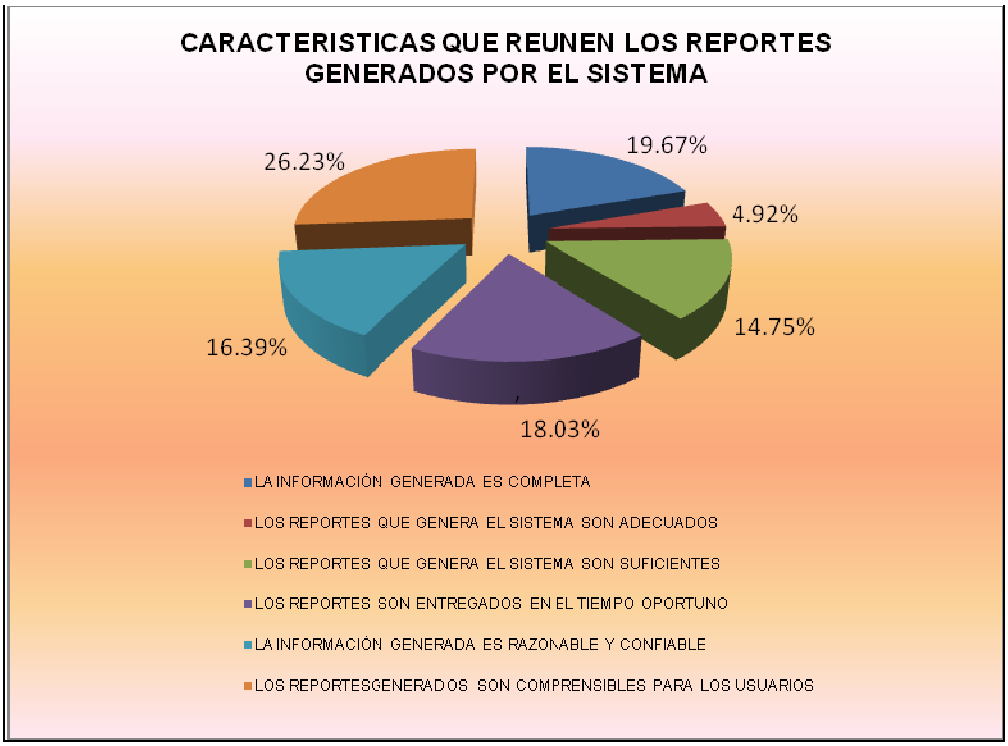
Análisis
De acuerdo a los resultados obtenidos el 57.69 % de la población considera que los reportes que suministra el sistema son adecuados y suficientes para las necesidades de la institución y para la toma de decisiones, mientras que el 42.31% restante considera que no cumplen con dichas características.

10. ¿Cuáles de las siguientes características reúnen los reportes suministrados por el sistema?

Objetivo: Establecer que características cualitativas cumplen los reportes suministrados por el sistema.

DISTRIBUCIÓN DE FRECUENCIAS

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
LA INFORMACIÓN GENERADA ES COMPLETA	12	19.67%
LOS REPORTES QUE GENERA EL SISTEMA SON ADECUADOS	3	4.92%
LOS REPORTES QUE GENERA EL SISTEMA SON SUFICIENTES	9	14.75%
LOS REPORTES SON ENTREGADOS EN EL TIEMPO OPORTUNO	11	18.03%
LA INFORMACIÓN GENERADA ES RAZONABLE Y CONFIABLE	10	16.39%
LOS REPORTESGENERADOS SON COMPRENSIBLES PARA LOS USUARIOS	16	26.23%
TOTAL	61	100.00%



Análisis

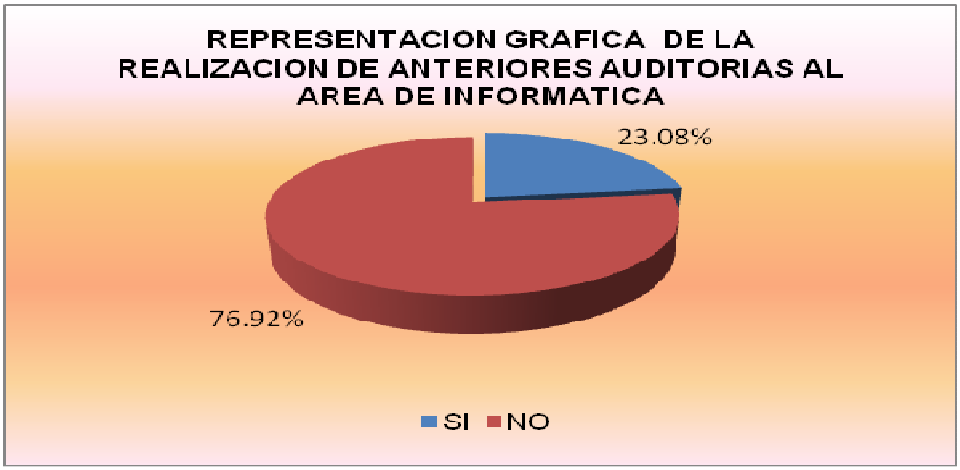
De acuerdo a los resultados obtenidos el 26.23% de la población en estudio considera que la principal característica que poseen los reportes que genera el sistema es la comprensibilidad para los usuarios; un 19.67% afirma que es información completa, es decir que no necesita ser reprocesada; otro 18.03% de los encuestados valora que es el tiempo oportuno en la entrega de los reportes; un 16.39% considera que es la razonabilidad y la confianza de la información generada; otro 14.75% opina que son los reportes en cuanto a que son los suficientes; y el resto que representa el 4.92% afirma que es lo adecuado de los reportes.

11. ¿Anteriormente, le han realizado auditoria al área informática de esta entidad?

Objetivo: Conocer si el área o departamento ha sido auditado alguna vez.

DISTRIBUCIÓN DE FRECUENCIAS

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
SI	6	23.08%
NO	20	76.92%
TOTAL	26	100.00%



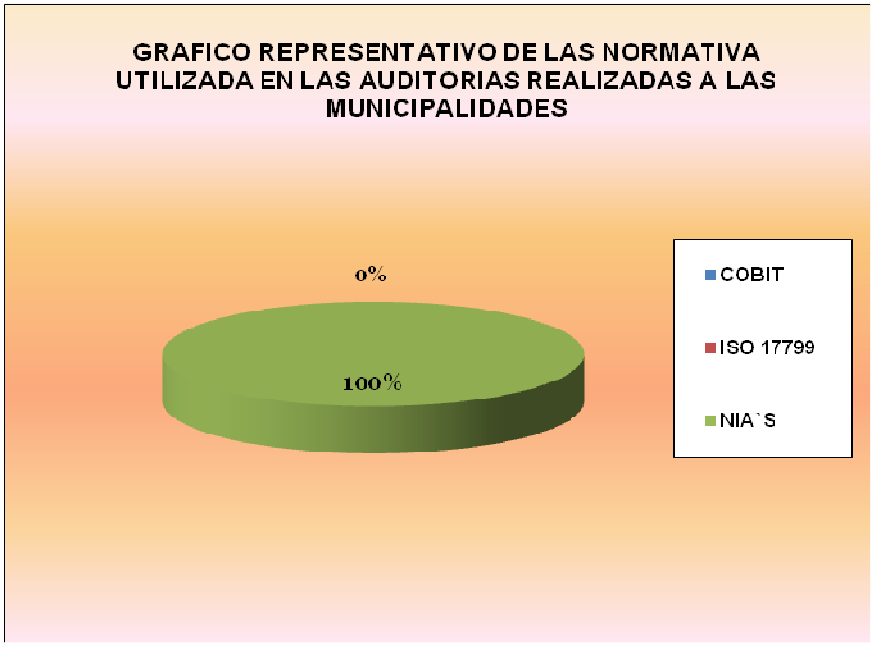
Análisis
De acuerdo a los resultados obtenidos el 76.92% de la población encuestada afirma que no les han realizado auditorias anteriormente al área de informática de la entidad, mientras que el 23.08 de los encuestados afirman que si les han realizado auditoria al área de informática.

12. ¿En base a cuál de las siguientes normativas técnicas ha sido realizada la Auditoría de Sistemas?

Objetivo: Conocer si se utilizó normativa técnica en la realización de la auditoria de sistemas y cual fue en particular.

DISTRIBUCIÓN DE FRECUENCIAS

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
COBIT	0	0.00%
ISO 17799	0	0.00%
NIA`S	**4**	100.00%
TOTAL	4	100.00%



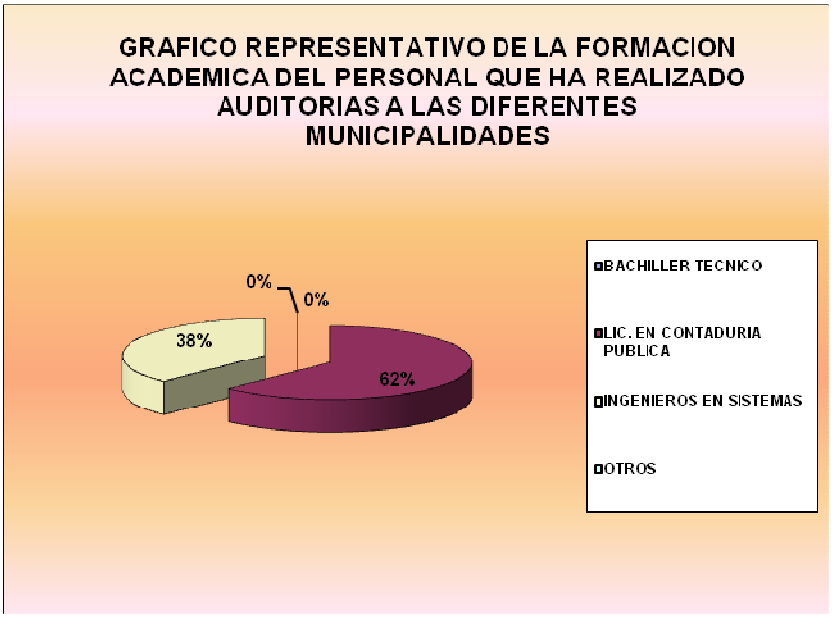
Análisis
El 100% de la población encuestada contesto que al momento de realizarles una auditoria esta se realizó en base a Normas Internacionales de Auditoría.

13. ¿Cuál es la formación académica del personal que realizó la auditoría al departamento de informática?

Objetivo: Determinar si el personal que realizó la auditoría tiene la formación académica apropiada para llevar a cabo dicha actividad.

DISTRIBUCIÓN DE FRECUENCIAS

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
BACHILLER TECNICO	0	0.00%
LIC. EN CONTADURIA PUBLICA	5	62.50%
INGENIEROS EN SISTEMAS	3	37.50%
OTROS	0	0.00%
TOTAL	8	100.00%



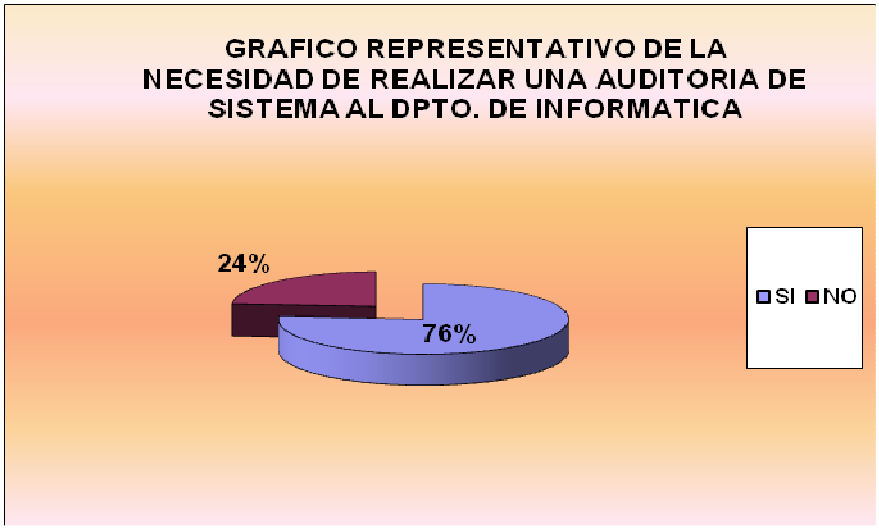
Análisis
El 62% de la población encuestada determino que el grado académico del personal que realizo la auditoria son Lic. En Contaduría Pública y el resto de la población con un 38% Ingenieros en Sistemas.

14. Si su respuesta en la pregunta once fue negativa ¿Considera necesaria una auditoria al área o departamento de informática de esta entidad?

Objetivo: Conocer si los usuarios consideran que es necesario realizar una auditoría al departamento de informática.

DISTRIBUCIÓN DE FRECUENCIAS

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
SI	16	76.19%
NO	5	23.81%
TOTAL	21	100.00%



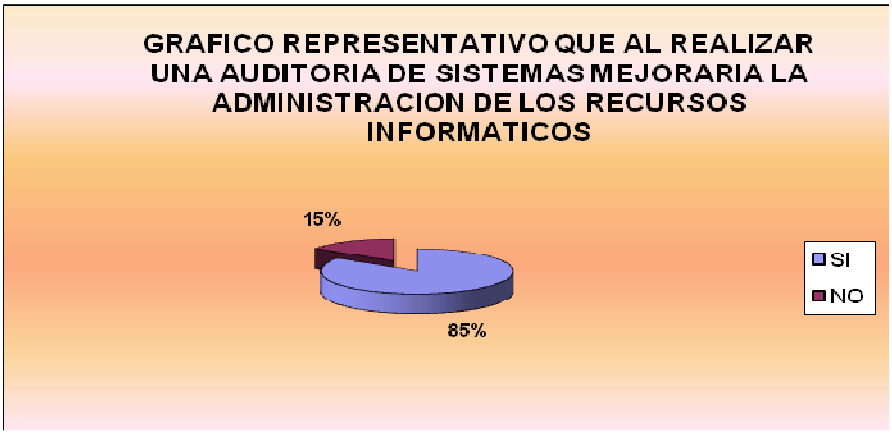
Análisis
De la población encuestada el 76% afirmó la necesidad de realizar una Auditoría de Sistemas al departamento de Informática y el resto con un 24% respondió de forma negativa.

15. ¿Considera que una auditoria de sistemas mejoraría la administración de los recursos informáticos y por ende los resultados de la información procesada por la institución?

Objetivo: Obtener el conocimiento sobre si los usuarios consideran que una auditoria mejoraría la administración de los recursos informáticos de la entidad.

DISTRIBUCIÓN DE FRECUENCIAS

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
SI	22	84.62%
NO	4	15.38%
TOTAL	26	100.00%



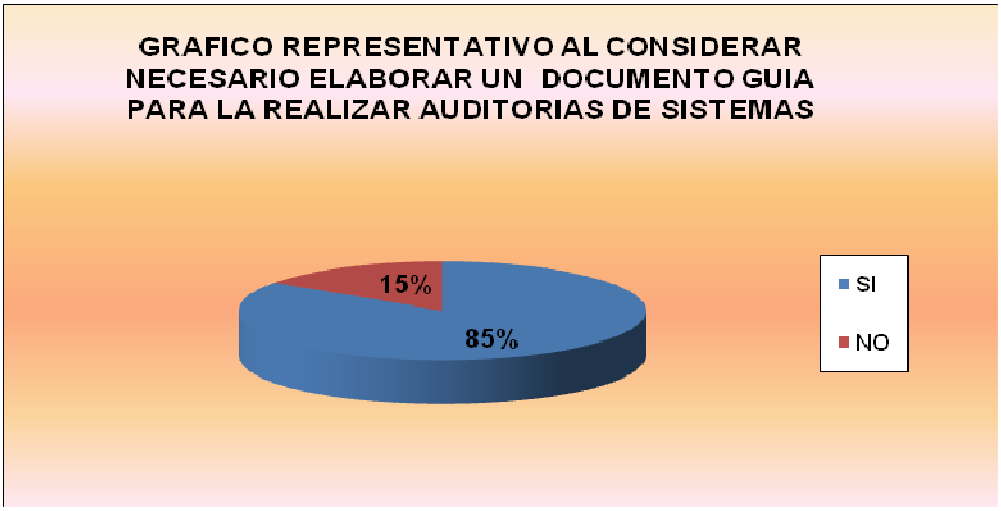
Análisis
Del total de la población encuestada el 85% respondió que al realizar la Auditoría mejoraría la buena administración en los recursos informáticos de dicha entidad y el resto de la población respondió de forma negativa.

16.¿Considera necesario contar con un documento que proporcione una guía para poder realizar una Auditoría de Sistemas?

Objetivo: Conocer si es necesario la elaboración de un documento que guie la realización de una auditoria de sistemas.

DISTRIBUCIÓN DE FRECUENCIAS

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
SI	22	84.62%
NO	4	15.38%
TOTAL	**26**	100.00%



Análisis
El 85% de la población respondió que es necesario elaborar un documento que sea utilizado como guía para la realización de una Auditoria de Sistemas para las entidades públicas o privadas y el resto con un 15% respondió que no es necesaria la elaboración de dicho documento.

ANEXO 6
NORMAS DE AUDITORÍA DE SISTEMAS

ESTATUTO DE AUDITORIA DOCUMENTO S1

La naturaleza especializada de la auditoría a los sistemas de información (SI), así como las destrezas necesarias para llevar a cabo tales auditorías, requiere de estándares que aplican específicamente a la auditoría de SI. Uno de los objetivos de la Asociación de Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Association®, ISACA®) es promover estándares aplicables internacionalmente para cumplir con su visión. El desarrollo y difusión de los Estándares de Auditoría de SI son una piedra angular de la contribución profesional de ISACA a la comunidad de auditoría. La estructura para los Estándares de Auditoría de SI brinda múltiples niveles de asesoramiento:

Los Estándare**s** definen requisitos obligatorios para la auditoría y el reporte de SI. Informan a:

- Los auditores de SI respecto al nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Los poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) respecto a los requisitos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación de la conducta del poseedor del certificado CISA por parte de la Junta de Directores de ISACA o del comité apropiado de ISACA y, en última instancia, en sanciones disciplinarias.

Las Directrices proporcionan asesoramiento en la aplicación de los Estándares de Auditoría de SI. El auditor de SI debe considerarlas al determinar cómo lograr la implementación de los estándares, utilizar un buen juicio profesional en su aplicación y estar dispuesto a justificar cualquier desviación de las mismas. El objetivo de las Directrices de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los Procedimientos proporcionan ejemplos de procedimientos que podría seguir un auditor de SI en el curso de un contrato de auditoría. Los documentos sobre procedimientos proporcionan información sobre cómo cumplir con los estándares al realizar trabajos de auditoría de SI, pero no establecen los requisitos correspondientes. El objetivo de los Procedimientos de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los recursos de **COBIT**® deben utilizarse como fuente de asesoramiento con respecto a las mejores prácticas. El *Marco Referencial* de COBIT establece que: "Es responsabilidad de la gerencia salvaguardar todos los activos de la empresa. Para descargar esta responsabilidad, así como para lograr sus expectativas, la gerencia debe establecer un adecuado sistema de control interno. " COBIT proporciona un conjunto detallado de controles y de técnicas de control para el entorno de administración/gestión de sistemas de información. La selección del material más relevante en

COBIT aplicable al alcance de la auditoría en particular se basa en la selección de procesos específicos de COBIT para TI, considerando además los criterios de información de COBIT.

Tal como se define en el *Marco Referencial* de COBIT*,* cada uno de los siguientes elementos está organizado de acuerdo con el proceso de administración/gestión de TI. COBIT está destinado para ser utilizado por la gerencia de la empresa y por la gerencia de TI, así como por los auditores de SI; por lo tanto, su utilización permite la comprensión de los objetivos del negocio, la comunicación de las mejores prácticas y las recomendaciones que deben hacerse, basándose en una referencia de estándares comúnmente comprendida y bien respetada. COBIT incluye:

- Objetivos de control—Declaraciones genéricas tanto de alto nivel como detalladas de un nivel mínimo de buen control
- Prácticas de control—Motivaciones prácticas y asesoramiento sobre "cómo implementar" los objetivos de control
- Directrices de auditoría—Asesoramiento para cada área de control sobre cómo obtener un entendimiento, evaluar cada control, evaluar el cumplimiento y sustanciar el riesgo de que los controles no se cumplan
- Directrices gerenciales—Asesoramiento sobre cómo evaluar y mejorar el desempeño del proceso de TI, utilizando modelos de madurez, métricas y factores críticos de éxito. Proporcionan un marco de referencia administrativo orientado hacia una continua y proactiva autoevaluación del control, enfocada específicamente en:
  - Medición del desempeño—¿Qué tan adecuadamente está apoyando la función de TI los requisitos del negocio? Las directrices gerenciales se pueden utilizar para apoyar talleres de autoevaluación, y también se pueden utilizar para apoyar a
  - la gerencia en la implementación de procedimientos de monitoreo y mejora continuos, como parte de un esquema de gobernabilidad de TI.
  - Perfil del control de TI—¿Cuáles procesos de TI son importantes? ¿Cuáles son los factores críticos de éxito para el control?
  - Concientización—¿Cuáles son los riesgos de no lograr los objetivos?
  - Benchmarking—¿Qué hacen los demás? ¿Cómo pueden medirse y compararse los resultados? Las directrices gerenciales proporcionan ejemplos de métricas que permiten la evaluación del desempeño de TI en términos del negocio. Los indicadores claves de resultados identifican y miden los resultados de los procesos de TI, y los indicadores claves de desempeño evalúan lo bien que están funcionando los procesos, al medir los facilitadores del proceso. Los modelos y los atributos de madurez proporcionan evaluaciones de capacidad así como benchmarking, ayudando a que la gerencia pueda medir la capacidad de control y pueda identificar vacíos de control y determinar estrategias para su mejora.

