AUDITORÍA SUPERIOR
CHIHUAHUA

GUÍA DE LA AUDITORÍA DE TECNOLOGÍAS DE INFORMACIÓN

Índice

ANEXOS

Diagrama de Flujo de la Auditoría de Tecnologías de Información

I. GENERALIDADES DE LA GUÍA DE AUDITORÍA DE TECNOLOGÍAS DE INFORMACIÓN

I. GENERALIDADES DE LA GUÍA DE AUDITORÍA DE TECNOLOGÍAS DE INFORMACIÓN

I.1. Antecedentes

La Auditoría Superior del Estado es el Órgano del Poder Legislativo del Estado de Chihuahua que por disposición de la Constitución Estatal y de conformidad con la ley que la crea, tiene la función de auditar el ingreso y la aplicación de los recursos públicos de los tres poderes de Gobierno del Estado, los Ayuntamientos, los organismos que por disposición constitucional estén dotados de autonomía, los organismos públicos descentralizados, empresas de participación y fideicomisos de la administración pública o privada, que reciba, maneje, recaude o administre recursos públicos, con la finalidad de coadyuvar al desarrollo permanente de la eficiencia, eficacia, economía y transparencia de la gestión pública.

La fiscalización de los recursos públicos debe realizarse desde el punto de vista financiero, contable, presupuestal, técnico de obra, legalidad y de gestión; la revisión de las cuentas públicas se realizaba de manera bidireccional, es decir solo desde el punto de vista financiero y de obra, lo que ocasionaba que la gestión gubernamental dejara de ser evaluada bajo la óptica de otras varias disciplinas para cumplir con mayor eficiencia la función que nos han encomendado, es indispensable incorporar en los procesos de auditoría, disciplinas tales como: Tecnologías de la Información, Ambiental, Legalidad y Desempeño, logrando así que el recurso público sea auditado y fiscalizado bajo la perspectiva multidisciplinaria, dando pauta a la fiscalización multidireccional.

Con el modelo multidireccional que la Auditoría Superior del Estado de Chihuahua está implementando para desarrollar su facultad de fiscalización de la cuenta pública, incorpora el área de auditoría de tecnologías de información, en donde una de las funciones de ésta área, es conocer la situación en la cual se encuentran las tecnologías de información de los entes públicos.

El área de auditoría de tecnologías de información tiene como uno de sus objetivos; promover y elevar la cultura del aprovechamiento en el uso de las tecnologías de información en los entes a fiscalizar, constatando que se lleven a cabo las mejores prácticas y se sigan los procedimientos que aseguren la veracidad, confidencialidad, confiabilidad y disponibilidad de la información, garantizando de esta manera la prevención ante posibles contingencias que puedan impedir la continuidad del uso de los recursos informáticos.

Realizar las actividades correspondientes a la verificación de los controles internos establecidos en el área de sistemas, así como el estudio de seguridad física y lógica, el análisis de los riesgos a que está expuesta la información y los equipos de cómputo.

Para el cumplimiento de los objetivos contenidos en sus planes y programas, el artículo 11 fracción XIV de la Ley de Auditoría Superior del Estado de Chihuahua; cita "Artículo 11. Son facultades del Auditor Superior del Estado de Chihuahua" fracción XIV "establecer las reglas técnicas, procedimientos, métodos y sistemas de contabilidad y de archivo de los libros y documentos justificativos y comprobatorios del ingreso y del gasto público, así como todos aquellos elementos que permitan la práctica idónea de las auditorías y revisiones".

I.2. Marco Legal

En este punto se describen la regulación y las mejores prácticas de Auditoría en Informática sobre la administración de los riesgos en la misma, en base a los organismos nacionales e internacionales, las cuales se han convertido en una pauta a seguir por diversos organismos.

En este capítulo se abordan las principales leyes existentes en materia informática así como las mejores prácticas que pueden ser aplicadas en el sector público o privado o cualquier organización que utilice la auditoría informática.

I.2.1 Legislación e instituciones nacionales

El Código Penal de la Federación, en el título noveno Revelación de secretos y acceso ilícito a sistemas y equipos de informática establece lo siguiente:

TÍTULO NOVENO

Revelación de secretos y acceso ilícito a sistemas y equipos de informática

CAPITULO I
Revelación de secretos

Artículo 210.- Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.

Artículo 211.- La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial.

Artículo 211 Bis.- A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada,

se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

Capítulo II
Acceso ilícito a sistemas y equipos de informática

Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución

de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por

algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 6.- Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

Artículo 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

Instituto Mexicano de Auditores Internos, IMAI

Dedicado a la capacitación e investigación en de Auditoría Interna y Control.

De acuerdo al IMAI su misión es "promover el mejoramiento constante de la Práctica Profesional de la Auditoría Interna, para fortalecer el prestigio de esta profesión y de quienes la practican".