Se puede encontrar el glosario de términos en el sitio web de ISACA *www.isaca.org/glossary*. Las palabras auditoría y revisión se utilizan indistintamente

Renuncia**:** ISACA ha definido este asesoramiento como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no hace declaración alguna de que el uso de este producto garantizará un resultado satisfactorio. La publicación no debe considerarse como incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén dirigidos razonablemente para la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, el profesional de control debe aplicar su buen juicio profesional a las circunstancias de control específicas presentadas por el entorno particular de sistemas o de la tecnología de información.

La Junta de Estándares de ISACA tiene el compromiso de realizar consultas extensas al preparar los Estándares, las Directrices y los Procedimientos de Auditoría de SI. Antes de emitir cualquier documento, la Junta de Estándares emite borradores de los mismos y los expone a nivel internacional para recibir comentarios del público en general. La Junta de Estándares también busca personas con pericia o interés especial en el tema bajo consideración para consultarlos, cuando esto sea necesario. La Junta de Estándares tiene un programa de desarrollo permanente y agradece los comentarios de los miembros de ISACA y de otras partes interesadas para identificar temas emergentes que requieran estándares nuevos. Toda sugerencia se deberá enviar por correo electrónico a (standards@isaca.org), por fax a (+1.847. 253.1443) o por correo (dirección al final del documento) a la Sede Internacional de ISACA, a la atención del director de investigación de estándares y relaciones académicas. Este material fue emitido el 15 de octubre de 2004.

S1 El Estatuto de Auditoría

Introducción

01 Los Estándares de ISACA contienen principios básicos y procedimientos esenciales, identificados en letras en negrita, los cuales son obligatorios, junto con la documentación relacionada.
02 El propósito de este Estándar de Auditoría de SI es establecer y proporcionar asesoramiento con respecto al Estatuto de Auditoría utilizado durante el proceso de auditoría.

Estándar

03 El propósito, responsabilidad, autoridad y rendición de cuentas de la función de auditoría de sistemas de información o de las asignaciones de auditoría de sistemas de información deben documentarse de manera apropiada en un estatuto de auditoría o carta de compromiso.
04 El estatuto de auditoría o la carta de compromiso deben ser aceptados y aprobados en el nivel apropiado dentro de la organización.

Comentario

05 Para una función de auditoría interna de sistemas de información, se debe preparar un estatuto de auditoría para las actividades permanentes. El estatuto de auditoría debe someterse a una revisión anual, o con mayor frecuencia si varían o cambian las responsabilidades. El auditor interno de SI puede utilizar una carta de compromiso para aclarar o confirmar su participación en tareas específicas de auditoría o de no auditoría. Para el caso de una auditoría externa de SI, normalmente debe prepararse una carta de compromiso para cada tarea de auditoría o de no auditoría.

06 El estatuto de auditoría o la carta de compromiso deben ser lo suficientemente detallados como para comunicar el propósito, la responsabilidad y las limitaciones de la función o de la auditoría asignada.

07 El estatuto de auditoría o la carta de compromiso deben revisarse periódicamente para garantizar que el propósito y la responsabilidad hayan sido documentados.

08 La siguiente documentación debe consultarse para obtener información adicional sobre la preparación de un estatuto de auditoría o una carta de compromiso.

- Directrices de Auditoría de SI G5, Estatuto de auditoría
- *Marco referencial de* COBIT, Objetivo de control M4

Fecha operativa

09 Este Estándar de ISACA estará en vigencia para todas las auditorías de sistemas de información que comiencen a partir del 1 de enero de 2005.

Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 EE.UU.
Teléfono: +1.847.253.1545
Fax: +1.847.253.1443
Correo electrónico: *standards@isaca.org*
Sitio web: *www.isaca.org*

INDEPENDENCIA DOCUMENTO S2

La naturaleza especializada de la auditoría a los sistemas de información (SI), así como las destrezas necesarias para llevar a cabo tales auditorías, requiere de estándares que aplican específicamente a la auditoría de SI. Uno de los objetivos de la Asociación de Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Association®, ISACA®) es promover estándares aplicables internacionalmente para cumplir con su visión. El desarrollo y difusión de los Estándares de Auditoría de SI son una piedra angular de la contribución profesional de ISACA a la comunidad de auditoría. La estructura para los Estándares de Auditoría de SI brinda múltiples niveles de asesoramiento:

Los Estándares definen requisitos obligatorios para la auditoría y el reporte de SI. Informan a:

- Los auditores de SI respecto al nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Los poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®,CISA®) respecto a los requisitos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación de la conducta del poseedor del certificado CISA por parte de la Junta de Directores de ISACA o del comité apropiado de ISACA y, en última instancia, en sanciones disciplinarias.

Las Directrices proporcionan asesoramiento en la aplicación de los Estándares de Auditoría de SI. El auditor de SI debe considerarlas al determinar cómo lograr la implementación de los estándares, utilizar un buen juicio profesional en su aplicación y estar dispuesto a justificar cualquier desviación de las mismas. El objetivo de las Directrices de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los Procedimientos proporcionan ejemplos de procedimientos que podría seguir un auditor de SI en el curso de un contrato de auditoría. Los documentos sobre procedimientos proporcionan información sobre cómo cumplir con los estándares al realizar trabajos de auditoría de SI, pero no establecen los requisitos correspondientes. El objetivo de los Procedimientos de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los recursos de **COBIT**® deben utilizarse como fuente de asesoramiento con respecto a las mejores prácticas. El *Marco Referencial* de COBIT establece que: "Es responsabilidad de la gerencia salvaguardar todos los activos de la empresa. Para descargar esta responsabilidad, así como para lograr sus expectativas, la gerencia debe establecer un adecuado sistema de control interno. " COBIT proporciona un conjunto detallado de controles y de técnicas de control para el entorno de administración/gestión de sistemas de información. La selección del material más relevante en

COBIT aplicable al alcance de la auditoría en particular se basa en la selección de procesos específicos de COBIT para TI, considerando además los criterios de información de COBIT.

Tal como se define en el *Marco Referencial* de COBIT*,* cada uno de los siguientes elementos está organizado de acuerdo con el proceso de administración/gestión de TI. COBIT está destinado para ser utilizado por la gerencia de la empresa y por la gerencia de TI, así como por los auditores de SI; por lo tanto, su utilización permite la comprensión de los objetivos del negocio, la comunicación de las mejores prácticas y las recomendaciones que deben hacerse, basándose en una referencia de estándares comúnmente comprendida y bien respetada. COBIT incluye:

- Objetivos de control—Declaraciones genéricas tanto de alto nivel como detalladas de un nivel mínimo de buen control
- Prácticas de control—Motivaciones prácticas y asesoramiento sobre "cómo implementar" los objetivos de control
- Directrices de auditoría—Asesoramiento para cada área de control sobre cómo obtener un entendimiento, evaluar cada control, evaluar el cumplimiento y sustanciar el riesgo de que los controles no se cumplan
- Directrices gerenciales—Asesoramiento sobre cómo evaluar y mejorar el desempeño del proceso de TI, utilizando modelos de madurez, métricas y factores críticos de éxito. Proporcionan un marco de referencia administrativo orientado hacia una continua y proactiva autoevaluación del control, enfocada específicamente en:
  - Medición del desempeño—¿Qué tan adecuadamente está apoyando la función de TI los requisitos del negocio? Las directrices gerenciales se pueden utilizar para apoyar talleres de autoevaluación, y también se pueden utilizar para apoyar a la gerencia en la implementación de procedimientos de monitoreo y mejora continuos, como parte de un esquema de gobernabilidad de TI.
  - Perfil del control de TI—¿Cuáles procesos de TI son importantes? ¿Cuáles son los factores críticos de éxito para el control?
  - Concientización—¿Cuáles son los riesgos de no lograr los objetivos?
  - Benchmarking—¿Qué hacen los demás? ¿Cómo pueden medirse y compararse los resultados? Las directrices gerenciales proporcionan ejemplos de métricas que permiten la evaluación del desempeño de TI en términos del negocio. Los indicadores claves de resultados identifican y miden los resultados de los procesos de TI, y los indicadores claves de desempeño evalúan lo bien que están funcionando los procesos, al medir los facilitadores del proceso. Los modelos y los atributos de madurez proporcionan evaluaciones de capacidad así como benchmarking, ayudando a que la gerencia pueda medir la capacidad de control y pueda identificar vacíos de control y determinar estrategias para su mejora.

Se puede encontrar el glosario de términos en el sitio web de ISACA *www.isaca.org/glossary*. Las palabras auditoría y revisión se utilizan indistintamente.

Renuncia**:** ISACA ha definido este asesoramiento como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no hace declaración alguna de que el uso de este producto garantizará un resultado satisfactorio. La publicación no debe considerarse como incluyente de

cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén dirigidos razonablemente para la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, el profesional de control debe aplicar su buen juicio profesional a las circunstancias de control específicas presentadas por el entorno particular de sistemas o de la tecnología de información.

La Junta de Estándares de ISACA tiene el compromiso de realizar consultas extensas al preparar los Estándares, las Directrices y los Procedimientos de Auditoría de SI. Antes de emitir cualquier documento, la Junta de Estándares emite borradores de los mismos y los expone a nivel internacional para recibir comentarios del público en general. La Junta de Estándares también busca personas con pericia o interés especial en el tema bajo consideración para consultarlos, cuando esto sea necesario. La Junta de Estándares tiene un programa de desarrollo permanente y agradece los comentarios de los miembros de ISACA y de otras partes interesadas para identificar temas emergentes que requieran estándares nuevos. Toda sugerencia se deberá enviar por correo electrónico a (standards@isaca.org), por fax a (+1.847. 253.1443) o por correo (dirección al final del documento) a la Sede Internacional de ISACA, a la atención del director de investigación de estándares y relaciones académicas. Este material fue emitido el 15 de octubre de 2004.

S2 Independencia

Introducción

01 Las Normas de ISACA contienen 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 estándares y guías relacionadas con la independencia durante el proceso de auditoría.

Estándar

03 Independencia profesional
En todos los aspectos relacionados con la auditoría, el auditor de SI debe ser independiente del auditado, tanto en actitud como en apariencia.
04 Independencia organizacional
La función de auditoría de SI debe ser independiente del área o actividad que se está revisando para permitir una conclusión objetiva de la tarea que se audita.

Comentario

05 El estatuto de auditoría o la carta de compromiso debe considerar la independencia y la responsabilidad de la función de auditoría.
06 El auditor de SI debe ser, y aparentar ser, independiente tanto en actitud como en apariencia en todo momento.
07 Si la independencia se ve menoscabada de hecho o en apariencia, los detalles de dicho menoscabo deben informarse a las partes interesadas.
08 Dentro de la estructura organizacional, el auditor de SI debe ser independiente del área que se va a auditar.
09 La independencia debe ser evaluada de manera regular por el auditor de SI, por la gerencia y por el comité de auditoría, en caso de que éste se haya establecido.

10 A menos que lo prohíban otras normas profesionales u organizaciones regulatorias, normativas o legisladoras, no es un requisito que el auditor de SI sea independiente, o parezca serlo, cuando la naturaleza de su participación en la iniciativa de SI es en un rol de no auditor o desempeña funciones que no son de auditoría.
11 La siguiente documentación debe consultarse para obtener mayor información sobre la independencia profesional u organizacional:

- Guía o Directriz de Auditoría de SI G17, Efecto del rol de no auditor en la independencia del auditor de SI
- Guía o Directriz de Auditoría de SI G12, Relaciones e independencia organizacional
- *Marco Referencial de* COBIT, Objetivo de control M4

Fecha operativa
12 Esta Norma de ISACA está en vigencia para todas las auditorías de sistemas de información que comiencen a partir del 1 de enero de 2005.

Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 EE.UU.
Teléfono: +1.847.253.1545
Fax: +1.847.253.1443
Correo electrónico: *standards@isaca.org*
Sitio web: *www.isaca.org*

ÉTICA Y NORMAS PROFESIONALES DOCUMENTO S3

La naturaleza especializada de la auditoría a los sistemas de información (SI), así como las destrezas necesarias para llevar a cabo tales auditorías, requiere de estándares que aplican específicamente a la auditoría de SI. Uno de los objetivos de la Asociación de Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Association®, ISACA®) es promover estándares aplicables internacionalmente para cumplir con su visión. El desarrollo y difusión de los Estándares de Auditoría de SI son una piedra angular de la contribución profesional de ISACA a la comunidad de auditoría. La estructura para los Estándares de Auditoría de SI brinda múltiples niveles de asesoramiento:

Los Estándares definen requisitos obligatorios para la auditoría y el reporte de SI. Informan a:

- Los auditores de SI respecto al nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Los poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) respecto a los requisitos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación de la conducta del poseedor del certificado CISA por parte de la Junta de Directores de ISACA o del comité apropiado de ISACA y, en última instancia, en sanciones disciplinarias.

Las Directrices proporcionan asesoramiento en la aplicación de los Estándares de Auditoría de SI. El auditor de SI debe considerarlas al determinar cómo lograr la implementación de los estándares, utilizar un buen juicio profesional en su aplicación y estar dispuesto a justificar cualquier desviación de las mismas. El objetivo de las Directrices de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los Procedimientos proporcionan ejemplos de procedimientos que podría seguir un auditor de SI en el curso de un contrato de auditoría. Los documentos sobre procedimientos proporcionan información sobre cómo cumplir con los estándares al realizar trabajos de auditoría de SI, pero no establecen los requisitos correspondientes. El objetivo de los Procedimientos de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los recursos de COBIT® deben utilizarse como fuente de asesoramiento con respecto a las mejores prácticas. El *Marco Referencial* de COBIT establece que: "Es responsabilidad de la gerencia salvaguardar todos los activos de la empresa. Para descargar esta responsabilidad, así como para lograr sus expectativas, la gerencia debe establecer un adecuado sistema de control interno. COBIT

proporciona un conjunto detallado de controles y de técnicas de control para el entorno de administración/gestión de sistemas de información. La selección del material más relevante en COBIT aplicable al alcance de la auditoría en particular se basa en la selección de procesos específicos de COBIT para TI, considerando además los criterios de información de COBIT.

Tal como se define en el *Marco Referencial* de COBIT*,* cada uno de los siguientes elementos está organizado de acuerdo con el proceso de administración/gestión de TI. COBIT está destinado para ser utilizado por la gerencia de la empresa y por la gerencia de TI, así como por los auditores de SI; por lo tanto, su utilización permite la comprensión de los objetivos del negocio, la comunicación de las mejores prácticas y las recomendaciones que deben hacerse, basándose en una referencia de estándares comúnmente comprendida y bien respetada. COBIT incluye:

- Objetivos de control—Declaraciones genéricas tanto de alto nivel como detalladas de un nivel mínimo de buen control
- Prácticas de control—Motivaciones prácticas y asesoramiento sobre "cómo implementar" los objetivos de control
- Directrices de auditoría—Asesoramiento para cada área de control sobre cómo obtener un entendimiento, evaluar cada control, evaluar el cumplimiento y sustanciar el riesgo de que los controles no se cumplan
- Directrices gerenciales—Asesoramiento sobre cómo evaluar y mejorar el desempeño del proceso de TI, utilizando modelos de madurez, métricas y factores críticos de éxito. Proporcionan un marco de referencia administrativo orientado hacia una continua y proactiva autoevaluación del control, enfocada específicamente en:
  - Medición del desempeño—¿Qué tan adecuadamente está apoyando la función de TI los requisitos del negocio? Las directrices gerenciales se pueden utilizar para apoyar talleres de autoevaluación, y también se pueden utilizar para apoyar a la gerencia en la implementación de procedimientos de monitoreo y mejora continuos, como parte de un esquema de gobernabilidad de TI.
  - Perfil del control de TI—¿Cuáles procesos de TI son importantes? ¿Cuáles son los factores críticos de éxito para el control?
  - Concientización—¿Cuáles son los riesgos de no lograr los objetivos?
  - Benchmarking—¿Qué hacen los demás? ¿Cómo pueden medirse y compararse los resultados? Las directrices gerenciales proporcionan ejemplos de métricas que permiten la evaluación del desempeño de TI en términos del negocio. Los indicadores claves de resultados identifican y miden los resultados de los procesos de TI, y los indicadores claves de desempeño evalúan lo bien que están funcionando los procesos, al medir los facilitadores del proceso. Los modelos y los atributos de madurez proporcionan evaluaciones de capacidad así como benchmarking, ayudando a que la gerencia pueda medir la capacidad de control y pueda identificar vacíos de control y determinar estrategias para su mejora.

Se puede encontrar el glosario de términos en el sitio web de ISACA *www.isaca.org/glossary*. Las palabras auditoría y revisión se utilizan indistintamente.

Renuncia**:** ISACA ha definido este asesoramiento como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no hace declaración alguna de que el uso de este producto garantizará un resultado satisfactorio. La publicación no debe considerarse como incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén dirigidos razonablemente para la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, el profesional de control debe aplicar su buen juicio profesional a las circunstancias de control específicas presentadas por el entorno particular de sistemas o de la tecnología de información.

La Junta de Estándares de ISACA tiene el compromiso de realizar consultas extensas al preparar los Estándares, las Directrices y los Procedimientos de Auditoría de SI. Antes de emitir cualquier documento, la Junta de Estándares emite borradores de los mismos y los expone a nivel internacional para recibir comentarios del público en general. La Junta de Estándares también busca personas con pericia o interés especial en el tema bajo consideración para consultarlos, cuando esto sea necesario. La Junta de Estándares tiene un programa de desarrollo permanente y agradece los comentarios de los miembros de ISACA y de otras partes interesadas para identificar temas emergentes que requieran estándares nuevos. Toda sugerencia se deberá enviar por correo electrónico a (standards@isaca.org), por fax a (+1.847. 253.1443) o por correo (dirección al final del documento) a la Sede Internacional de ISACA, a la atención del director de investigación de estándares y relaciones académicas. Este material fue emitido el 15 de octubre de 2004.

S3 Ética y Estándares profesionales

Introducción

01 Los estándares de ISACA contienen 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 un estándar y proporcionar una guía para el auditor de SI con el fin de que cumpla con el Código de Ética Profesional de ISACA y ejerza el debido cuidado profesional al realizar tareas de auditoría.

Estándar

03 El auditor de SI debe cumplir con el Código de Ética Profesional de ISACA al realizar tareas de auditoría.
04 El auditor de SI debe ejercer el debido cuidado profesional, lo cual incluye cumplir con los estándares profesionales de auditoría aplicables al realizar tareas de auditoría.

Comentario

05 El Código de Ética Profesional emitido por ISACA será actualizado cada cierto tiempo para mantenerlo acorde con las tendencias emergentes y con las exigencias de la profesión de auditoría. Los miembros de ISACA y los auditores de SI deben mantenerse al día con las actualizaciones del Código de Ética Profesional y cumplir con las especificaciones de dicho código al realizar tareas como auditores de SI.
06 Los Estándares de Auditoría de SI emitidos por ISACA son revisadas periódicamente para realizar mejoras continuas, y son actualizados de acuerdo con las necesidades para mantenerse al ritmo de los desafíos que surjan en la profesión de auditoría.
Los miembros de ISACA y los auditores de SI deben conocer los Estándares de Auditoría de SI más recientes que resultaran aplicables, y ejercer el debido cuidado profesional al llevar a cabo tareas de auditoría.
07 El incumplimiento del Código de Ética Profesional de ISACA y/o de las Normas de Auditoría de SI puede resultar en una investigación de la conducta de un miembro de ISACA o del poseedor de la certificación CISA y, en última instancia, en sanciones disciplinarias.
08 Los miembros de ISACA y los auditores de SI deben comunicarse con los miembros de su equipo y asegurar que éstos cumplan con el Código de Ética Profesional y se observen las Normas de Auditoría de SI aplicables al realizar las tareas de auditoría.
09 Los auditores de SI deben resolver de manera apropiada todas las inquietudes que surjan, con respecto a la aplicación de la ética profesional o de las Normas de Auditoría de SI durante la realización de una tarea de auditoría. Si el cumplimiento de las guías de ética profesional o de las Normas de Auditoría de SI se ve menoscabado o parece menoscabado, el auditor de SI debe considerar suspender su participación.
10 El auditor de SI debe mantener el más alto grado de integridad y conducta, y no adoptar ningún método que pueda considerarse ilegal, no ético o poco profesional para obtener o realizar tareas de auditoría.
11 Debe consultarse la siguiente documentación para obtener mayor información sobre la ética y las normas profesionales:

- Guías de Auditoría de SI G19, Irregularidades y acciones ilegales
- Guías de Auditoría de SI G7, Debido cuidado profesional
- Guías de Auditoría de SI G12, Relación e independencia organizacional
- *Marco Referencial de* COBIT, Objetivo de control M4

Fecha de operación
12 Esta Norma de Auditoría de SI está en vigencia para todas las auditorías de sistemas de información que comiencen a partir del 1 de enero de 2005.

Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 EE.UU.
Teléfono: +1.847.253.1545
Fax: +1.847.253.1443
Correo electrónico: *standards@isaca.org*
Sitio web: *www.isaca.org*

COMPETENCIA PROFESIONAL DOCUMENTO S4

La naturaleza especializada de la auditoría a los sistemas de información (SI), así como las destrezas necesarias para llevar a cabo tales auditorías, requiere de estándares que aplican específicamente a la auditoría de SI. Uno de los objetivos de la Asociación de Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Association®, ISACA®) es promover estándares aplicables internacionalmente para cumplir con su visión. El desarrollo y difusión de los Estándares de Auditoría de SI son una piedra angular de la contribución profesional de ISACA a la comunidad de auditoría. La estructura para los Estándares de Auditoría de SI brinda múltiples niveles de asesoramiento:

Los Estándares definen requisitos obligatorios para la auditoría y el reporte de SI. Informan a:

- Los auditores de SI respecto al nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Los poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®,CISA®) respecto a los requisitos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación de la conducta del poseedor del certificado CISA por parte de la Junta de Directores de ISACA o del comité apropiado de ISACA y, en última instancia, en sanciones disciplinarias.

Las Directrices proporcionan asesoramiento en la aplicación de los Estándares de Auditoría de SI. El auditor de SI debe considerarlas al determinar cómo lograr la implementación de los estándares, utilizar un buen juicio profesional en su aplicación y estar dispuesto a justificar cualquier desviación de las mismas. El objetivo de las Directrices de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los Procedimientos proporcionan ejemplos de procedimientos que podría seguir un auditor de SI en el curso de un contrato de auditoría. Los documentos sobre procedimientos proporcionan información sobre cómo cumplir con los estándares al realizar trabajos de auditoría de SI, pero no establecen los requisitos correspondientes. El objetivo de los Procedimientos de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los recursos de COBIT® deben utilizarse como fuente de asesoramiento con respecto a las mejores prácticas. El Marco Referencial de COBIT establece que: "Es responsabilidad de la gerencia salvaguardar todos los activos de la empresa. Para descargar esta responsabilidad, así como para lograr sus expectativas, la gerencia debe establecer un adecuado sistema de control interno. COBIT proporciona un conjunto detallado de controles y de técnicas de control para el entorno de

administración/gestión de sistemas de información. La selección del material más relevante en COBIT aplicable al alcance de la auditoría en particular se basa en la selección de procesos específicos de COBIT para TI, considerando además los criterios de información de COBIT.

Tal como se define en el Marco Referencial de COBIT, cada uno de los siguientes elementos está organizado de acuerdo con el proceso de administración/gestión de TI. COBIT está destinado para ser utilizado por la gerencia de la empresa y por la gerencia de TI, así como por los auditores de SI; por lo tanto, su utilización permite la comprensión de los objetivos del negocio, la comunicación de las mejores prácticas y las recomendaciones que deben hacerse, basándose en una referencia de estándares comúnmente comprendida y bien respetada. COBIT incluye:

- Objetivos de control—Declaraciones genéricas tanto de alto nivel como detalladas de un nivel mínimo de buen control
- Prácticas de control—Motivaciones prácticas y asesoramiento sobre "cómo implementar" los objetivos de control
- Directrices de auditoría—Asesoramiento para cada área de control sobre cómo obtener un entendimiento, evaluar cada control, evaluar el cumplimiento y sustanciar el riesgo de que los controles no se cumplan
- Directrices gerenciales—Asesoramiento sobre cómo evaluar y mejorar el desempeño del proceso de TI, utilizando modelos de madurez, métricas y factores críticos de éxito. Proporcionan un marco de referencia administrativo orientado hacia una continua y proactiva autoevaluación del control, enfocada específicamente en:
  - Medición del desempeño—¿Qué tan adecuadamente está apoyando la función de TI los requisitos del negocio? Las directrices gerenciales se pueden utilizar para apoyar talleres de autoevaluación, y también se pueden utilizar para apoyar a la gerencia en la implementación de procedimientos de monitoreo y mejora continuos, como parte de un esquema de gobernabilidad de TI. Perfil del control de TI—¿Cuáles procesos de TI son importantes? ¿Cuáles son los factores críticos de éxito para el control?
  - Concientización—¿Cuáles son los riesgos de no lograr los objetivos?
  - Benchmarking—¿Qué hacen los demás? ¿Cómo pueden medirse y compararse los resultados? Las directrices gerenciales proporcionan ejemplos de métricas que permiten la evaluación del desempeño de TI en términos del negocio. Los indicadores claves de resultados identifican y miden los resultados de los procesos de TI, y los indicadores claves de desempeño evalúan lo bien que están funcionando los procesos, al medir los facilitadores del proceso. Los modelos y los atributos de madurez proporcionan evaluaciones de capacidad así como benchmarking, ayudando a que la gerencia pueda medir la capacidad de control y pueda identificar vacíos de control y determinar estrategias para su mejora.

Se puede encontrar el glosario de términos en el sitio web de ISACA *www.isaca.org/glossary*. Las palabras auditoría y revisión se utilizan indistintamente.

Renuncia: ISACA ha definido este asesoramiento como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no hace declaración alguna de que el uso de este producto garantizará un resultado satisfactorio. La publicación no debe considerarse como incluyente de

cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén dirigidos razonablemente para la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, el profesional de control debe aplicar su buen juicio profesional a las circunstancias de control específicas presentadas por el entorno particular de sistemas o de la tecnología de información.

La Junta de Estándares de ISACA tiene el compromiso de realizar consultas extensas al preparar los Estándares, las Directrices y los Procedimientos de Auditoría de SI. Antes de emitir cualquier documento, la Junta de Estándares emite borradores de los mismos y los expone a nivel internacional para recibir comentarios del público en general. La Junta de Estándares también busca personas con pericia o interés especial en el tema bajo consideración para consultarlos, cuando esto sea necesario. La Junta de Estándares tiene un programa de desarrollo permanente y agradece los comentarios de los miembros de ISACA y de otras partes interesadas para identificar temas emergentes que requieran estándares nuevos. Toda sugerencia se deberá enviar por correo electrónico a (standards@isaca.org), por fax a (+1.847. 253.1443) o por correo (dirección al final del documento) a la Sede Internacional de ISACA, a la atención del director de investigación de estándares y relaciones académicas. Este material fue emitido el 15 de octubre de 2004.

S4 Competencia profesional

Introducción

01 Los Estándares de Auditoría de SI de ISACA contienen 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 y brindar asesoría a fin de que el auditor de SI logre y mantenga un nivel de competencia profesional.

Estándar

03 El auditor de SI debe ser profesionalmente competente y tener las destrezas y los conocimientos para realizar la tarea de auditoría.
04 El auditor de SI debe mantener competencia profesional por medio de una apropiada educación y capacitación profesional continua.

Comentario

05 El auditor de SI debe proporcionar una garantía razonable de que dispone de suficientes aptitudes profesionales (destrezas, conocimiento y experiencia relativa a la tarea planificada) antes de iniciarse las labores. De no ser así, el auditor de SI deberá rechazar o retirarse de la tarea.
06 Si lo tiene, el auditor de SI debe cumplir con los requisitos de educación o desarrollo profesional continuos de CISA y otras designaciones profesionales relacionadas con las auditorías. Los miembros de ISACA que no tengan una designación CISA u otra designación profesional relacionada con la auditoría deben haber recibido suficiente educación formal, capacitación y tener experiencia laboral.
07 En los casos en que el auditor de SI lidere un equipo para realizar una revisión, el auditor de SI debe proporcionar una garantía razonable de que todos los miembros del equipo tengan el nivel apropiado de aptitud profesional para las labores que desempeñan.

08 Debe consultarse la siguiente documentación para obtener mayor información sobre la aptitud profesional:

- Certificación CISA y material de capacitación
- Requisitos de certificación CISA y requisitos de educación continua
- *Marco referencial de* COBIT, Objetivos de control M2, M3 y M4

Fecha de operación

09 Esta Norma de Auditoría de SI está en vigencia para todas las auditorías de sistemas de información que comiencen a partir del 1 de enero de 2005.

Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 EE.UU.
Teléfono: +1.847.253.1545
Fax: +1.847.253.1443
Correo electrónico: *standards@isaca.org*
Sitio web: *www.isaca.org*

PLANEACIÓN DOCUMENTO S5

La naturaleza especializada de la auditoría a los sistemas de información (SI), así como las destrezas necesarias para llevar a cabo tales auditorías, requiere de estándares que aplican específicamente a la auditoría de SI. Uno de los objetivos de la Asociación de Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Association, ISACA) es promover estándares aplicables internacionalmente para cumplir con su visión. El desarrollo y difusión de los Estándares de Auditoría de SI son una piedra angular de la contribución profesional de ISACA a la comunidad de auditoría. La estructura para los Estándares de Auditoría de SI brinda múltiples niveles de asesoramiento:
Los Estándares definen requisitos obligatorios para la auditoría y el reporte de SI. Informan a:

- Los auditores de SI respecto al nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Los poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) respecto a los requisitos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación de la conducta del poseedor del certificado CISA por parte de la Junta de Directores de ISACA o del comité apropiado de ISACA y, en última instancia, en sanciones disciplinarias.

Las **Directrices** proporcionan asesoramiento en la aplicación de los Estándares de Auditoría de SI. El auditor de SI debe considerarlas al determinar cómo lograr la implementación de los estándares, utilizar un buen juicio profesional en su aplicación y estar dispuesto a justificar cualquier desviación de las mismas. El objetivo de las Directrices de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.
Los **Procedimientos** proporcionan ejemplos de procedimientos que podría seguir un auditor de SI en el curso de un contrato de auditoría. Los documentos sobre procedimientos proporcionan información sobre cómo cumplir con los estándares al realizar trabajos de auditoría de SI, pero no establecen los requisitos correspondientes. El objetivo de los Procedimientos de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.
Los recursos de **COBIT**_ deben utilizarse como fuente de asesoramiento con respecto a las mejores prácticas. El mejores prácticas. El *Marco Referencial* de COBIT establece que: "Es responsabilidad de la gerencia salvaguardar todos los activos de la empresa. Para descargar esta responsabilidad, así como para lograr sus expectativas, la gerencia debe establecer un adecuado sistema de control interno. " COBIT proporciona un conjunto detallado de controles y de técnicas de control para el entorno de administración/gestión de sistemas de información. La selección del material más

relevante en COBIT aplicable al alcance de la auditoría en particular se basa en la selección de procesos específicos de COBIT para TI, considerando además los criterios de información de COBIT.

Tal como se define en el *Marco Referencial* de COBIT, cada uno de los siguientes elementos está organizado de acuerdo con el proceso de administración/gestión de TI. COBIT está destinado para ser utilizado por la gerencia de la empresa y por la gerencia de TI, así como por los auditores de SI; por lo tanto, su utilización permite la comprensión de los objetivos del negocio, la comunicación de las mejores prácticas y las recomendaciones que deben hacerse, basándose en una referencia de estándares comúnmente comprendida y bien respetada. COBIT incluye:

- Objetivos de control—Declaraciones genéricas tanto de alto nivel como detalladas de un nivel mínimo de buen control
- Prácticas de control—Motivaciones prácticas y asesoramiento sobre "cómo implementar" los objetivos de control
- Directrices de auditoría—Asesoramiento para cada área de control sobre cómo obtener un entendimiento, evaluar cada control, evaluar el cumplimiento y sustanciar el riesgo de que los controles no se cumplan
- Directrices gerenciales—Asesoramiento sobre cómo evaluar y mejorar el desempeño del proceso de TI, utilizando modelos de madurez, métricas y factores críticos de éxito. Proporcionan un marco de referencia administrativo orientado hacia una continua y proactiva autoevaluación del control, enfocada específicamente en:
  - Medición del desempeño—¿Qué tan adecuadamente está apoyando la función de TI los requisitos del negocio? Las directrices gerenciales se pueden utilizar para apoyar talleres de autoevaluación, y también se pueden utilizar para apoyar a la gerencia en la implementación de procedimientos de monitoreo y mejora continuos, como parte de un esquema de gobernabilidad de TI.
  - Perfil del control de TI—¿Cuáles procesos de TI son importantes? ¿Cuáles son los factores críticos de éxito para el control?
  - Concientización—¿Cuáles son los riesgos de no lograr los objetivos?
  - Benchmarking—¿Qué hacen los demás? ¿Cómo pueden medirse y compararse los resultados? Las directrices gerenciales proporcionan ejemplos de métricas que permiten la evaluación del desempeño de TI en términos del negocio. Los indicadores claves de resultados identifican y miden los resultados de los procesos de TI, y los indicadores claves de desempeño evalúan lo bien que están funcionando los procesos, al medir los facilitadores del proceso. Los modelos y los atributos de madurez proporcionan evaluaciones de capacidad así como benchmarking, ayudando a que la gerencia pueda medir la capacidad de control y pueda identificar vacíos de control y determinar estrategias para su mejora.

Se puede encontrar el **glosario** de términos en el sitio web de ISACA *www.isaca.org/glossary*. Las palabras auditoría y revisión se utilizan indistintamente.

Renuncia: ISACA ha definido este asesoramiento como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no hace declaración alguna de que el uso de este producto garantizará un resultado satisfactorio. La publicación no debe considerarse como incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén dirigidos razonablemente para la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, el profesional de control debe aplicar su buen juicio profesional a las circunstancias de control específicas presentadas por el entorno particular de sistemas o de la tecnología de información.

La Junta de Estándares de ISACA tiene el compromiso de realizar consultas extensas al preparar los Estándares, las Directrices y los Procedimientos de Auditoría de SI. Antes de emitir cualquier documento, la Junta de Estándares emite borradores de los mismos y los expone a nivel internacional para recibir comentarios del público en general. La Junta de Estándares también busca personas con pericia o interés especial en el tema bajo consideración para consultarlos, cuando esto sea necesario. La Junta de Estándares tiene un programa de desarrollo permanente y agradece los comentarios de los miembros de ISACA y de otras partes interesadas para identificar temas emergentes que requieran estándares nuevos. Toda sugerencia se deberá enviar por correo electrónico a (standards@isaca.org), por fax a (+1.847. 253.1443) o por correo (dirección al final del documento) a la Sede Internacional de ISACA, a la atención del director de investigación de estándares y relaciones académicas. Este material fue emitido el 15 de octubre de 2004.

S5 Planeación
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

Fecha operativa

13 Esta Norma de Auditoría de SI está en vigencia para todas las auditorías de sistemas de información que comiencen a partir del 1 de enero de 2005.

REALIZACIÓN DE LABORES DE AUDITORIA
DOCUMENTO S6

La naturaleza especializada de la auditoría a los sistemas de información (SI), así como las destrezas necesarias para llevar a cabo tales auditorías, requiere de estándares que aplican específicamente a la auditoría de SI. Uno de los objetivos de la Asociación de Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Association®, ISACA®) es promover estándares aplicables internacionalmente para cumplir con su visión. El desarrollo y difusión de los Estándares de Auditoría de SI son una piedra angular de la contribución profesional de ISACA a la comunidad de auditoría. La estructura para los Estándares de Auditoría de SI brinda múltiples niveles de asesoramiento:

Los Estándares definen requisitos obligatorios para la auditoría y el reporte de SI. Informan a:

- Los auditores de SI respecto al nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Los poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) respecto a los requisitos que deben cumplir. El incumplimiento de estos estándares puede resultar en unainvestigación de la conducta del poseedor del certificado CISA por parte de la Junta de Directores de ISACA o del comité apropiado de ISACA y, en última instancia, en sanciones disciplinarias.

Las Directrices proporcionan asesoramiento en la aplicación de los Estándares de Auditoría de SI. El auditor de SI debe considerarlas al determinar cómo lograr la implementación de los estándares, utilizar un buen juicio profesional en su aplicación y estar dispuesto a justificar cualquier desviación de las mismas. El objetivo de las Directrices de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los Procedimientos proporcionan ejemplos de procedimientos que podría seguir un auditor de SI en el curso de un contrato de auditoría. Los documentos sobre procedimientos proporcionan información sobre cómo cumplir con los estándares al realizar trabajos de auditoría de SI, pero no establecen los requisitos correspondientes. El objetivo de los Procedimientos de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los recursos de COBIT® deben utilizarse como fuente de asesoramiento con respecto a las mejores prácticas. El *Marco Referencial* de COBIT establece que: "Es responsabilidad de la gerencia salvaguardar todos los activos de la empresa. Para descargar esta responsabilidad, así como para lograr sus expectativas, la gerencia debe establecer un adecuado sistema de control interno. " COBIT proporciona un conjunto detallado de controles y de técnicas de control para el entorno de administración/gestión de sistemas de información. La selección del material más relevante en COBIT aplicable al alcance de la auditoría en particular se basa en la selección de procesos específicos de COBIT para TI, considerando además los criterios de información de COBIT.

Tal como se define en el *Marco Referencial* de COBIT, cada uno de los siguientes elementos está organizado de acuerdo con el proceso de administración/gestión de TI. COBIT está destinado para ser utilizado por la gerencia de la empresa y por la gerencia de TI, así como por los auditores de SI; por lo tanto, su utilización permite la comprensión de los objetivos del negocio, la comunicación de las mejores prácticas y las recomendaciones que deben hacerse, basándose en una referencia de estándares comúnmente comprendida y bien respetada. COBIT incluye:

- Objetivos de control—Declaraciones genéricas tanto de alto nivel como detalladas de un nivel mínimo de buen control
- Prácticas de control—Motivaciones prácticas y asesoramiento sobre “cómo implementar” los objetivos de control
- Directrices de auditoría—Asesoramiento para cada área de control sobre cómo obtener un entendimiento, evaluar cada control, evaluar el cumplimiento y sustanciar el riesgo de que los controles no se cumplan
- Directrices gerenciales—Asesoramiento sobre cómo evaluar y mejorar el desempeño del proceso de TI, utilizando modelos de madurez, métricas y factores críticos de éxito. Proporcionan un marco de referencia administrativo orientado hacia una continua y proactiva autoevaluación del control, enfocada específicamente en:
  - Medición del desempeño—¿Qué tan adecuadamente está apoyando la función de TI los requisitos del negocio? Las directrices gerenciales se pueden utilizar para apoyar talleres de autoevaluación, y también se pueden utilizar para apoyar a la gerencia en la implementación de procedimientos de monitoreo y mejora continuos, como parte de un esquema de gobernabilidad de TI.

  – Perfil del control de TI—¿Cuáles procesos de TI son importantes? ¿Cuáles son los factores críticos de éxito para el control?
  – Concientización—¿Cuáles son los riesgos de no lograr los objetivos?
  – Benchmarking—¿Qué hacen los demás? ¿Cómo pueden medirse y compararse los resultados? Las directrices gerenciales proporcionan ejemplos de métricas que permiten la evaluación del desempeño de TI en términos del negocio. Los
  indicadores claves de resultados identifican y miden los resultados de los procesos de TI, y los indicadores claves de desempeño evalúan lo bien que están funcionando los procesos, al medir los facilitadores del proceso. Los modelos y los atributos de madurez proporcionan evaluaciones de capacidad así como benchmarking, ayudando a que la gerencia pueda medir la capacidad de control y pueda identificar vacíos de control y determinar estrategias para su mejora.

Se puede encontrar el glosario de términos en el sitio web de ISACA *www.isaca.org/glossary*. Las palabras auditoría y revisión se utilizan indistintamente.

Renuncia: ISACA ha definido este asesoramiento como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no hace declaración alguna de que el uso de este producto garantizará un resultado satisfactorio. La publicación no debe considerarse como incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén dirigidos razonablemente para la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, el profesional de control debe aplicar su buen juicio profesional a las circunstancias de control específicas presentadas por el entorno particular de sistemas o de la tecnología de información.