Marco jurídico que sirve de referencia para la realización de pruebas sustantivas y de cumplimiento, entre otras disposiciones legales, son las siguientes:

- Constitución Política de los Estados Unidos Mexicanos
- Constitución Política del Estado de Chihuahua
- Ley Orgánica del Poder Ejecutivo del Estado de Chihuahua
- Ley de Entidades Para Estatales del Estado de Chihuahua
- Ley de la Auditoría Superior del Estado de Chihuahua
- Código Municipal del Estado de Chihuahua
- Presupuestos de Egresos de Gobierno del Estado y sus Municipios
- Ley de Ingresos de Gobierno del Estado y sus Municipios

I.2.2 Legislación e instituciones internacionales

INTOSAI

ISSAI 5310 – Information System Security Review Methodology (Directriz sobre el Control de Sistemas de Seguridad de la Tecnología de Información)

Institute of System Audit and Association, ISACA

Asociación de Auditoría y Control de Sistemas de Información, lleva a cabo proyectos de investigación de gran escala para expandir los conocimientos y el valor del campo de gobernación y control de TI.

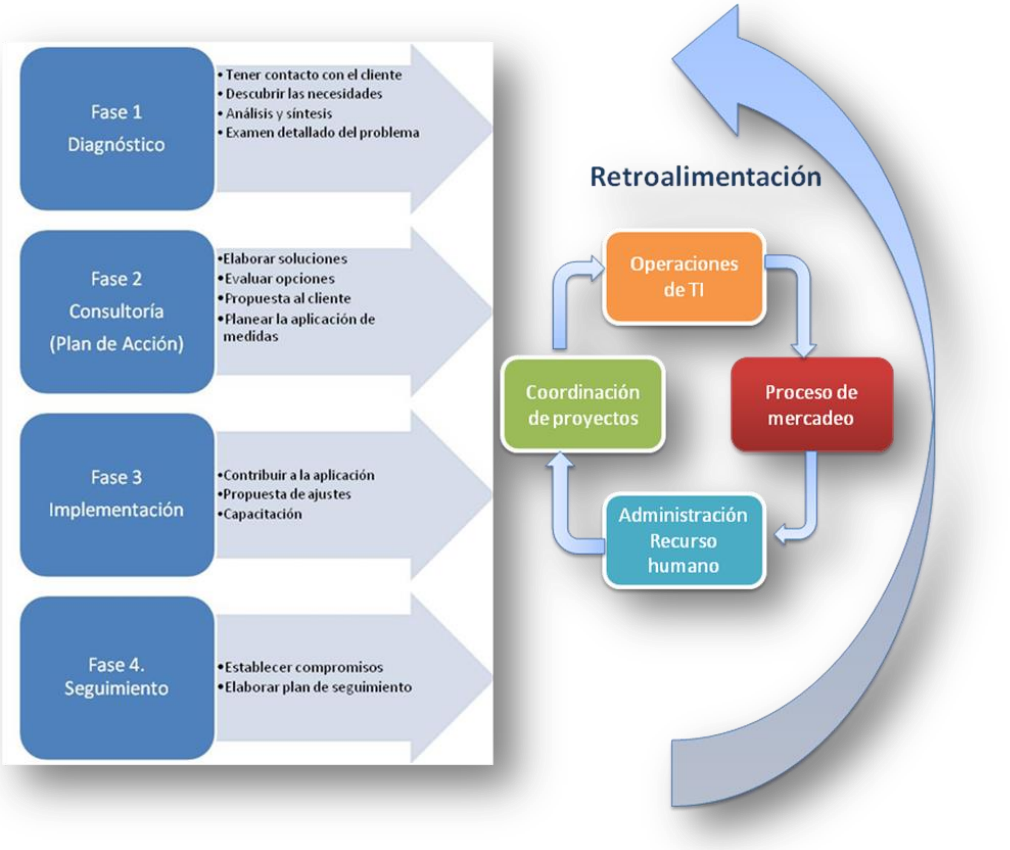
Institute of Internal Auditors, IIA

Organización profesional, reconocida mundialmente como una autoridad, pues es el principal educador y el líder en la certificación, la investigación y la guía tecnológica en la profesión de la auditoría interna.

Control Objectives for Information and related Technology, COBIT

Herramienta que permite evaluar la calidad del soporte de TI actual de la organización, vinculando los distintos procesos del negocio con los recursos informáticos que los sustentan.

Figura 1. Estructura del marco de control COBIT.