La Junta de Estándares de ISACA tiene el compromiso de realizar consultas extensas al preparar los Estándares, las Directrices y los Procedimientos de Auditoría de SI. Antes de emitir cualquier documento, la Junta de Estándares emite borradores de los mismos y los expone a nivel internacional para recibir comentarios del público en general. La Junta de Estándares también busca personas con pericia o interés especial en el tema bajo consideración para consultarlos, cuando esto sea necesario. La Junta de Estándares tiene un programa de desarrollo permanente y agradece los comentarios de los miembros de ISACA y de otras partes interesadas para identificar temas emergentes que requieran estándares nuevos. Toda sugerencia se deberá enviar por correo electrónico a (standards@isaca.org), por fax a (+1.847. 253.1443) o por correo (dirección al final del documento) a la Sede Internacional de ISACA, a la atención del director de investigación de estándares y relaciones académicas. Este material fue emitido el 15 de octubre de 2004.

S6 Ejecución de la auditoría
Introducción
01 Las Normas de ISACA contienen principios básicos y procedimientos esenciales, identificados en letras en negrita, los cuales son obligatorios, junto con la documentación relacionada.

02 El propósito de este Estándar de Auditoría de SI es establecer normas y proporcionar asesoría con respecto a la realización de las labores de auditoría.

Estándar
03 Supervisión—El personal de auditoría de SI debe ser supervisado para brindar una garantía razonable de que se lograrán los objetivos de la auditoría y que se cumplirán las normas profesionales de auditoría aplicables.

04 Evidencia—Durante el transcurso de la auditoría, el auditor de SI debe obtener evidencia suficiente, confiable y pertinente para alcanzar los objetivos de auditoría. Los hallazgos y conclusiones de la auditoría deberán ser soportados mediante un apropiado análisis e interpretación de dicha evidencia.

05 Documentación—El proceso de auditoría deberá documentarse, describiendo las labores de auditoría realizadas y la
evidencia de auditoría que respalda los hallazgos y conclusiones del auditor de SI.

Comentario

06 Se deben establecer los roles y responsabilidades del equipo de auditoría de SI al iniciarse la auditoría, y como mínimo deben definirse los roles de decisión, ejecución y revisión.

07 Las labores realizadas durante la ejecución del trabajo deben organizarse y documentarse siguiendo procedimientos documentados predefinidos. La documentación debe incluir aspectos tales como los objetivos y alcance del trabajo, el programa de auditoría, los pasos de auditoría realizados, la evidencia recogida, los hallazgos, conclusiones y recomendaciones.

08 La documentación de auditoría debe ser suficiente para permitir que una tercera entidad independiente vuelva a realizar todas las tareas realizadas durante la auditoría para llegar a las mismas conclusiones.

09 La documentación de auditoría debe incluir detalles de quién realizó cada tarea de auditoría y sus funciones. Como regla general, cada tarea, decisión, paso o resultado de la auditoría realizado por un miembro o grupo de miembros del equipo deberá ser revisado por otra persona del equipo, nombrada de acuerdo con la importancia del elemento considerado.

10 El auditor de SI debe planificar el uso de la evidencia de auditoría obtenida de manera coherente con la importancia del objetivo de la auditoría y el tiempo y esfuerzo involucrados en obtener la evidencia de auditoría.

11 La evidencia de auditoría debe ser suficiente, confiable y pertinente para formar una opinión o respaldar los hallazgos y conclusiones del auditor de SI. Si, en opinión del auditor de SI, la evidencia de auditoría obtenida no cumple con estos criterios, el auditor de SI deberá obtener evidencia de auditoría adicional.

12 Debe consultarse la siguiente documentación para obtener más información sobre la realización de las labores de auditoría:

- *Marco Referencial de* COBIT, Objetivos de control

Fecha de operación

13 Esta Norma de Auditoría de SI está en vigencia para todas las auditorías de sistemas de información que comiencen a partir del 1 de enero de 2005.

Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 EE.UU.
Teléfono: +1.847.253.1545
Fax: +1.847.253.1443
Correo electrónico: *standards@isaca.org*
Sitio web: *www.isaca.org*

REPORTE DOCUMENTO S7

La naturaleza especializada de la auditoría a los sistemas de información (SI), así como las destrezas necesarias para llevar a cabo tales auditorías, requiere de estándares que aplican específicamente a la auditoría de SI. Uno de los objetivos de la Asociación de Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Association®, ISACA®) es promover estándares aplicables internacionalmente para cumplir con su visión. El desarrollo y difusión de los Estándares de Auditoría de SI son una piedra angular de la contribución profesional de ISACA a la comunidad de auditoría. La estructura para los Estándares de Auditoría de SI brinda múltiples niveles de asesoramiento:

Los Estándares definen requisitos obligatorios para la auditoría y el reporte de SI. Informan a:

- Los auditores de SI respecto al nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Los poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) respecto a los requisitos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación de la conducta del poseedor del certificado CISA por parte de la Junta de Directores de ISACA o del comité apropiado de ISACA y, en última instancia, en sanciones disciplinarias.

Las Directrices proporcionan asesoramiento en la aplicación de los Estándares de Auditoría de SI. El auditor de SI debe considerarlas al determinar cómo lograr la implementación de los estándares, utilizar un buen juicio profesional en su aplicación y estar dispuesto a justificar cualquier desviación de las mismas. El objetivo de las Directrices de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los Procedimientos proporcionan ejemplos de procedimientos que podría seguir un auditor de SI en el curso de un contrato de auditoría. Los documentos sobre procedimientos proporcionan información sobre cómo cumplir con los estándares al realizar trabajos de auditoría de SI, pero no establecen los requisitos correspondientes. El objetivo de los Procedimientos de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los recursos de COBIT® deben utilizarse como fuente de asesoramiento con respecto a las mejores prácticas. El *Marco Referencial* de COBIT establece que: "Es responsabilidad de la gerencia salvaguardar todos los activos de la empresa. Para descargar esta responsabilidad, así como para lograr sus expectativas, la gerencia debe establecer un adecuado sistema de control interno. " COBIT proporciona un conjunto detallado de controles y de técnicas de control para el entorno de

administración/gestión de sistemas de información. La selección del material más relevante en COBIT aplicable al alcance de la auditoría en particular se basa en la selección de procesos específicos de COBIT para TI, considerando además los criterios de información de COBIT.

Tal como se define en el *Marco Referencial* de COBIT, cada uno de los siguientes elementos está organizado de acuerdo con el proceso de administración/gestión de TI. COBIT está destinado para ser utilizado por la gerencia de la empresa y por la gerencia de TI, así como por los auditores de SI; por lo tanto, su utilización permite la comprensión de los objetivos del negocio, la comunicación de las mejores prácticas y las recomendaciones que deben hacerse, basándose en una referencia de estándares comúnmente comprendida y bien respetada. COBIT incluye:

- Objetivos de control—Declaraciones genéricas tanto de alto nivel como detalladas de un nivel mínimo de buen control Prácticas de control—Motivaciones prácticas y asesoramiento sobre "cómo implementar" los objetivos de control
- Directrices de auditoría—Asesoramiento para cada área de control sobre cómo obtener un entendimiento, evaluar cada control, evaluar el cumplimiento y sustanciar el riesgo de que los controles no se cumplan
- Directrices gerenciales—Asesoramiento sobre cómo evaluar y mejorar el desempeño del proceso de TI, utilizando modelos de madurez, métricas y factores críticos de éxito. Proporcionan un marco de referencia administrativo orientado hacia una continua y proactiva autoevaluación del control, enfocada específicamente en:
  - Medición del desempeño—¿Qué tan adecuadamente está apoyando la función de TI los requisitos del negocio? Las directrices gerenciales se pueden utilizar para apoyar talleres de autoevaluación, y también se pueden utilizar para apoyar a la gerencia en la implementación de procedimientos de monitoreo y mejora continuos, como parte de un esquema de gobernabilidad de TI.
  - Perfil del control de TI—¿Cuáles procesos de TI son importantes? ¿Cuáles son los factores críticos de éxito para el control?
  - Concientización—¿Cuáles son los riesgos de no lograr los objetivos?
  - Benchmarking—¿Qué hacen los demás? ¿Cómo pueden medirse y compararse los resultados? Las directrices gerenciales proporcionan ejemplos de métricas que permiten la evaluación del desempeño de TI en términos del negocio. Los indicadores claves de resultados identifican y miden los resultados de los procesos de TI, y los indicadores claves de desempeño evalúan lo bien que están funcionando los procesos, al medir los facilitadores del proceso. Los modelos y los atributos de madurez proporcionan evaluaciones de capacidad así como benchmarking, ayudando a que la gerencia pueda medir la capacidad de control y pueda identificar vacíos de control y determinar estrategias para su mejora.

Se puede encontrar el glosario de términos en el sitio web de ISACA *www.isaca.org/glossary*. Las palabras auditoría y revisión se utilizan indistintamente.

Renuncia: ISACA ha definido este asesoramiento como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no hace declaración alguna de que el uso de este producto garantizará un resultado satisfactorio. La publicación no debe considerarse como incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén dirigidos razonablemente para la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, el profesional de control debe aplicar su buen juicio profesional a las circunstancias de control específicas presentadas por el entorno particular de sistemas o de la tecnología de información.
La Junta de Estándares de ISACA tiene el compromiso de realizar consultas extensas al preparar los Estándares, las Directrices y los

Procedimientos de Auditoría de SI. Antes de emitir cualquier documento, la Junta de Estándares emite borradores de los mismos y los expone a nivel internacional para recibir comentarios del público en general. La Junta de Estándares también busca personas con pericia o interés especial en el tema bajo consideración para consultarlos, cuando esto sea necesario. La Junta de Estándares tiene un programa de desarrollo permanente y agradece los comentarios de los miembros de ISACA y de otras partes interesadas para identificar temas emergentes que requieran estándares nuevos.
Toda sugerencia se deberá enviar por correo electrónico a (standards@isaca.org), por fax a (+1.847. 253.1443) o por correo (dirección al final del documento) a la Sede Internacional de ISACA, a la atención del director de investigación de estándares y relaciones académicas. Este material fue emitido el 15 de octubre de 2004.

S7 Reporte
Introducción

01 Las Normas de Auditoría de SI de ISACA contienen 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 y proporcionar asesoría sobre la generación del informe, a fin de que el auditor de SI pueda cumplir con esta responsabilidad.

Estándar

03 El auditor de SI debe suministrar un informe, en un formato apropiado, al finalizar la auditoría. El informe debe identificar la organización, los destinatarios previstos y respetar cualquier restricción con respecto a su circulación.

04 El informe de auditoría debe indicar el alcance, los objetivos, el período de cobertura y la naturaleza, plazo y extensión de las labores de auditoría realizadas.

05 El informe debe indicar los hallazgos, conclusiones y recomendaciones, así como cualquier reserva, calificación o limitación que el auditor de SI tuviese en cuanto al alcance de la auditoría.

06 El auditor de SI debe tener evidencia de auditoría suficiente y apropiada para respaldar los resultados reportados.
07 Al emitirse, el informe del auditor de SI debe ser firmado, fechado y distribuido de acuerdo con los términos del estatuto de auditoría o carta de compromiso.

Comentario

08 El formato y contenido del informe generalmente varían según el tipo de servicio o contrato. Un auditor de SI puede realizar cualquiera de las siguientes acciones:

- Auditoría (de manera directa o como testigo)
- Revisión (de manera directa o como testigo)
- Procedimientos acordados

09 Cuando se requiera que el auditor de SI proporcione una opinión sobre el entorno de control y exista evidencia de auditoría sobre una debilidad material o significativa, el auditor de SI no deberá concluir que los controles internos son eficaces. El informe del auditor de SI debe describir la debilidad material o significativa y el efecto en el logro de los objetivos de los criterios de control.

10 El auditor de SI debe comentar el contenido del informe en borrador con la gerencia del área bajo revisión antes de la finalización y divulgación, e incluir los comentarios de la gerencia en el informe final cuando corresponda.

11 Cuando el auditor de SI encuentre deficiencias significativas en el entorno de control, el auditor de SI debe informar sobre estas deficiencias al comité de auditoría o a la autoridad responsable y comentar en el informe que se han comunicado dichas deficiencias significativas.

12 Cuando el auditor de SI emita informes separados, el informe final deberá hacer referencia a todos los informes separados.

13 El auditor de SI debe considerar y evaluar si comunicará a la gerencia acerca de las deficiencias en los controles internos de menor magnitud que las deficiencias significativas. En tales casos, el auditor de SI debe informar al comité de auditoría o a la autoridad responsable que se han comunicado a la gerencia dichas deficiencias del control interno.

14 El auditor de SI debe solicitar y evaluar la información sobre los hallazgos, las conclusiones y las recomendaciones de informes anteriores a fin de determinar si se han implementado las acciones apropiadas de manera oportuna.

15 Debe consultarse la siguiente documentación para obtener más información sobre la generación del informe:

- Guía de Auditoría de SI G20, Reporte
- *Marco Referencial de* COBIT, Objetivos de control M4.7 y M4.8

Fecha de operación
16 Esta Norma de Auditoría de SI está en vigencia para todas las auditorías de sistemas de información que comiencen a partir del 1 de enero de 2005.

Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 EE.UU.
Teléfono: +1.847.253.1545
Fax: +1.847.253.1443
Correo electrónico: *standards@isaca.org*
Sitio web: *www.isaca.org*

ACTIVIDADES DE SEGUIMIENTO DOCUMENTO S8

La naturaleza especializada de la auditoría a los sistemas de información (SI), así como las destrezas necesarias para llevar a cabo tales auditorías, requiere de estándares que aplican específicamente a la auditoría de SI. Uno de los objetivos de la Asociación de Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Association®, ISACA®) es promover estándares aplicables internacionalmente para cumplir con su visión. El desarrollo y difusión de los Estándares de Auditoría de SI son una piedra angular de la contribución profesional de ISACA a la comunidad de auditoría. La estructura para los Estándares de Auditoría de SI brinda múltiples niveles de asesoramiento:

Los Estándares definen requisitos obligatorios para la auditoría y el reporte de SI. Informan a:

- Los auditores de SI respecto al nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Los poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®,CISA®) respecto a los requisitos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación de la conducta del poseedor del certificado CISA por parte de la Junta de Directores de ISACA o del comité apropiado de ISACA y, en última instancia, en sanciones disciplinarias.

Las Directrices proporcionan asesoramiento en la aplicación de los Estándares de Auditoría de SI. El auditor de SI debe considerarlas al determinar cómo lograr la implementación de los estándares, utilizar un buen juicio profesional en su aplicación y estar dispuesto a justificar cualquier desviación de las mismas. El objetivo de las Directrices de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los Procedimientos proporcionan ejemplos de procedimientos que podría seguir un auditor de SI en el curso de un contrato de auditoría. Los documentos sobre procedimientos proporcionan información sobre cómo cumplir con los estándares al realizar trabajos de auditoría de SI, pero no establecen los requisitos correspondientes. El objetivo de los Procedimientos de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los recursos de COBIT® deben utilizarse como fuente de asesoramiento con respecto a las mejores prácticas. El *Marco Referencial* de COBIT establece que: "Es responsabilidad de la gerencia

salvaguardar todos los activos de la empresa. Para descargar esta responsabilidad, así como para lograr sus expectativas, la gerencia debe establecer un adecuado sistema de control interno. "COBIT proporciona un conjunto detallado de controles y de técnicas de control para el entorno de administración/gestión de sistemas de información. La selección del material más relevante en COBIT aplicable al alcance de la auditoría en particular se basa en la selección de procesos específicos de COBIT para TI, considerando además los criterios de información de COBIT.

Tal como se define en el *Marco Referencial* de COBIT*,* cada uno de los siguientes elementos está organizado de acuerdo con el proceso de administración/gestión de TI. COBIT está destinado para ser utilizado por la gerencia de la empresa y por la gerencia de TI, así como por los auditores de SI; por lo tanto, su utilización permite la comprensión de los objetivos del negocio, la comunicación de las mejores prácticas y las recomendaciones que deben hacerse, basándose en una referencia de estándares comúnmente comprendida y bien respetada. COBIT incluye:

- Objetivos de control—Declaraciones genéricas tanto de alto nivel como detalladas de un nivel mínimo de buen control
- Prácticas de control—Motivaciones prácticas y asesoramiento sobre “cómo implementar” los objetivos de control
- Directrices de auditoría—Asesoramiento para cada área de control sobre cómo obtener un entendimiento, evaluar cada control, evaluar el cumplimiento y sustanciar el riesgo de que los controles no se cumplan
- Directrices gerenciales—Asesoramiento sobre cómo evaluar y mejorar el desempeño del proceso de TI, utilizando modelos de madurez, métricas y factores críticos de éxito. Proporcionan un marco de referencia administrativo orientado hacia una continua y proactiva autoevaluación del control, enfocada específicamente en:
  - Medición del desempeño—¿Qué tan adecuadamente está apoyando la función de TI los requisitos del negocio? Las directrices gerenciales se pueden utilizar para apoyar talleres de autoevaluación, y también se pueden utilizar para apoyar a la gerencia en la implementación de procedimientos de monitoreo y mejora continuos, como parte de un esquema de gobernabilidad de TI.
  - Perfil del control de TI—¿Cuáles procesos de TI son importantes? ¿Cuáles son los factores críticos de éxito para el control?
  - Concientización—¿Cuáles son los riesgos de no lograr los objetivos?
  - Benchmarking—¿Qué hacen los demás? ¿Cómo pueden medirse y compararse los resultados? Las directrices gerenciales proporcionan ejemplos de métricas que permiten la evaluación del desempeño de TI en términos del negocio. Los indicadores claves de resultados identifican y miden los resultados de los procesos de TI, y los indicadores claves de desempeño evalúan lo bien que están funcionando los procesos, al medir los facilitadores del proceso. Los modelos y los atributos de madurez proporcionan evaluaciones de capacidad así como benchmarking, ayudando a que la gerencia pueda medir la capacidad de control y pueda identificar vacíos de control y determinar estrategias para su mejora.

Se puede encontrar el glosario de términos en el sitio web de ISACA *www.isaca.org/glossary*. Las palabras auditoría y revisión se utilizan indistintamente.

Renuncia: ISACA ha definido este asesoramiento como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no hace declaración alguna de que el uso de este producto garantizará un resultado satisfactorio. La publicación no debe considerarse como incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén dirigidos razonablemente para la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, el profesional de control debe aplicar su buen juicio profesional a las circunstancias de control específicas presentadas por el entorno particular de sistemas o de la tecnología de información.

La Junta de Estándares de ISACA tiene el compromiso de realizar consultas extensas al preparar los Estándares, las Directrices y los Procedimientos de Auditoría de SI. Antes de emitir cualquier documento, la Junta de Estándares emite borradores de los mismos y los expone a nivel internacional para recibir comentarios del público en general. La Junta de Estándares también busca personas con pericia o interés especial en el tema bajo consideración para consultarlos, cuando esto sea necesario. La Junta de Estándares tiene un programa de desarrollo permanente y agradece los comentarios de los miembros de ISACA y de otras partes interesadas para identificar temas emergentes que requieran estándares nuevos. Toda sugerencia se deberá enviar por correo electrónico a (standards@isaca.org), por fax a (+1.847. 253.1443) o por correo (dirección al final del documento) a la Sede Internacional de ISACA, a la atención del director de investigación de estándares y relaciones académicas. Este material fue emitido el 15 de octubre de 2004.

S8 Actividades de seguimiento

Introducción

01 Las Normas de ISACA contienen 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 proporcionar asesoría con respecto a las actividades de seguimiento realizadas durante un proceso de auditoría de SI.

Estándar

03 Después de informar/reportar sobre los hallazgos y las recomendaciones, el auditor de SI debe solicitar y evaluar la información relevante para concluir si la gerencia tomó las acciones apropiadas de manera oportuna.

Comentario

04 Si las acciones propuestas por la gerencia para implementar las recomendaciones notificadas se proporcionaron al auditor de SI, o se comentaron con éste, dichas acciones deberán registrarse en el informe final como la respuesta de la gerencia.
05 La naturaleza, los plazos y la extensión de las actividades de seguimiento deben tener en cuenta la importancia de los hallazgos reportados y el impacto, en caso de no haberse tomado las acciones correctivas. Los plazos de las actividades de seguimiento de una auditoría de SI en relación con el informe original deben basarse en el juicio profesional y depender de una serie de consideraciones tales como la naturaleza o magnitud de los riesgos y costos asociados a la entidad.

06 La función de auditoría interna de SI debe establecer un proceso de seguimiento para monitorear y asegurar que las acciones de la gerencia efectivamente han sido implementadas o que la gerencia superior ha aceptado el riesgo de no haber tomado la acción pertinente**.** La responsabilidad por estas actividades de seguimiento puede definirse en el estatuto de auditoría.
07 Dependiendo del alcance y de los términos del contrato, los auditores externos de SI pueden recurrir a la función de auditoría interna de SI para realizar el seguimiento de sus recomendaciones aceptadas.
08 Cuando la gerencia proporcione información sobre las acciones tomadas para implementar las recomendaciones y el auditor de SI tenga dudas con respecto a la información suministrada, se deberán llevar a cabo las pruebas apropiadas u otros procedimientos para determinar la posición o estado reales antes de concluir las actividades de seguimiento.
09 Puede presentarse un informe, sobre el estado de las actividades de seguimiento, que incluya las recomendaciones aceptadas no implementadas, ante el comité de auditoría en caso de que éste se haya establecido, o, como alternativa, al nivel apropiado de la gerencia de la entidad.
10 Como parte de las actividades de seguimiento, el auditor de SI deberá evaluar si los hallazgos no implementados siguen siendo importantes.

Fecha de operación
11 Esta Norma de Auditoría de SI está en vigencia para todas las auditorías de sistemas de información que comiencen a partir del 1 de enero de 2005.

Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 EE.UU.
Teléfono: +1.847.253.1545
Fax: +1.847.253.1443
Correo electrónico: *standards@isaca.org*
Sitio web: *www.isaca.org*

IRREGULARIDADES Y ACCIONES ILEGALES DOCUMENTO S9

La naturaleza especializada de la auditoría a los sistemas de información (SI), así como las destrezas necesarias para realizarlas, requiere de estándares que aplican específicamente a la auditoría de SI. Uno de los objetivos de la Asociación de Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Association®, ISACA®) es promover estándares aplicables internacionalmente para cumplir con su visión. El desarrollo y difusión de los Estándares de Auditoría de SI son una piedra angular de la contribución profesional de ISACA a la comunidad de auditoría. La estructura para los Estándares de Auditoría de SI brinda múltiples niveles de asesoría:

Los Estándares definen requisitos obligatorios para la auditoría de SI y el informe correspondiente. Informan a:

- Los auditores de SI respecto al nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Los poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®,CISA®) respecto a los requisitos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación de la conducta del poseedor del certificado CISA por parte de la Junta de Directores de ISACA o del comité apropiado de ISACA y, en última instancia, en sanciones disciplinarias.

Las Directrices proporcionan guías sobre la aplicación de los Estándares de Auditoría de SI. El auditor de SI debe considerarlas al determinar cómo lograr la implementación de los estándares, utilizar un buen juicio profesional en su aplicación y estar dispuesto a justificar cualquier desviación de las mismas. El objetivo de las Directrices de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los Procedimientos proporcionan ejemplos de procedimientos que podría seguir un auditor de SI durante la ejecución de una auditoría. Los documentos sobre procedimientos proporcionan información sobre cómo cumplir con los estándares al realizar trabajos de auditoría de SI, pero no establecen los requisitos correspondientes. El objetivo de los Procedimientos de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los recursos de COBIT® deben utilizarse como fuente de asesoría con respecto a las mejores prácticas. El *Marco Referencial* de COBIT establece que: "Es responsabilidad de la gerencia

salvaguardar todos los activos de la empresa. Para descargar esta responsabilidad, así como para lograr sus expectativas, la gerencia debe establecer un adecuado sistema de control interno". COBIT proporciona un conjunto detallado de controles y de técnicas de control para el entorno de administración/gestión de sistemas de información. La selección del material más relevante en COBIT aplicable al alcance de la auditoría en particular se basa en la selección de procesos específicos de COBIT para TI, considerando además los criterios de información de COBIT.

Tal como se define en el *Marco Referencial* de COBIT, cada uno de los siguientes elementos está organizado de acuerdo con el proceso de administración/gestión de TI. COBIT está destinado para ser utilizado por la gerencia de la empresa y por la gerencia de TI, así como por los auditores de SI; por lo tanto, su uso permite la comprensión de los objetivos del negocio, la comunicación de las mejores prácticas y las recomendaciones que deben hacerse, con base en estándares de referencia comúnmente comprendidos y respetados. COBIT incluye:

- Objetivos de control—Declaraciones genéricas tanto de alto nivel como detalladas de un nivel mínimo de buen control
- Prácticas de control—Razonamiento práctico y guías sobre "cómo implementar" los objetivos de control
- Directrices de auditoría—Guías para cada área de control sobre cómo obtener un entendimiento, evaluar cada control, evaluar el cumplimiento y sustanciar el riesgo de que los controles no se cumplan
- Directrices gerenciales—Guías sobre cómo evaluar y mejorar el desempeño del proceso de TI, utilizando modelos de madurez, métricas y factores críticos de éxito. Proporcionan un marco de referencia administrativo orientado hacia una continua y proactiva auto-evaluación del control, enfocada específicamente en:
  - Medición del desempeño—¿Qué tan adecuadamente está apoyando la función de TI los requerimientos del negocio? Las directrices gerenciales se pueden utilizar para apoyar talleres sobre auto-evaluación, y también se pueden utilizar para apoyar a la gerencia en la implementación de procedimientos de monitoreo y mejora continuos, como parte de un esquema de gobernabilidad de TI.
  - Perfil del control de TI—¿Cuáles procesos de TI son importantes? ¿Cuáles son los factores críticos de éxito para el control?
  - Concientización—¿Cuáles son los riesgos de no lograr los objetivos?
  - Benchmarking—¿Qué hacen los demás? ¿Cómo pueden medirse y compararse los resultados? Las directrices gerenciales proporcionan ejemplos de métricas que permiten la evaluación del desempeño de TI en términos del negocio. Los indicadores claves de resultados identifican y miden los resultados de los procesos de TI, y los indicadores claves de desempeño evalúan lo bien que están funcionando los procesos, al medir los facilitadores del proceso. Los modelos y los atributos de madurez proporcionan evaluaciones de capacidad así como benchmarking, ayudando a que la gerencia pueda medir la capacidad de control y pueda identificar vacíos de control y determinar estrategias para su mejora.

El glosario de términos se encuentra en el sitio web de ISACA *www.isaca.org/glossary*. Las palabras auditoría y revisión se utilizan indistintamente.

Límite de responsabilidad**:** ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantizará un resultado satisfactorio. La publicación no debe considerarse como incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, el profesional de control debe aplicar su buen juicio profesional a las circunstancias de control específicas presentadas por el entorno particular de sistemas o de la tecnología de información.

La Junta de Estándares de ISACA tiene el compromiso de realizar consultas extensas al preparar los Estándares, las Directrices y los Procedimientos de Auditoría de SI. Antes de emitir cualquier documento, la Junta de Estándares emite borradores de los mismos y los expone a nivel internacional para recibir comentarios del público en general. La Junta de Estándares también busca personas con pericia o interés especial en el tema bajo consideración para consultarlos cuando sea necesario. La Junta de Estándares tiene un programa de desarrollo permanente y agradece los comentarios de los miembros de ISACA y de otras partes interesadas para identificar temas emergentes que requieran estándares nuevos. Toda sugerencia se deberá enviar por correo electrónico (standards@isaca.org), por fax (+1.847.253.1443) o por correo (dirección al final del documento) a la Sede Internacional de ISACA, a la atención del director de investigación de estándares y relaciones académicas. Este material fue publicado el 1 de julio de 2005.

Irregularidades y acciones ilegales S9

Introducción
01 Los estándares de ISACA contienen principios básicos y procedimientos esenciales, identificados en letras en negrita, que son obligatorios junto con la documentación relacionada.
02 El propósito de este estándar de ISACA es establecer y proporcionar asesoría sobre irregularidades y acciones ilegales que el auditor de SI debe tener en cuenta durante el proceso de auditoría.

Estándar
03 Al planificar y realizar la auditoría para reducir el riesgo de auditoría a un nivel bajo, el auditor de SI debe tener en cuenta el riesgo de irregularidades y acciones ilegales.
04 El auditor de SI debe mantener una actitud de escepticismo profesional durante la auditoría, reconociendo la posibilidad de que podrían existir declaraciones materialmente incorrectas debido a irregularidades y acciones ilegales, independientemente de su propia evaluación del riesgo de irregularidades y acciones ilegales.
05 El auditor de SI debe obtener un entendimiento de la organización y su entorno, incluidos los controles internos.
06 El auditor de SI debe obtener evidencia de auditoría suficiente y relevante para determinar si la gerencia u otras personas dentro de la organización tienen conocimientos de cualquier irregularidad y acción ilegal real, sospechada o alegada.

07 Al realizar procedimientos de auditoría para obtener un entendimiento de la organización y su entorno, el auditor de SI debe considerar relaciones inusuales o inesperadas que pueden indicar un riesgo de declaraciones materialmente incorrectas debido a irregularidades y acciones ilegales.
08 El auditor de SI debe diseñar y realizar procedimientos para probar lo adecuado de los controles internos y el riesgo de anulación de los controles por parte de la gerencia.
09 Cuando el auditor de SI identifica una declaración incorrecta, el auditor de SI debe evaluar si tal declaración incorrecta puede indicar la existencia de una irregularidad o acción ilegal. Si existe tal indicación, el auditor de SI debe tener en cuenta las implicaciones en relación con otros aspectos de la auditoría y, en particular, las declaraciones de la gerencia.
10 El auditor de SI debe obtener declaraciones escritas de la gerencia al menos una vez al año o con mayor frecuencia, dependiendo del contrato de auditoría. La gerencia debe:

- Reconocer su responsabilidad en el diseño e implementación de controles internos para prevenir y detectar irregularidades o acciones ilegales
- Revelar al auditor de SI los resultados de la evaluación de riesgos cuando pueda existir una declaración materialmente incorrecta como resultado de una irregularidad o acción ilegal
- Revelar al auditor de SI cuando tenga conocimiento de irregularidades o acciones ilegales que estén afectando la organización en relación a:
  - La gerencia
  - Empleados que tienen funciones significativas en el control interno
- Revelar al auditor de SI cuando tenga conocimiento de cualquier declaración de irregularidades o acciones ilegales, o sospechas de irregularidades o acciones ilegales que estén afectando la organización tal como lo hayan comunicado los empleados, ex empleados, funcionarios responsables de la normatividad dentro de la organización y otros

11 Si el auditor de SI ha identificado una irregularidad material o acción ilegal, u obtiene información de que puede existir una irregularidad material o acción ilegal, el auditor de SI debe comunicarlo sin demora al nivel de dirección apropiado.
12 Si el auditor de SI ha identificado una irregularidad material o acción ilegal que involucra a la gerencia o a empleados que tienen funciones significativas en el control interno, el auditor de SI debe comunicarlo sin demora a los responsables del gobierno corporativo.
13 El auditor de SI debe dar recomendaciones al nivel apropiado de la gerencia y a aquellos responsables del gobierno corporativo sobre las debilidades materiales en el diseño e implementación del control interno para prevenir y detectar irregularidades y acciones ilegales que el auditor de SI pueda haber notado durante la auditoría.
14 Si el auditor de SI encuentra circunstancias excepcionales que afectan su capacidad para continuar ejecutando la auditoria debido a una declaración materialmente incorrecta o una acción ilegal, el auditor de SI debe tener en cuenta la responsabilidad legal y profesional aplicable en tales circunstancias, incluyendo que pueda existir el requisito para el auditor de SI de notificar a aquellos que celebraron el contrato o, en algunos casos, a los responsables del gobierno corporativo o a las autoridades responsables de la normatividad dentro de la organización o incluso considerar retirarse del contrato.
15 El auditor de SI debe documentar todas las comunicaciones, planeación, resultados, evaluaciones y conclusiones relacionadas con irregularidades materiales y acciones ilegales que han sido notificadas a la gerencia, a los responsables del gobierno corporativo, autoridades responsables de la normatividad dentro de la organización y otros.

Comentario

16 El auditor de SI debe consultar la Directriz de Auditoría de SI G19, Irregularidades y Acciones Ilegales, para obtener la definición de que constituye una irregularidad y una acción ilegal.

17 El auditor de SI debe obtener una garantía razonable de que no existen declaraciones materialmente incorrectas debido a irregularidades y acciones ilegales. Un auditor de SI no puede tener garantía absoluta con base en factores tales como el buen juicio, el alcance de las pruebas y las limitaciones inherentes de los controles internos. La evidencia de auditoría de que disponga el auditor de SI durante una auditoría debe ser de naturaleza persuasiva y no concluyente.

18 El riesgo de no detectar una declaración materialmente incorrecta que surge de una acción ilegal es mayor que el riesgo de no detectar una declaración materialmente incorrecta que surge de una irregularidad o error, porque las acciones ilegales pueden involucrar esquemas complejos diseñados para ocultar eventos o declaraciones intencionalmente incorrectas ante el auditor de SI.

19 La experiencia previa del auditor de SI y su conocimiento de la organización deben ayudarle al auditor de SI durante la auditoría. Al hacer investigaciones y realizar procedimientos de auditoría, no se espera que el auditor de SI descarte por completo su experiencia previa, pero se espera que mantenga un nivel de escepticismo profesional. El auditor de SI no debe estar satisfecho con evidencia de auditoría que sea menos que persuasiva basándose en la creencia de que la gerencia y los responsables del gobierno corporativo son honestos e íntegros. El auditor de SI y el equipo involucrado deben discutir la susceptibilidad de la organización a irregularidades y acciones ilegales como parte del proceso de planeación y durante la auditoría.

20 Para evaluar el riesgo de la existencia de irregularidades materiales y acciones ilegales, el auditor de SI debe considerar el uso de:

- Sus conocimientos y experiencia previos con la organización (incluida su experiencia con respecto a la honestidad e integridad de la gerencia y los responsables del gobierno corporativo)
- Información obtenida al entrevistar a la gerencia
- Declaraciones de la gerencia y verificaciones firmadas de los controles internos
- Otra información confiable obtenida durante el curso de la auditoría
- La evaluación de la gerencia del riesgo de irregularidades y acciones ilegales, y su proceso para identificar y responder a tales riesgos

21 Debe consultarse la documentación siguiente para obtener mayor información sobre irregularidades y acciones ilegales:

- Directriz de Auditoría de SI G5, Estatuto de auditoría
- Marco Referencial de COBIT, objetivos de control DS3, DS5, DS9, DS11 y PO6
- Ley Sarbanes-Oxley de 2002
- Ley sobre Prácticas Extranjeras Corruptas 1977

Fecha de Vigencia
22 Este estándar de ISACA estará en vigencia para todas las auditorías de sistemas de información que comiencen a partir del 1 de septiembre de 2005.

Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 EE.UU.
Teléfono: +1.847.253.1545
Fax: +1.847.253.1443
Correo electrónico: *standards@isaca.org*
Sitio web: *www.isaca.org*

GOBERNABILIDAD DE TI DOCUMENTO S10

La naturaleza especializada de la auditoría a los sistemas de información (SI), así como las destrezas necesarias para llevar a cabo tales auditorías, requiere de estándares que aplican específicamente a la auditoría de SI. Uno de los objetivos de la Asociación de Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Association®, ISACA®) es promover estándares aplicables internacionalmente para cumplir con su visión. El desarrollo y difusión de los Estándares de Auditoría de SI son una piedra angular de la contribución profesional de ISACA a la comunidad de auditoría. La estructura para los Estándares de Auditoría de SI brinda múltiples niveles de asesoría:

Los Estándares definen requisitos obligatorios para la auditoría de SI y el informe correspondiente. Informan a:

- Los auditores de SI respecto al nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Los poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®,CISA®) respecto a los requisitos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación de la conducta del poseedor del certificado CISA por parte de la Junta de Directores de ISACA o del comité apropiado de ISACA y, en última instancia, en sanciones disciplinarias.

Las Directrices proporcionan guías sobre la aplicación de los Estándares de Auditoría de SI. El auditor de SI debe considerarlas al determinar cómo lograr la implementación de los estándares, utilizar un buen juicio profesional en su aplicación y estar dispuesto a justificar cualquier desviación de las mismas. El objetivo de las Directrices de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los Procedimientos proporcionan ejemplos de procedimientos que podría seguir un auditor de SI durante la ejecución de una auditoría. Los documentos sobre procedimientos proporcionan información sobre cómo cumplir con los estándares al realizar trabajos de auditoría de SI, pero no establecen los requisitos correspondientes. El objetivo de los Procedimientos de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los recursos de COBIT® deben utilizarse como fuente de asesoría con respecto a las mejores prácticas. El *Marco Referencial* de COBIT establece que: "Es responsabilidad de la gerencia

salvaguardar todos los activos de la empresa. Para descargar esta responsabilidad, así como para lograr sus expectativas, la gerencia debe establecer un adecuado sistema de control interno". COBIT proporciona un conjunto detallado de controles y de técnicas de control para el entorno de administración/gestión de sistemas de información. La selección del material más relevante en COBIT aplicable al alcance de la auditoría en particular se basa en la selección de procesos específicos de COBIT para TI, considerando además los criterios de información de COBIT.

Tal como se define en el *Marco Referencial* de COBIT*,* cada uno de los siguientes elementos está organizado de acuerdo con el proceso de administración de TI. COBIT está destinado para ser utilizado por la gerencia de la empresa y por la gerencia de TI, así como por los auditores de SI; por lo tanto, su uso permite la comprensión de los objetivos del negocio, la comunicación de mejores prácticas y las recomendaciones con base en estándares de referencia comúnmente comprendidos y respetados. COBIT incluye:

- Objetivos de control—Declaraciones genéricas tanto de alto nivel como detalladas de un nivel mínimo de buen control
- Prácticas de control—Razonamiento práctico y guías sobre “cómo implementar” los objetivos de control
- Directrices de auditoría—Guías para cada área de control sobre cómo obtener un entendimiento, evaluar cada control, evaluar el cumplimiento y sustanciar el riesgo de que los controles no se cumplan
- Directrices gerenciales—Guías sobre cómo evaluar y mejorar el desempeño del proceso de TI, utilizando modelos de madurez, métricas y factores críticos de éxito. Proporcionan un marco de referencia administrativo orientado hacia una continua y proactiva
- auto-evaluación del control, enfocada específicamente en:
  - Medición del desempeño—¿Qué tan adecuadamente está apoyando la función de TI los requerimientos del negocio? Las directrices gerenciales se pueden utilizar para apoyar talleres sobre auto-evaluación, y también se pueden utilizar para apoyar a
  - la gerencia en la implementación de procedimientos de monitoreo y mejora continuos, como parte de un esquema de gobernabilidad de TI.
  - Perfil del control de TI—¿Cuáles procesos de TI son importantes? ¿Cuáles son los factores críticos de éxito para el control?
  - Concientización—¿Cuáles son los riesgos de no lograr los objetivos?
  - Benchmarking—¿Qué hacen los demás? ¿Cómo pueden medirse y compararse los resultados? Las directrices gerenciales proporcionan ejemplos de métricas que permiten la evaluación del desempeño de TI en términos del negocio. Los indicadores claves de resultados identifican y miden los resultados de los procesos de TI, y los indicadores claves de desempeño evalúan lo bien que están funcionando los procesos, al medir los facilitadores del proceso. Los modelos y los atributos de madurez Proporcionan evaluaciones de capacidad así como benchmarking, ayudando a que la gerencia pueda medir la capacidad de control y pueda identificar vacíos de control y determinar estrategias para su mejora.

El glosario de términos se encuentra en el sitio web de ISACA *www.isaca.org/glossary*. Las palabras auditoría y revisión se utilizan indistintamente.

Límite de responsabilidad**:** ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantizará un resultado satisfactorio. La publicación no debe considerarse como incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, el profesional de control debe aplicar su buen juicio profesional a las circunstancias de control específicas presentadas por el entorno particular de sistemas o de la tecnología de información.

La Junta de Estándares de ISACA tiene el compromiso de realizar consultas extensas al preparar los Estándares, las Directrices y los Procedimientos de Auditoría de SI. Antes de emitir cualquier documento, la Junta de Estándares emite borradores de los mismos y los expone a nivel internacional para recibir comentarios del público en general. La Junta de Estándares también busca personas con pericia o interés especial en el tema bajo consideración para consultarlos, cuando sea necesario. La Junta de Estándares tiene un programa de desarrollo permanente y agradece los comentarios de los miembros de ISACA y de otras partes interesadas para identificar temas emergentes que requieran estándares nuevos. Toda sugerencia se deberá enviar por correo electrónico (standards@isaca.org), por fax (+1.847.253.1443) o por correo (dirección al final del documento) a la Sede Internacional de ISACA, a la atención del director de investigación de estándares y relaciones académicas. Este material fue publicado el 1 de julio de 2005.

Gobernabilidad de TI S10

Introducción

01 Los estándares de ISACA contienen principios básicos y procedimientos esenciales, identificados en letras en negrita, que son obligatorios junto con la documentación relacionada.

02 El propósito de este estándar de ISACA es establecer y proporcionar asesoría en las áreas de gobernabilidad de TI que el auditor de SI debe tener en cuenta durante el proceso de auditoría.

Estándar

03 El auditor de SI debe revisar y evaluar si la función de SI está alineada con la misión, visión, valores, objetivos y estrategias de la organización.

04 El auditor de SI debe revisar si la función de SI tiene una declaración clara en cuanto al desempeño esperado por la empresa (eficacia y eficiencia) y evaluar su cumplimiento.

05 El auditor de SI debe revisar y evaluar la eficacia de los recursos de SI y el desempeño de los procesos administrativos.

06 El auditor de SI debe revisar y evaluar el cumplimiento de los requisitos legales, ambientales y de calidad de la información, así como de los requisitos fiduciarios y de seguridad.

07 El auditor de SI debe utilizar un enfoque basado en riesgos para evaluar la función de SI.

08 El auditor de SI debe revisar y evaluar el ambiente de control de la organización.

09 El auditor de SI debe revisar y evaluar los riesgos que pueden afectar de manera adversa el entorno de SI.

Guía adicional

10 El auditor de SI debe consultar la Directriz de Auditoría de SI G18, Gobernabilidad de TI.

11 El auditor de SI debe revisar y evaluar los riesgos del entorno de trabajo de SI que apoyan los procesos del negocio. La actividad de auditoría de SI debe asistir a la organización identificando y evaluando las exposiciones significativas al riesgo y contribuir al mejoramiento de la administración de riegos y los sistemas de control.

12 La Gobernabilidad de TI puede ser revisada por sí misma o considerarse en cada revisión de la función de SI.

13 El auditor de SI debe consultar las siguientes guías para obtener mayor información sobre Gobernabilidad de TI:

- Guías de auditoría de SI:
  - G5 Estatuto de auditoría
  - G6 Conceptos de materialidad para la auditoría de sistemas de información
  - G12 Relaciones e independencia organizacional
  - G13 Uso de la evaluación de riesgos en la planeación de la auditoría
  - G15 Planeación
  - G16 Efecto de terceros en los controles de TI de una organización
  - G17 Efecto del rol de no auditor en la independencia del auditor de SI
- *Directrices Gerenciales de* COBIT
- *Marco referencial de* COBIT, *Objetivos de control*; esta norma está relacionada con todos los objetivos de control en todos los dominios COBIT.
- *Informe de la Junta sobre la Gobernabilidad de TI, 2da Edición*, Instituto de Gobernabilidad de TI
- *Objetivos de control de TI para Sarbanes-Oxley*, Instituto de Gobernabilidad de TI
- Ley Sarbanes-Oxley de 2002 de EE.UU. y otras normativas específicas que también podrían ser aplicables.

Fecha de vigencia
14 Este estándar de ISACA está en vigencia para todas las auditorías de sistemas de información que comiencen a partir del 1 de septiembre de 2005.

Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 EE.UU.
Teléfono: +1.847.253.1545
Fax: +1.847.253.1443
Correo electrónico: *standards@isaca.org*
Sitio web: *www.isaca.org*

USO DE LA EVALUACIÓN DE RIESGOS EN LA PLANEACION DE LA AUDITORÍA DOCUMENTO S11

La naturaleza especializada de la auditoría a los sistemas de información (SI), así como las destrezas necesarias para llevar a cabo tales auditorías, requiere de estándares que aplican específicamente a la auditoría de SI. Uno de los objetivos de la Asociación de Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Association®, ISACA®) es promover estándares aplicables internacionalmente para cumplir con su visión. El desarrollo y difusión de los Estándares de Auditoría de SI son una piedra angular de la contribución profesional de ISACA a la comunidad de auditoría. La estructura para los Estándares de Auditoría de SI brinda múltiples niveles de asesoría:

Los **Estándares** definen requisitos obligatorios para la auditoría de SI y el informe correspondiente. Informan a:

- Los auditores de SI respecto al nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Los poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) respecto a los requisitos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación de la conducta del poseedor del certificado CISA por parte de la Junta de Directores de ISACA o del comité apropiado de ISACA y, en última instancia, en sanciones disciplinarias.

Las Directrices proporcionan guías sobre la aplicación de los Estándares de Auditoría de SI. El auditor de SI debe considerarlas al determinar cómo lograr la implementación de los estándares, utilizar un buen juicio profesional en su aplicación y estar dispuesto a justificar cualquier desviación de las mismas. El objetivo de las Directrices de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los Procedimientos proporcionan ejemplos de procedimientos que podría seguir un auditor de SI en el curso de la ejecución de una auditoría. Los documentos sobre procedimientos proporcionan información sobre cómo cumplir con los estándares al realizar trabajos de auditoría de SI, pero no establecen los requisitos correspondientes. El objetivo de los Procedimientos de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los recursos de **COBIT**® deben utilizarse como fuente de asesoría con respecto a las mejores prácticas. El *Marco Referencial* de COBIT establece que: "Es responsabilidad de la gerencia salvaguardar todos los activos de la empresa. Para descargar esta responsabilidad, así como para lograr sus expectativas, la gerencia debe establecer un adecuado sistema de control interno". COBIT proporciona un conjunto detallado de controles y de técnicas de control para el entorno de

administración/gestión de sistemas de información. La selección del material más relevante en COBIT aplicable al alcance de la auditoría en particular se basa en la selección de procesos específicos de COBIT para TI, considerando además los criterios de información de COBIT.

Tal como se define en el *Marco Referencial* de COBIT, cada uno de los siguientes elementos está organizado de acuerdo con el proceso de administración/gestión de TI. COBIT está destinado para ser utilizado por la gerencia de la empresa y por la gerencia de TI, así como por los auditores de SI; por lo tanto, su uso permite la comprensión de los objetivos del negocio, la comunicación de las mejores prácticas y las recomendaciones que deben hacerse, con base en estándares de referencia comúnmente comprendidos y respetados. COBIT incluye:

- Objetivos de control—Declaraciones genéricas tanto de alto nivel como detalladas de un nivel mínimo de buen control
- Prácticas de control—Razonamiento práctico y guías sobre "cómo implementar" los objetivos de control
- Directrices de auditoría—Guías para cada área de control sobre cómo obtener un entendimiento, evaluar cada control, evaluar el cumplimiento y sustanciar el riesgo de que los controles no se cumplan
- Directrices gerenciales—Guías sobre cómo evaluar y mejorar el desempeño del proceso de TI, utilizando modelos de madurez, métricas y factores críticos de éxito. Proporcionan un marco de referencia administrativo orientado hacia una continua y proactiva auto-evaluación del control, enfocada específicamente en:
  - Medición del desempeño—¿Qué tan adecuadamente está apoyando la función de TI los requerimientos del negocio? Las directrices gerenciales se pueden utilizar para apoyar talleres sobre auto-evaluación, y también se pueden utilizar para apoyar a la gerencia en la implementación de procedimientos de monitoreo y mejora continuos, como parte de un esquema de gobernabilidad de TI.
  - Perfil del control de TI—¿Cuáles procesos de TI son importantes? ¿Cuáles son los factores críticos de éxito para el control?
  - Concientización—¿Cuáles son los riesgos de no lograr los objetivos?
  - Benchmarking—¿Qué hacen los demás? ¿Cómo pueden medirse y compararse los resultados? Las directrices gerenciales proporcionan ejemplos de métricas que permiten la evaluación del desempeño de TI en términos del negocio. Los indicadores claves de resultados identifican y miden los resultados de los procesos de TI, y los indicadores claves de desempeño evalúan lo bien que están funcionando los procesos, al medir los facilitadores del proceso. Los modelos y los atributos de madurez proporcionan evaluaciones de capacidad así como benchmarking, ayudando a que la gerencia pueda medir la capacidad de control y pueda identificar vacíos de control y determinar estrategias para su mejora.

Se puede encontrar el **glosario** de términos en el sitio web de ISACA *www.isaca.org/glossary*. Las palabras auditoría y revisión se utilizan indistintamente.

Renuncia: ISACA ha definido este asesoramiento como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética

Profesional de ISACA. ISACA no hace declaración alguna de que el uso de este producto garantizará un resultado satisfactorio. La publicación no debe considerarse como incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén dirigidos razonablemente para la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, el profesional de control debe aplicar su buen juicio profesional a las circunstancias de control específicas presentadas por el entorno particular de sistemas o de la tecnología de información.

La Junta de Estándares de ISACA tiene el compromiso de realizar consultas extensas al preparar los Estándares, las Directrices y los Procedimientos de Auditoría de SI. Antes de emitir cualquier documento, la Junta de Estándares emite borradores de los mismos y los expone a nivel internacional para recibir comentarios del público en general. La Junta de Estándares también busca personas con pericia o interés especial en el tema bajo consideración para consultarlos, cuando esto sea necesario. La Junta de Estándares tiene un programa de desarrollo permanente y agradece los comentarios de los miembros de ISACA y de otras partes interesadas para identificar temas emergentes que requieran estándares nuevos. Toda sugerencia se deberá enviar por correo electrónico a (standards@isaca.org), por fax a (+1.847. 253.1443) o por correo (dirección al final del documento) a la Sede Internacional de ISACA, a la atención del director de investigación de estándares y relaciones académicas. Este material fue emitido el 15 de octubre de 2004.

S7 Reporte
Introducción

01 Las Normas de Auditoría de SI de ISACA contienen 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 y proporcionar asesoría sobre la generación del informe, a fin de que el auditor de SI pueda cumplir con esta responsabilidad.

Estándar

03 El auditor de SI debe suministrar un informe, en un formato apropiado, al finalizar la auditoría. El informe debe identificar la organización, los destinatarios previstos y respetar cualquier restricción con respecto a su circulación.

04 El informe de auditoría debe indicar el alcance, los objetivos, el período de cobertura y la naturaleza, plazo y extensión de las labores de auditoría realizadas.

05 El informe debe indicar los hallazgos, conclusiones y recomendaciones, así como cualquier reserva, calificación o limitación que el auditor de SI tuviese en cuanto al alcance de la auditoría.

06 El auditor de SI debe tener evidencia de auditoría suficiente y apropiada para respaldar los resultados reportados.

07 Al emitirse, el informe del auditor de SI debe ser firmado, fechado y distribuido de acuerdo con los términos del estatuto de auditoría o carta de compromiso.

Comentario

08 El formato y contenido del informe generalmente varían según el tipo de servicio o contrato. Un auditor de SI puede realizar cualquiera de las siguientes acciones:

- Auditoría (de manera directa o como testigo)
- Revisión (de manera directa o como testigo)
- Procedimientos acordados

09 Cuando se requiera que el auditor de SI proporcione una opinión sobre el entorno de control y exista evidencia de auditoría sobre una debilidad material o significativa, el auditor de SI no deberá concluir que los controles internos son eficaces. El informe del auditor de SI debe describir la debilidad material o significativa y el efecto en el logro de los objetivos de los criterios de control.

10 El auditor de SI debe comentar el contenido del informe en borrador con la gerencia del área bajo revisión antes de la finalización y divulgación, e incluir los comentarios de la gerencia en el informe final cuando corresponda.

11 Cuando el auditor de SI encuentre deficiencias significativas en el entorno de control, el auditor de SI debe informar sobre estas deficiencias al comité de auditoría o a la autoridad responsable y comentar en el informe que se han comunicado dichas deficiencias significativas.

12 Cuando el auditor de SI emita informes separados, el informe final deberá hacer referencia a todos los informes separados.

13 El auditor de SI debe considerar y evaluar si comunicará a la gerencia acerca de las deficiencias en los controles internos de menor magnitud que las deficiencias significativas. En tales casos, el auditor de SI debe informar al comité de auditoría o a la autoridad responsable que se han comunicado a la gerencia dichas deficiencias del control interno.

14 El auditor de SI debe solicitar y evaluar la información sobre los hallazgos, las conclusiones y las recomendaciones de informes anteriores a fin de determinar si se han implementado las acciones apropiadas de manera oportuna.

15 Debe consultarse la siguiente documentación para obtener más información sobre la generación del informe:

- Guía de Auditoría de SI G20, Reporte
- *Marco Referencial de* COBIT, Objetivos de control M4.7 y M4.8

Fecha de operación

16 Esta Norma de Auditoría de SI está en vigencia para todas las auditorías de sistemas de información que comiencen a partir del 1 de enero de 2005.

Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 EE.UU.
Teléfono: +1.847.253.1545
Fax: +1.847.253.1443
Correo electrónico: *standards@isaca.org*
Sitio web: *www.isaca.org*

MATERIALIDAD DE AUDITORIA DOCUMENTO S12

La naturaleza especializada de la auditoría a los sistemas de información (SI), así como las habilidades necesarias para ejecutarla, requiere de estándares que sean específicamente aplicables a la auditoría de SI. Uno de los objetivos de ISACA® es promover estándares globalmente aplicables para cumplir con su visión. El desarrollo y difusión de los Estándares de Auditoría de SI son una piedra angular de la contribución profesional de ISACA a la comunidad de auditoría. La estructura de los Estándares de Auditoría de SI brinda múltiples niveles de asesoría:

Los Estándares definen requisitos obligatorios para la auditoría de SI y el informe correspondiente. Informan a:

- Los auditores de SI respecto al nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y a demás interesados en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Los poseedores del Certificado de Auditor de Sistemas de Información (Certified Information Systems Auditor®, CISA®) respecto a los requisitos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación de la conducta del poseedor del certificado CISA por parte de la Junta de Directores de ISACA o del comité apropiado de ISACA y, en última instancia, en sanciones disciplinarias.

Las Directrices proporcionan guías sobre la aplicación de los Estándares de Auditoría de SI. El auditor de SI debe considerarlas al determinar cómo lograr la implementación de los estándares, utilizar un buen juicio profesional en su aplicación y estar dispuesto a justificar cualquier desviación de las mismas. El objetivo de las Directrices de Auditoría de SI es proporcionar mayor información con respecto al cumplimiento de los Estándares de Auditoría de SI.

Los Procedimientos proporcionan ejemplos de procedimientos que podría seguir un auditor de SI en el curso de una auditoría. Los documentos sobre procedimientos proporcionan información sobre cómo cumplir con los estándares al realizar trabajos de auditoría de SI, pero no establecen los requisitos correspondientes. El objetivo de los Procedimientos de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los recursos de COBIT® deben utilizarse como fuente de asesoría con respecto a las mejores prácticas. La estructura COBIT indica que: 'Es responsabilidad de la dirección salvaguardar todos los activos de la empresa. Para llevar a cabo esta responsabilidad, así como para lograr sus expectativas, la dirección debe establecer un sistema adecuado de control interno.' COBIT proporciona un conjunto detallado de controles y de técnicas de control para el entorno de administración/gestión de sistemas de información. La selección del material más relevante en

COBIT aplicable a la auditoría en particular se basa en la selección de procesos específicos de COBIT para TI, considerando además los criterios de información de COBIT.

Tal como se define en el *Marco de Referencia* de COBIT, cada uno de los siguientes elementos está organizado de acuerdo con el proceso de administración/gestión de TI. COBIT está destinado a ser utilizado por la gerencia de la empresa y por la gerencia de TI, así como por los auditores de SI; por lo tanto, su uso permite la comprensión de los objetivos del negocio, la comunicación de las mejores prácticas y las recomendaciones que deben hacerse, en base a estándares de referencia comúnmente comprendidos y respetados.
COBIT incluye:

- Objetivos de control—Declaraciones genéricas tanto de alto nivel como detalladas con un nivel mínimo de buen control
- Prácticas de control—Razonamiento práctico y guías sobre "cómo implementar" los objetivos de control
- Directrices de auditoría—Guías para cada área de control sobre cómo obtener un entendimiento, juzgar cada control, evaluar su conformidad y corroborar el riesgo de que los controles no se cumplan
- Directrices de gestión—Guías sobre evaluación y mejora de ejecución del proceso de TI, utilizando modelos de madurez, métricas y factores críticos de éxito. Proporcionan un marco de referencia de gestión orientado hacia una continua y proactiva autoevaluación del control, enfocada específicamente en:
  - Evaluación del rendimiento— ¿Qué tan adecuadamente está apoyando la función de TI los requerimientos del negocio? Las directrices de gestión se pueden utilizar para apoyar talleres de auto-evaluación, y también para apoyar a la gerencia en la implementación de procedimientos de monitorización y mejora continuos, como parte de un esquema de gobierno de TI.
  - Perfil del control de TI— ¿Cuáles son los procesos de TI importantes? ¿Cuáles son los factores críticos de éxito para el control?
  - Concienciación— ¿Cuáles son los riesgos de no lograr los objetivos?
  - Benchmarking— ¿Qué hacen los demás? ¿Cómo se pueden medir y comparar los resultados? Las directrices de gestión proporcionan ejemplos de métricas que permiten la evaluación de la función de TI en términos del negocio. Los indicadores clave de resultados identifican y miden los resultados de los procesos de TI, y los indicadores clave de rendimiento evalúan lo bien que están funcionando los procesos, al medir los catalizadores del proceso. Los modelos y atributos de madurez proporcionan evaluaciones de capacidad así como comparaciones de mercado, ayudando a la gerencia a medir la capacidad de control y poder identificar vacíos de control y determinar estrategias de mejora.

El glosario de términos se encuentra en el sitio web de ISACA *www.isaca.org/glossary*. Las palabras auditoría y revisión se utilizan indistintamente.

Límite de responsabilidad: ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado satisfactorio. La publicación no debe considerarse como incluyente de cualquier procedimiento y

prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, el profesional de control debe utilizar su buen juicio profesional a las circunstancias de control específicas presentadas por el entorno particular de sistemas o de tecnologías de información.

La Junta de Estándares de ISACA tiene el compromiso de realizar consultas extensas al preparar los Estándares, las Directrices y los Procedimientos de Auditoría de SI. Antes de emitir cualquier documento, la Junta de Estándares emite borradores de los mismos y los expone a nivel internacional para recibir comentarios del público en general. La Junta de Estándares también busca personas con habilidad o interés especial en el tema bajo consideración para consultarlos, cuando sea necesario. La Junta de Estándares tiene un programa de desarrollo permanente y agradece los comentarios de los miembros de ISACA y de otras partes interesadas para identificar temas emergentes que requieran estándares nuevos. Toda sugerencia se deberá enviar por correo electrónico a (standards@isaca.org), por fax a (+1.847.253.1443) o por correo (dirección al final del documento) a la Sede Internacional de ISACA, a la atención del director de estándares de investigación y relaciones académicas. Este material fue publicado el 15 de mayo de 2006.

S12 Materialidad de la auditoría

Introducción
01 Los estándares de ISACA contienen principios básicos y procedimientos esenciales, identificados con letra negrita, que junto con la documentación relacionada son obligatorios.
02 El propósito de este estándar de auditoría de SI es establecer y proporcionar una guía con respecto al concepto de materialidad de la auditoría y su relación con el riesgo de auditoría.

Estándar
03 El auditor de SI debe considerar la materialidad de la auditoría y su relación con el riesgo de auditoría a la vez que determina la naturaleza, los plazos y el alcance de los procedimientos de auditoría.
04 Mientras planifica la auditoría, el auditor de SI debe considerar las posibles debilidades o la ausencia de controles, y si tales debilidades o ausencias de controles pueden ocasionar una deficiencia importante o una debilidad material en el sistema de información.
05 El auditor de SI debe considerar el efecto acumulativo de las deficiencias o debilidades menores de control y la usencia de controles que pueden traducirse en una deficiencia significativa o debilidad material en el sistema de información.
06 El informe del auditor de SI debe divulgar los controles ineficaces o la ausencia de controles, y el significado de estas deficiencias, así como la posibilidad de que estas debilidades ocasionen una deficiencia importante o debilidad material.

Guía adicional
07 El riesgo de auditoría es el riesgo de que el auditor de SI llegue a una conclusión incorrecta basándose en los hallazgos de auditoría. El auditor de SI también debe tener conciencia de los tres componentes del riesgo de auditoría, a saber: el riesgo inherente, el riesgo del control y el riesgo de

detección. Consulte *G13, Uso de la evaluación de riesgos en la planificación de auditoría*, para obtener una explicación más detallada de los riesgos.

08 Mientras planifica y realiza la auditoría, el auditor de SI debe intentar reducir el riesgo de auditoría a un nivel aceptablemente bajo y cumplir con los objetivos de la auditoría. Esto se logra mediante la evaluación apropiada de SI y de los controles relacionados.

09 La debilidad en el control se considera "material" si la ausencia del mismo ocasiona que no exista una garantía razonable de que se cumplirá con el objetivo de control.

10 Una debilidad clasificada como material implica lo siguiente:

- Los controles no están establecidos y/o los controles no son utilizados y/o los controles son inadecuados.
- Puede producir un escalamiento.

11 Una debilidad material es una deficiencia importante o una combinación de deficiencias importantes que originan, con una probabilidad más que remota, que un evento indeseado no sea prevenido o detectado.

12 Existe una relación inversa entre materialidad y el nivel de riesgo de auditoría aceptable para el auditor de SI; es decir, cuanto mayor sea el nivel de materialidad, menor será la capacidad de aceptación del riesgo de auditoría, y viceversa. Esto permite al auditor de SI determinar la naturaleza, los plazos y el alcance de los procedimientos de auditoría. Por ejemplo, al planificar un procedimiento específico de auditoría, el auditor de SI determina que la materialidad es menor, aumentando por lo tanto el riesgo de auditoría. El auditor de SI querrá entonces compensarlo ya sea extendiendo la prueba de los controles (reducir la evaluación del riesgo del control) o extendiendo los procedimientos de pruebas sustantivas (reducir la evaluación del riesgo de detección).

13 Al determinar si una deficiencia de control o una combinación de deficiencias de control representan una deficiencia importante o una debilidad material, el auditor de SI deberá evaluar el efecto de los controles compensatorios y si los mismos resultan eficaces.

14 La evaluación del auditor de SI de la materialidad y del riesgo de auditoría puede variar de vez en cuando, dependiendo de las circunstancias y el entorno cambiante.

15 El auditor de SI debe consultar la Directriz de Auditoría de SI *G6 Conceptos de materialidad de la auditoría de sistemas de información.*

16 Consulte la siguiente guía para obtener más información sobre la materialidad de auditoría:

- Directrices de auditoría de SI:
  - G2 Requisitos de evidencia de auditoría
  - G5 Estatuto de auditoría
  - G8 Documentación de auditoría
  - G9 Consideraciones de auditoría sobre irregularidades
  - G13 Uso de la evaluación de riesgos en la planificación de la auditoría
- COBIT 4.0, IT Governance Institute, 2005
- Objetivos de control de TI de Sarbanes-Oxley, IT Governance Institute, 2004

Fecha de Vigencia

17 Este estándar de ISACA entrará en vigor para todas aquellas auditorías de sistemas de información que comiencen a partir del 1 de julio de 2006.

Information Systems Audit and Control Association® (ISACA)
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 EE.UU.
Teléfono: +1.847.253.1545
Fax: +1.847.253.1443
Correo electrónico: *standards@isaca.org*
Sitio web: *www.isaca.org*

USO DEL TRABAJO DE OTROS EXPERTOS DOCUMENTO S13

La naturaleza especializada de la auditoría a los sistemas de información (SI), así como las habilidades necesarias para ejecutarla, requiere de estándares que sean específicamente aplicables a la auditoría de SI. Uno de los objetivos de ISACA® es promover estándares globalmente aplicables para cumplir con su visión. El desarrollo y difusión de los Estándares de Auditoría de SI son una piedra angular de la contribución profesional de ISACA a la comunidad de auditoría. La estructura de los Estándares de Auditoría de SI brinda múltiples niveles de asesoría:

Los Estándares definen requisitos obligatorios para la auditoría de SI y el informe correspondiente. Informan a:

- Los auditores de SI respecto al nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.
- La dirección y a demás interesados en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Los poseedores del Certificado de Auditor de Sistemas de Información (Certified Information Systems Auditor®, CISA®) respecto a los requisitos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación de la conducta del poseedor del certificado CISA por parte de la Junta de Directores de ISACA o del comité apropiado de ISACA y, en última instancia, en sanciones disciplinarias.

Las Directrices proporcionan guías sobre la aplicación de los Estándares de Auditoría de SI. El auditor de SI debe considerarlas al determinar cómo lograr la implementación de los estándares, utilizar un buen juicio profesional en su aplicación y estar dispuesto a justificar cualquier desviación de las mismas. El objetivo de las Directrices de Auditoría de SI es proporcionar mayor información con respecto al cumplimiento de los Estándares de Auditoría de SI.

Los Procedimientos proporcionan ejemplos de procedimientos que podría seguir un auditor de SI en el curso de una auditoría. Los documentos sobre procedimientos proporcionan información sobre cómo cumplir con los estándares al realizar trabajos de auditoría de SI, pero no establecen los requisitos correspondientes. El objetivo de los Procedimientos de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los recursos de COBIT® deben utilizarse como fuente de asesoría con respecto a las mejores prácticas. La estructura COBIT indica que: 'Es responsabilidad de la dirección salvaguardar todos los activos de la empresa. Para llevar a cabo esta responsabilidad, así como para lograr sus expectativas, la dirección debe establecer un sistema adecuado de control interno.' COBIT proporciona un conjunto detallado de controles y de técnicas de control para el entorno de administración/gestión de sistemas de información. La selección del material más relevante en

COBIT aplicable a la auditoría en particular se basa en la selección de procesos específicos de COBIT para TI, considerando además los criterios de información de COBIT.

Tal como se define en el *Marco de Referencia* de COBIT, cada uno de los siguientes elementos está organizado de acuerdo con el proceso de administración/gestión de TI. COBIT está destinado a ser utilizado por la gerencia de la empresa y por la gerencia de TI, así como por los auditores de SI; por lo tanto, su uso permite la comprensión de los objetivos del negocio, la comunicación de las mejores prácticas y las recomendaciones que deben hacerse, en base a estándares de referencia comúnmente comprendidos y respetados. COBIT incluye:

- Objetivos de control—Declaraciones genéricas tanto de alto nivel como detalladas con un nivel mínimo de buen control
- Prácticas de control—Razonamiento práctico y guías sobre "cómo implementar" los objetivos de control
- Directrices de auditoría—Guías para cada área de control sobre cómo obtener un entendimiento, juzgar cada control, evaluar su conformidad y corroborar el riesgo de que los controles no se cumplan
- Directrices de gestión—Guías sobre evaluación y mejora de ejecución del proceso de TI, utilizando modelos de madurez, métricas y factores críticos de éxito. Proporcionan un marco de referencia de gestión orientado hacia una continua y proactiva
- auto-evaluación del control, enfocada específicamente en:
  - Evaluación del rendimiento—¿Qué tan adecuadamente está apoyando la función de TI los requerimientos del negocio?
  - Las directrices de gestión se pueden utilizar para apoyar talleres de auto-evaluación, y también para apoyar a la gerencia en la implementación de procedimientos de monitorización y mejora continuos, como parte de un esquema de gobierno de TI.
  - Perfil del control de TI—¿Cuáles son los procesos de TI importantes? ¿Cuáles son los factores críticos de éxito para el control?
  - Concienciación—¿Cuáles son los riesgos de no lograr los objetivos?
  - Benchmarking—¿Qué hacen los demás? ¿Cómo se pueden medir y comparar los resultados? Las directrices de gestión proporcionan ejemplos de métricas que permiten la evaluación de la función de TI en términos del negocio. Los indicadores clave de resultados identifican y miden los resultados de los procesos de TI, y los indicadores clave de rendimiento evalúan lo bien que están funcionando los procesos, al medir los catalizadores del proceso. Los modelos y atributos de madurez proporcionan evaluaciones de capacidad así como comparaciones de mercado, ayudando a la gerencia a medir la capacidad de control y poder identificar vacíos de control y determinar estrategias de mejora.

El glosario de términos se encuentra en el sitio web de ISACA *www.isaca.org/glossary*. Las palabras auditoría y revisión se utilizan indistintamente.

Límite de responsabilidad**:** ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice bgvftr un resultado satisfactorio. La publicación no debe considerarse como incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, el profesional de control debe utilizar su buen juicio profesional a las circunstancias de control específicas presentadas por el entorno particular de sistemas o de tecnologías de información.

La Junta de Estándares de ISACA tiene el compromiso de realizar consultas extensas al preparar los Estándares, las Directrices y los
Procedimientos de Auditoría de SI. Antes de emitir cualquier documento, la Junta de Estándares emite borradores de los mismos y los expone a nivel internacional para recibir comentarios del público en general. La Junta de Estándares también busca personas con habilidad o interés especial en el tema bajo consideración para consultarlos, cuando sea necesario. La Junta de Estándares tiene un programa de desarrollo permanente y agradece los comentarios de los miembros de ISACA y de otras partes interesadas para identificar temas emergentes que requieran estándares nuevos. Toda sugerencia se deberá enviar por correo electrónico a (standards@isaca.org), por fax a (+1.847.253.1443) o por correo (dirección al final del documento) a la Sede Internacional de ISACA, a la atención del director de estándares de investigación y relaciones académicas. Este material fue publicado el 15 de mayo de 2006

S13 Uso del trabajo de otros expertos

Introducción
01 Los estándares de ISACA contienen principios básicos y procedimientos esenciales, identificados con letra negrita, que junto con la documentación relacionada son obligatorios.
02 El propósito de este Estándar de Auditoría de SI es establecer y proporcionar asesoramiento al auditor de SI que utilice el trabajo de otros expertos durante una auditoría.

Estándares
03 El auditor de SI debe, donde resulte apropiado, considerar el uso del trabajo de otros expertos para realizar la auditoría.
04 El auditor de SI debe evaluar y estar satisfecho con las credenciales profesionales, competencias, experiencia relevante, recursos, independencia y procesos de control de calidad de otros expertos, antes de su contratación.
05 El auditor de SI debe evaluar, revisar y calificar el trabajo de otros expertos como parte de la auditoría y concluir el grado de utilidad y la fiabilidad del trabajo del experto.
06 El auditor de SI debe determinar y concluir si el trabajo de otros expertos resulta adecuado y suficiente para permitir que el auditor de SI saque sus conclusiones con respecto a los objetivos actuales de la auditoría. Dicha conclusión debe documentarse claramente.
07 El auditor de SI debe aplicar procedimientos de prueba adicionales para lograr una evidencia de auditoría suficiente y apropiada en circunstancias en las que el trabajo de otros expertos no la proporciona.

08 El auditor de SI debe proporcionar una opinión de auditoría apropiada e incluir los límites del alcance cuando no se obtenga la evidencia requerida mediante procedimientos de prueba adicionales.

Guía adicional
09 El auditor de SI debe considerar la incorporación de otros expertos durante la auditoría cuando existan limitaciones que pudieran perjudicar el trabajo de auditoría a realizar o cuando se anticipe una ganancia en la calidad de la misma. Algunos ejemplos incluyen los conocimientos requeridos debido a la naturaleza técnica de las tareas que deben realizarse, escasos recursos de auditoría y restricciones de tiempo.
10 Un "experto" podría ser un auditor de SI procedente de una empresa contable externa, un consultor gerencial, un experto de TI o un experto en el área de la auditoría que ha sido nombrado por la alta gerencia o por el equipo de auditoría de SI.
11 Un experto podría ser interno o externo a la organización. Si un experto es contratado por otra parte de la organización, se puede confiar en el informe del experto. En algunos casos, esto puede disminuir la necesidad de cobertura de auditoría de
SI aunque el auditor de SI no tenga acceso a la documentación de apoyo y a los documentos de trabajo. El auditor de SI debe tener cuidado al proporcionar una opinión en tales casos.
12 El auditor de SI debe tener acceso a todos los documentos de trabajo, documentación de apoyo e informes de otros expertos, donde dicho acceso no ocasione problemas legales. Donde el acceso del experto a registros ocasione problemas legales y por tanto, no se dispone del mismo, el auditor de SI debe determinar y concluir apropiadamente el grado de utilidad y confianza en el trabajo del experto.
13 Las opiniones/relevancia/comentarios del auditor de SI sobre la posibilidad de adoptar el informe del experto deben formar parte del informe del auditor de SI.
14 El auditor de SI debe consultar el Estándar de Auditoría de SI S6, Ejecución del trabajo de auditoría, que declara que el auditor de SI debe obtener evidencia suficiente, fiable, relevante y útil para alcanzar los objetivos de la auditoría.
15 Si el auditor de SI no tiene la habilidad requerida u otras competencias para realizar la auditoría, debe buscar asistencia competente de otros expertos; no obstante, el auditor de SI debe tener buenos conocimientos del trabajo realizado aunque no debe esperarse que tenga un nivel de conocimientos equivalente al experto.
16 El auditor de SI debe consultar la Directriz de Auditoría de SI *G1 Utilización del trabajo de otros auditores y expertos*.
17 Consulte la siguiente guía para obtener más información sobre el uso del trabajo de otros auditores y expertos:

- Directrices de auditoría de SI:
  - *G5 Estatuto de auditoría*
  - *G8 Documentación de auditoría*
  - *G2 Requisitos de evidencia de auditoría*
  - *G10 Muestreo de auditoría*
  - *G13 Uso de la evaluación de riesgos en la planificación de la auditoría*

- COBIT 4.0, IT Governance Institute, 2005
- *Objetivos de control de TI de Sarbanes-Oxley*, IT Governance Institute, 2004

Fecha de Vigencia
18 Este estándar de ISACA entrará en vigor para todas las auditorías de sistemas de información que comiencen a partir del 1 de julio de 2006.

Information Systems Audit and Control Association® (ISACA)
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 EE.UU.
Teléfono: +1.847.253.1545
Fax: +1.847.253.1443
Correo electrónico: *standards@isaca.org*
Sitio web: *www.isaca.org*

EVIDENCIA DE AUDITORÍA DOCUMENTO S14

La naturaleza especializada de la auditoría a los sistemas de información (SI), así como las habilidades necesarias para ejecutarla, requiere de estándares que sean específicamente aplicables a la auditoría de SI. Uno de los objetivos de ISACA® es promover estándares globalmente aplicables para cumplir con su visión. El desarrollo y difusión de los Estándares de Auditoría de SI son una piedra angular de la contribución profesional de ISACA a la comunidad de auditoría. La estructura de los Estándares de Auditoría de SI brinda múltiples niveles de asesoría:

- Los Estándares definen requisitos obligatorios para la auditoría de SI y el informe correspondiente. Informan a:
  - Los auditores de SI respecto al nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. La dirección y a demás interesados en las expectativas de la profesión con respecto al trabajo de sus profesionales.
  - Los poseedores del Certificado de Auditor de Sistemas de Información (Certified Information Systems Auditor®, CISA®) respecto a los requisitos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación de la conducta del poseedor del certificado CISA por parte de la Junta de Directores de ISACA o del comité apropiado de ISACA y, en última
  - instancia, en sanciones disciplinarias.
- Las Directrices proporcionan guías sobre la aplicación de los Estándares de Auditoría de SI. El auditor de SI debe considerarlas al determinar cómo lograr la implementación de los estándares, utilizar un buen juicio profesional en su aplicación y estar dispuesto a justificar cualquier desviación de las mismas. El objetivo de las Directrices de Auditoría de SI es proporcionar mayor información con respecto al cumplimiento de los Estándares de Auditoría de SI.
- Los Procedimientos proporcionan ejemplos de procedimientos que podría seguir un auditor de SI en el curso de una auditoría. Los documentos sobre procedimientos proporcionan información sobre cómo cumplir con los estándares al realizar trabajos de auditoría de SI, pero no establecen los requisitos correspondientes. El objetivo de los Procedimientos de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Los recursos de **COBIT®** deben utilizarse como fuente de asesoría con respecto a las mejores prácticas. La estructura COBIT indica que: 'Es responsabilidad de la dirección salvaguardar todos los activos de la empresa. Para llevar a cabo esta responsabilidad, así como para lograr sus expectativas, la dirección debe establecer un sistema adecuado de control interno.' COBIT proporciona un conjunto detallado de controles y de técnicas de control para el entorno de administración/gestión de sistemas de información. La selección del material más relevante en

COBIT aplicable a la auditoría en particular se basa en la selección de procesos específicos de COBIT para TI, considerando además los criterios de información de COBIT.
Tal como se define en el Marco de Referencia de COBIT, cada uno de los siguientes elementos está organizado de acuerdo con el proceso de administración/gestión de TI. COBIT está destinado a ser utilizado por la gerencia de la empresa y por la gerencia de TI, así como por los auditores de SI; por lo tanto, su uso permite la comprensión de los objetivos del negocio, la comunicación de las mejores prácticas y las recomendaciones que deben hacerse, en base a estándares de referencia comúnmente comprendidos y respetados. COBIT incluye:

- Objetivos de control—Declaraciones genéricas tanto de alto nivel como detalladas con un nivel mínimo de buen control
- Prácticas de control—Razonamiento práctico y guías sobre 'cómo implementar' los objetivos de control
- Directrices de auditoría—Guías para cada área de control sobre cómo obtener un entendimiento, juzgar cada control, evaluar su conformidad y corroborar el riesgo de que los controles no se cumplan
- Directrices de gestión—Guías sobre evaluación y mejora de ejecución del proceso de TI, utilizando modelos de madurez, métricas y factores críticos de éxito. Proporcionan un marco de referencia de gestión orientado hacia una continua y proactiva auto-evaluación del control, enfocada específicamente en:
  - Evaluación del rendimiento—¿Qué tan adecuadamente está apoyando la función de TI los requerimientos del negocio? Las directrices de gestión se pueden utilizar para apoyar talleres de auto-evaluación, y también para apoyar a la gerencia en la implementación de procedimientos de monitorización y mejora continuos, como parte de un esquema de gobierno de TI.
  - Perfil del control de TI—¿Cuáles son los procesos de TI importantes? ¿Cuáles son los factores críticos de éxito para el control?
  - Concienciación—¿Cuáles son los riesgos de no lograr los objetivos?
  - Benchmarking—¿Qué hacen los demás? ¿Cómo se pueden medir y comparar los resultados? Las directrices de gestión proporcionan ejemplos de métricas que permiten la evaluación de la función de TI en términos del negocio. Los indicadores clave de resultados identifican y miden los resultados de los procesos de TI, y los indicadores clave de rendimiento evalúan lo bien que están funcionando los procesos, al medir los catalizadores del proceso. Los modelos y atributos de madurez proporcionan evaluaciones de capacidad así como comparaciones de mercado, ayudando a la gerencia a medir la capacidad de control y poder identificar vacíos de control y determinar estrategias de mejora.

El **glosario** de términos se encuentra en el sitio web de ISACA www.isaca.org/glossary. Las palabras auditoría y revisión se utilizan indistintamente.

Límite de responsabilidad: ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado satisfactorio. La publicación no debe considerarse como incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente

dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, el profesional de control debe utilizar su buen juicio profesional a las circunstancias de control específicas presentadas por el entorno particular de sistemas o de tecnologías de información.

La Junta de Estándares de ISACA tiene el compromiso de realizar consultas extensas al preparar los Estándares, las Directrices y los Procedimientos de Auditoría de SI. Antes de emitir cualquier documento, la Junta de Estándares emite borradores de los mismos y los expone a nivel internacional para recibir comentarios del público en general. La Junta de Estándares también busca personas con habilidad o interés especial en el tema bajo consideración para consultarlos, cuando sea necesario. La Junta de Estándares tiene un programa de desarrollo permanente y agradece los comentarios de los miembros de ISACA y de otras partes interesadas para identificar temas emergentes que requieran estándares nuevos. Toda sugerencia se deberá enviar por correo electrónico a (standards@isaca.org), por fax a (+1.847.253.1443) o por correo (dirección al final del documento) a la Sede Internacional de ISACA, a la atención del director de estándares de investigación y relaciones académicas. Este material fue publicado el 15 de mayo de 2006.

S14 Evidencia de auditoría

Introducción

01 Los estándares de ISACA contienen principios básicos y procedimientos esenciales, identificados con letra negrita, que junto con la documentación relacionada son obligatorios.

02 El propósito de este estándar es establecer estándares y proporcionar una guía sobre lo que constituye evidencia de auditoría, y la calidad y cantidad de evidencias de auditoría que deberá obtener el auditor de SI.

Estándar

03 El auditor de SI debe obtener evidencias de auditoría suficientes y apropiadas para llegar a conclusiones razonables sobre las que basar los resultados de la auditoría.

04 El auditor de SI debe evaluar la suficiencia de las evidencias de auditoría obtenidas durante la misma.

Comentario

Evidencia apropiada

05 Evidencia de auditoría:

- Incluye los procedimientos realizados por el auditor
- Incluye los resultados de los procedimientos realizados por el auditor de SI
- Incluye los documentos fuente (en formato electrónico o impresos en papel), registros e información de corroboración utilizados para apoyar la auditoría
- Incluye los hallazgos y resultados del trabajo de auditoría
- Demuestra que el trabajo fue realizado y cumple con las leyes, normativas y políticas aplicables

06 Al obtener una evidencia de auditoría de una prueba de controles, el auditor de SI debe considerar la completitud de la evidencia de auditoría para apoyar el nivel de riesgo del control evaluado.

07 Es necesario identificar, obtener las referencias cruzadas y catalogar de forma adecuada la evidencia de auditoría.

08 Deben tenerse en cuenta propiedades tales como la fuente, naturaleza (por ejemplo, escrito, oral, visual, electrónica) y autenticidad (por ejemplo, firmas digitales y manuales, sellos) de la evidencia de auditoría al evaluar su nivel de fiabilidad.

Evidencia fiable

09 En términos generales, la fiabilidad de la evidencia de auditoría es mayor cuando:
- Aparece en forma escrita, en lugar de presentarse como expresiones orales
- Se obtiene de fuentes independientes
- Es obtenida por el auditor de SI en lugar de obtenerlo de la entidad que se está auditando
- Es certificada por una entidad independiente
- Es mantenida por una entidad independiente

10 El auditor de SI debe considerar la forma más económica de recopilar la evidencia necesaria para satisfacer los objetivos y riesgos de la auditoría. Sin embargo, la dificultad o coste no es una razón válida para omitir un proceso necesario.

11 Los procedimientos usados para recopilar evidencias de auditoría dependen de la temática auditada (es decir, su naturaleza, plazos de la auditoría, juicio profesional). El auditor de SI debe seleccionar el procedimiento más apropiado para cada objetivo de auditoría.

12 El auditor de SI puede obtener una evidencia de auditoría por:
- Inspección
- Observación
- Consulta y confirmación
- Repetición de la ejecución
- Repetición del cálculo
- Computación
- Procedimientos analíticos
- Otros métodos generalmente aceptados

13 El auditor de SI debe considerar la fuente y la naturaleza de cualquier información obtenida para evaluar su fiabilidad y ulteriores requisitos de verificación.

Evidencia suficiente

14 La evidencia puede considerarse suficiente si soporta todas las preguntas materiales referentes al objetivo y al alcance de la auditoría.

15 La evidencia de auditoría debe ser objetiva y suficiente para permitir que un tercero independiente repita la ejecución de las pruebas y obtenga los mismos resultados. La evidencia debe ser proporcional a la materialidad del elemento y a los riesgos involucrados.

16 La suficiencia es una medida de la cantidad de evidencias de auditoría, mientras que lo apropiado es la medida de la calidad de la evidencia de auditoría, estando ambos conceptos relacionados entre sí. En este contexto, cuando se obtiene información de la organización que es utilizada por el auditor de SI para realizar los procedimientos de auditoría, el auditor de SI debe también poner énfasis en la precisión y completitud de la información.

17 En aquellas situaciones en las que el auditor de SI cree que no se puede obtener evidencia suficiente de auditoría, el auditor de SI deberá reportar este hecho de una manera coherente durante la comunicación de los resultados de auditoría.

Protección y retención

18 La evidencia de auditoría debe protegerse de accesos y modificaciones no autorizados.

19 La evidencia de auditoría debe retenerse después de completarse el trabajo de auditoría durante el tiempo que resulte necesario para cumplir con todas las leyes, normas y políticas aplicables.

Referencia

20 Consulte la siguiente guía para obtener más información sobre la evidencia de auditoría:

- Estándar de Auditoría de SI S6 Ejecución del trabajo de auditoría
- Directriz de Auditoría de SI G2 Requisitos de evidencia de auditoría
- Directriz de Auditoría de SI G8 Documentación de auditoría
- Objetivos de control de COBIT ME2 Monitorizar y evaluar el control interno y ME3 Garantizar el cumplimiento normativo.

Fecha de Vigencia

21 Este estándar entrará en vigor para todas las auditorías de sistemas de información que comiencen a partir del 1 de julio de 2006.

CONTROLES DE TI DOCUMENTO S15

La naturaleza especializada de la auditoría a los sistemas de información (SI), así como las habilidades necesarias para ejecutarla, requiere de estándares que sean específicamente aplicables a la auditoría de SI. Uno de los objetivos de ISACA® es promover estándares globalmente aplicables para cumplir con su visión. El desarrollo y difusión de los Estándares de Auditoría de SI son una piedra angular de la contribución profesional de ISACA a la comunidad de auditoría. La estructura de los Estándares de Auditoría de SI brinda múltiples niveles de asesoría:

Los Estándares definen requisitos obligatorios para la auditoría de SI y el informe correspondiente. Informan a:
– Los auditores de SI respecto al nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA
– La dirección y a demás interesados en las expectativas de la profesión con respecto al trabajo de sus profesionales
– Los poseedores del Certificado de Auditor de Sistemas de Información (Certified Information Systems Auditor™, CISA®) respecto a los requisitos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación de la conducta del poseedor del certificado CISA por parte de la Junta de Directores de ISACA o del comité apropiado de ISACA y, en última instancia, en sanciones disciplinarias.

Las Directrices proporcionan guías sobre la aplicación de los Estándares de Auditoría de SI. El auditor de SI debe considerarlas al determinar cómo lograr la implementación de los estándares, utilizar un buen juicio profesional en su aplicación y estar dispuesto a justificar cualquier desviación de las mismas. El objetivo de las Directrices de Auditoría de SI es proporcionar mayor información con respecto al cumplimiento de los Estándares de Auditoría de SI.

Los Procedimientos proporcionan ejemplos de procedimientos que podría seguir un auditor de SI en el curso de una auditoría. Los documentos sobre procedimientos proporcionan información sobre cómo cumplir con los estándares al realizar trabajos de auditoría de SI, pero no establecen los requisitos correspondientes. El objetivo de los Procedimientos de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Objetivos de Control para Información y Tecnología Relacionada (*Control Objectives for Information and related Technology,* COBIT®) es un marco de referencia de dirección de tecnología de información (TI) y conjunto herramientas de apoyo que permite a los gerentes superar las diferencias entre los requisitos de control, cuestiones técnicas y riesgos del negocio. COBIT permite un desarrollo claro de políticas y buenas prácticas para el control de TI a lo largo de organizaciones. Enfatiza el cumplimiento normativo, ayuda a las organizaciones a aumentar el valor obtenido a partir de TI, permite el alineamiento y simplifica la implementación de los conceptos de la estructura COBIT.

COBIT está destinado a ser utilizado por la gerencia de la empresa y por la gerencia de TI, así como por los auditores de SI; por lo tanto, su uso permite la comprensión de los objetivos del negocio, la comunicación de las mejores prácticas y las recomendaciones que deben hacerse, en base a una estructura comúnmente comprendida y bien respetada. COBIT está disponible para su descarga del sitio Web de ISACA: *www.isaca.org/cobit*. Tal como se define en la estructura de COBIT, cada uno de los siguientes productos y/o elementos está organizado de acuerdo con el proceso de administración/gestión de TI:

- Objetivos de control—Declaraciones genéricas de un mínimo buen control en relación con los procesos de TI
- Directrices de gestión—Guías sobre evaluación y mejora de ejecución del proceso de TI, utilizando modelos de madurez, cuadros RACI (quién es Responsable de, quién rinde cuentas A, a quién se le Consulta y/o a quién se le Informa), metas y métricas. Proporcionan un marco de referencia de gestión orientado hacia una continua y proactiva auto-evaluación del control, enfocada específicamente en:
  - Medición del rendimiento/desempeño
  - Perfil de control de TI
  - Concienciación
  - benchmarking
- *Prácticas de control de COBIT*—Declaraciones de riesgo y valor y guías sobre 'cómo implementar' los objetivos de control
- *Guía de garantía de TI*—Guías para cada área de control sobre cómo obtener un entendimiento, juzgar cada control, evaluar su conformidad y validar el riesgo de que los controles no se cumplan

El glosario de términos se encuentra en el sitio web de ISACA *www.isaca.org/glossary*. Las palabras "auditoría" y "revisión" se usan de manera indistinta en los Estándares, las Directrices y los Procedimientos de Auditoría de SI.

Límite de responsabilidad: ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado satisfactorio. La publicación no debe considerarse como incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, el profesional de control debe utilizar su buen juicio profesional a las circunstancias de control específicas presentadas por el entorno particular de sistemas o de tecnologías de información.

La Junta de Estándares de ISACA tiene el compromiso de realizar consultas extensas al preparar los Estándares, las Directrices y los Procedimientos de Auditoría de SI. Antes de emitir cualquier documento, la Junta de Estándares emite borradores de los mismos y los expone a nivel internacional para recibir comentarios del público en general. La Junta de Estándares también busca personas con habilidad o interés especial en el tema bajo consideración para consultarlos, cuando

sea necesario. La Junta de Estándares tiene un programa de desarrollo permanente y agradece los comentarios de los miembros de ISACA y de otras partes interesadas para identificar temas emergentes que requieran estándares nuevos. Toda sugerencia se deberá enviar por correo electrónico a (*standards@isaca.org*), por fax a (+1.847.253.1443) o por correo (dirección al final del documento) a la Sede Internacional de ISACA, a la atención del director de estándares de investigación y relaciones académicas. Este material fue emitido el 1 de diciembre de 2007.

S15 Controles de TI

Introducción

01 Los estándares de ISACA contienen principios básicos y obligatorios, así como procedimientos esenciales, identificados con letra negrita, junto con la documentación relacionada.

02 El propósito de este estándar de ISACA es el de establecer normas y proporcionar guías relativas a los controles de TI.

Estándar

03 El auditor de SI debe evaluar y supervisar los controles de TI que son parte integral del entorno de control interno de la organización.

04 El auditor de SI debe asistir a la gerencia proporcionando consejos con respecto al diseño, la implementación, la operación y la mejora de controles de TI.

Comentario

05 La gerencia es responsable del entorno de control interno de una organización, incluidos los controles de TI. Un entorno de control interno proporciona la disciplina, el marco de referencia y la estructura para lograr el objetivo principal del sistema de control interno.

06 COBIT define el control como 'las políticas, procedimientos, prácticas y estructuras organizativas diseñadas para proporcionar una garantía razonable de que se lograrán los objetivos del negocio, y que los eventos indeseados serán prevenidos o detectados y corregidos'. Además, COBIT define un objetivo de control como 'una declaración del resultado deseado o propósito que debe lograrse al implementar procedimientos de control en un proceso en particular'.

07 Los controles de TI están compuestos por controles generales de TI, que incluyen controles transversales, controles detallados y controles de aplicación, referidos a controles sobre la adquisición, implementación, entrega y soporte a los sistemas y servicios de TI.

08 Los controles generales de TI son controles que minimizan el riesgo en el funcionamiento general de los sistemas e infraestructura de TI de la organización, y un extenso conjunto de soluciones automatizadas (aplicaciones).

09 Los controles de aplicación son un conjunto de controles incrustados dentro de las aplicaciones.

10 Los controles de TI transversales son controles generales de TI que están diseñados para administrar/gestionar y monitorizar el entorno de TI y, por tanto, afectan a todas las actividades relacionadas con TI. Son un subconjunto de controles generales TI enfocados en la administración/gestión y monitorización de TI.

11 Los controles detallados de TI están compuestos por controles de aplicación, más aquellos controles generales de TI no incluidos en controles transversales de TI.

12 El auditor de SI debe utilizar una técnica o enfoque apropiados de evaluación de riesgos al desarrollar el plan general de auditoría de SI, y al determinar prioridades para una asignación eficaz de los recursos de auditoría de SI, y para proporcionar una garantía con respecto al estado de los procesos de control de TI. Los procesos de control son las políticas, procedimientos y actividades

que forman parte de un entorno de control, diseñados para asegurar que los riesgos se mantienen dentro de los niveles de tolerancia establecidos por el proceso de administración/gestión de riesgos.
13 El auditor de SI debe considerar la utilización de técnicas de análisis de datos, incluida la utilización de una garantía continua, que permita a los auditores de SI monitorizar la fiabilidad del sistema de forma continua y, recoger evidencias selectivas de auditoría por medio del ordenador/computadora al revisar los controles de TI.
14 Cuando las organizaciones utilizan a terceros, éstos pueden convertirse en un componente clave de los controles de la organización y su logro de objetivos de control relacionados. El auditor de SI debe evaluar el rol que el tercero desempeña en relación con el entorno de TI, los controles relacionados y los objetivos de control de TI.
15 La siguiente guía de ISACA y de IT Governance Institute® (ITGI™) debe consultarse para obtener mayor información sobre los controles de TI:

- Guía GF3 Utilización de técnicas de auditoría asistida por ordenadores/computadoras (Computer- Assisted Audit Techniques, CAAT)
- Guía G11 El efecto de los controles transversales de SI
- Guía G13 Uso de la evaluación de riesgos en la planificación de la auditoría
- Guía G15 Planificación
- Guía G16 Efecto de terceros en los controles de TI de una organización
- Guía G20 Preparación de informes
- Guía G36 Controles biométricos
- Guía G38 Controles de acceso
- Marco de referencia COBIT y objetivos de control

Fecha de Vigencia

16 Este estándar de ISACA entrará en vigor para las auditorías de sistemas de información que comiencen a partir del 1 de febrero de 2008.

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 EE.UU.
Teléfono: +1.847.253.1545
Fax: +1.847.253.1443
Correo electrónico: *standards@isaca.org*
Sitio web: *www.isaca.org*

COMERCIO ELECTRONICO DOCUMENTO S16

La naturaleza especializada de la auditoría a los sistemas de información (SI), así como las habilidades necesarias para ejecutarla, requiere de estándares que sean específicamente aplicables a la auditoría de SI. Uno de los objetivos de ISACA® es promover estándares globalmente aplicables para cumplir con su visión. El desarrollo y difusión de los Estándares de Auditoría de SI son una piedra angular de la contribución profesional de ISACA a la comunidad de auditoría. La estructura de los Estándares de Auditoría de SI brinda múltiples niveles de asesoría:

Los Estándares definen requisitos obligatorios para la auditoría de SI y el informe correspondiente. Informan a:
– Los auditores de SI respecto al nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA
– La dirección y a demás interesados en las expectativas de la profesión con respecto al trabajo de sus profesionales
– Los poseedores del Certificado de Auditor de Sistemas de Información (Certified Information Systems Auditor™, CISA®) respecto a los requisitos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación de la conducta del poseedor del certificado CISA por parte de la Junta de Directores de ISACA o del comité apropiado de ISACA y, en última instancia, en sanciones disciplinarias.

Las Directrices proporcionan guías sobre la aplicación de los Estándares de Auditoría de SI. El auditor de SI debe considerarlas al determinar cómo lograr la implementación de los estándares, utilizar un buen juicio profesional en su aplicación y estar dispuesto a justificar cualquier desviación de las mismas. El objetivo de las Directrices de Auditoría de SI es proporcionar mayor información con respecto al cumplimiento de los Estándares de Auditoría de SI.

Los Procedimientos proporcionan ejemplos de procedimientos que podría seguir un auditor de SI en el curso de una auditoría. Los documentos sobre procedimientos proporcionan información sobre cómo cumplir con los estándares al realizar trabajos de auditoría de SI, pero no establecen los requisitos correspondientes. El objetivo de los Procedimientos de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

Objetivos de Control para Información y Tecnología Relacionada (*Control Objectives for Information and related Technology,*COBIT®) es un marco de referencia de dirección de tecnología de información (TI) y conjunto herramientas de apoyo que permite a los gerentes superar las diferencias entre los requisitos de control, cuestiones técnicas y riesgos del negocio. COBIT permite un desarrollo claro de políticas y buenas prácticas para el control de TI a lo largo de organizaciones. Enfatiza el cumplimiento normativo, ayuda a las organizaciones a aumentar el valor obtenido a partir de TI, permite el alineamiento y simplifica la implementación de los conceptos de la estructura COBIT.

COBIT está destinado a ser utilizado por la gerencia de la empresa y por la gerencia de TI, así como por los auditores de SI; por lo tanto, su uso permite la comprensión de los objetivos del negocio, la comunicación de las mejores prácticas y las recomendaciones que deben hacerse, en base a una estructura comúnmente comprendida y bien respetada. COBIT está disponible para su descarga del sitio Web de ISACA: *www.isaca.org/cobit*. Tal como se define en la estructura de COBIT, cada uno de los siguientes productos y/o elementos está organizado de acuerdo con el proceso de administración/gestión de TI:

- Objetivos de control—Declaraciones genéricas de un mínimo buen control en relación con los procesos de TI
- Directrices de gestión—Guías sobre evaluación y mejora de ejecución del proceso de TI, utilizando modelos de madurez, cuadros RACI (quién es Responsable de, quién rinde cuentas A, a quién se le Consulta y/o a quién se le Informa), metas y métricas. Proporcionan un marco de referencia de gestión orientado hacia una continua y proactiva auto-evaluación del control, enfocada específicamente en:
  - Medición del rendimiento/desempeño
  - Perfil de control de TI
  - Concienciación
  - Benchmarking
- Prácticas de control de COBIT—Declaraciones de riesgo y valor y guías sobre 'cómo implementar' los objetivos de control
- Guía de garantía de TI—Guías para cada área de control sobre cómo obtener un entendimiento, juzgar cada control, evaluar su conformidad y validar el riesgo de que los controles no se cumplan.

El glosario de términos se encuentra en el sitio web de ISACA *www.isaca.org/glossary*. Las palabras "auditoría" y "revisión" se usan de manera indistinta en los Estándares, las Directrices y los Procedimientos de Auditoría de SI.

Límite de responsabilidad: ISACA ha definido esta guía como el nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA. ISACA no pretende que el uso de este producto garantice un resultado satisfactorio. La publicación no debe considerarse como incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, el profesional de control debe utilizar su buen juicio profesional a las circunstancias de control específicas presentadas por el entorno particular de sistemas o de tecnologías de información.

La Junta de Estándares de ISACA tiene el compromiso de realizar consultas extensas al preparar los Estándares, las Directrices y los Procedimientos de Auditoría de SI. Antes de emitir cualquier documento, la Junta de Estándares emite borradores de los mismos y los expone a nivel internacional para recibir comentarios del público en general. La Junta de Estándares también busca personas con habilidad o interés especial en el tema bajo consideración para consultarlos, cuando

sea necesario. La Junta de Estándares tiene un programa de desarrollo permanente y agradece los comentarios de los miembros de ISACA y de otras partes interesadas para identificar temas emergentes que requieran estándares nuevos. Toda sugerencia se deberá enviar por correo electrónico a (standards@isaca.org), por fax a (+1.847.253.1443) o por correo (dirección al final del documento) a la Sede Internacional de ISACA, a la atención del director de estándares de investigación y relaciones académicas. Este material fue emitido el 1 de diciembre de 2007.

S16 Comercio electrónico

Introducción

01 Los estándares de ISACA contienen principios básicos y procedimientos esenciales, identificados con letra negrita, que junto con la documentación relacionada son obligatorios.

02 El propósito de este estándar de ISACA es el de establecer normas y proporcionar guías relativas a la revisión de entornos de comercio electrónico.

Estándar

03 El auditor de SI debe evaluar los controles aplicables, y cotejar los riesgos al revisar entornos de comercio electrónico, para asegurar que las transacciones de comercio electrónico están correctamente controladas.

Comentario

04 El comercio electrónico se define como aquellos procesos, a través de los cuales, las organizaciones realizan negocios por medios electrónicos con sus clientes, proveedores y otros socios comerciales externos, utilizando Internet como una tecnología habilitadora. Por lo tanto, incluye modelos de comercio electrónico de negocio a negocio (B2B), y de negocio a consumidor (B2C).

05 El auditor de SI debe utilizar una técnica o enfoque apropiado de evaluación de riesgos para desarrollar el plan general de auditoría de SI debe cubrir los entornos de comercio electrónico**.**

06 El auditor de SI debe considerar la utilización de técnicas de análisis de datos, incluida la utilización de una garantía continua, que permita a los auditores de SI monitorizar la fiabilidad del sistema de forma continua, y recoger evidencias selectivas de auditoría por medio del ordenador/computadora, al revisar las actividades de comercio electrónico.

07 El nivel de habilidad y conocimiento requerido, para comprender las implicaciones de control y administración/gestión de riesgos del comercio electrónico, varía con la complejidad de las actividades de comercio electrónico de la organización.

08 El auditor de SI debe comprender la naturaleza y la criticidad del proceso del negocio soportado por la aplicación de comercio electrónico antes de comenzar la auditoría, de modo que los resultados puedan evaluarse en el contexto apropiado.

09 Debe consultarse la guía siguiente para obtener mayor información con respecto al comercio electrónico:

• Guía G21 Revisión de sistemas de planificación de recursos empresariales (Enterprise Resource Planning, ERP)
• Guía G22 Revisión de comercio electrónico del negocio al consumidor (B2C)
• Guía G24 Banca en Internet
• Guía G25 Revisión de redes privadas virtuales (Virtual Private Networks, VPN)

• Guía G33 Consideraciones generales respecto al uso de Internet
• Procedimiento P6 Cortafuegos (firewalls)
• Marco de referencia COBIT y objetivos de control

Fecha de Vigencia

10 Este estándar de ISACA entrará en vigor para las auditorías de sistemas de información que comiencen a partir del 1 de febrero de 2008.

ISACA 3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 EE.UU.
Teléfono: +1.847.253.1545
Fax: +1.847.253.1443
Correo electrónico: *standards@isaca.org*
Sitio web: *www.isaca.org*