BS 7799 e ISO 17799

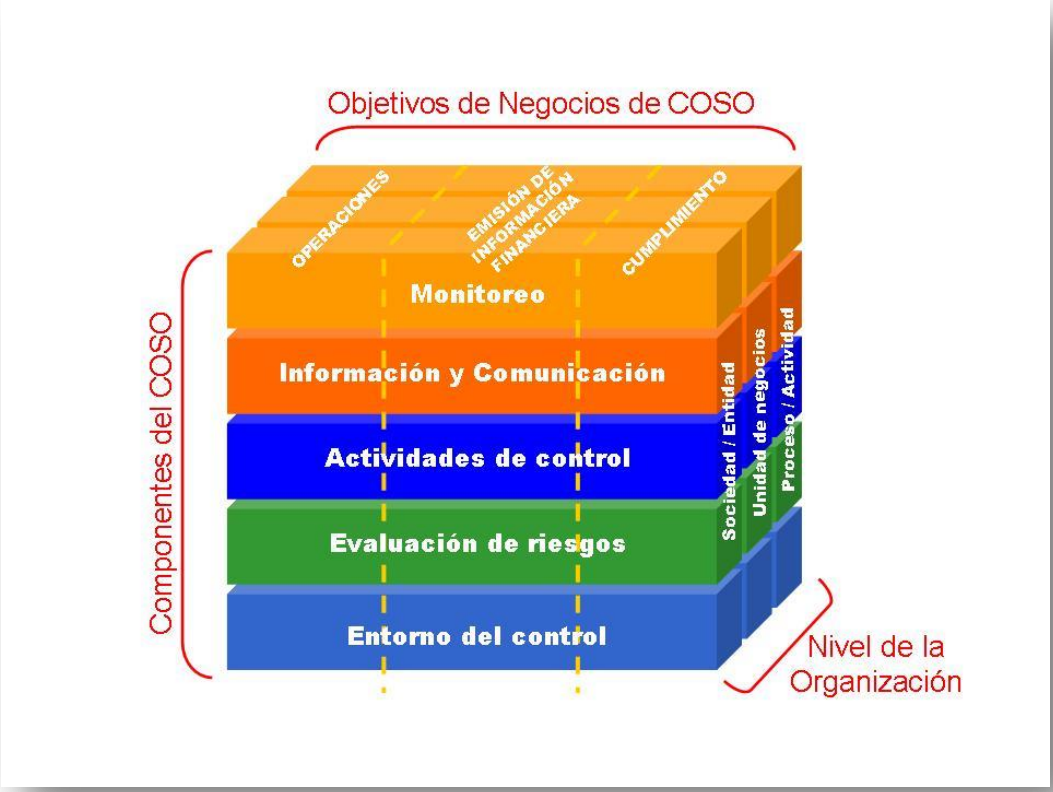
British Standard Institute (BSI) publica la norma BS 7799, un código de buenas prácticas para la gestión de la seguridad de la información. En 1998 también el BSI publica la norma BS 7799-2 con especificaciones para los sistemas de gestión de la seguridad de la información. Actualmente las empresas deben asegurar que sus recursos y la propiedad intelectual estén protegidos.

Committee of Sponsoring Organizations, COSO

Marco de control interno que plantea el informe COSO consta de cinco componentes interrelacionados, derivados del estilo de la dirección, e integrados al proceso de gestión:

- Ambiente de control
- Evaluación de riesgos
- Actividades de control
- Información y comunicación
- Supervisión

Figura 2. Cubo de los procesos y actividades del COSO



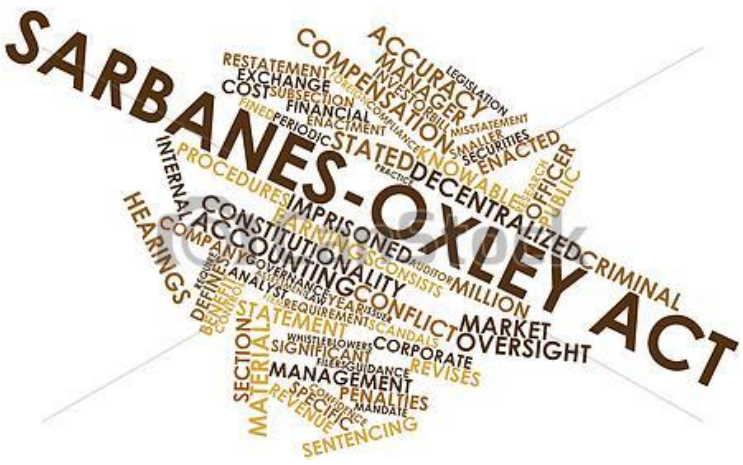
Metodología de análisis y gestión de riesgos de los sistemas de información, MAGERIT

Esta metodología presenta un objetivo definido en el estudio de los riesgos que afectan los sistemas de información y el entorno de ellos haciendo recomendaciones de las medidas apropiadas que deberían adoptarse para conocer, prevenir, evaluar y controlar los riesgos investigados.

Sarbanes-Oxley, SOX

Actualmente las organizaciones están expuestas a ataques que propicien la pérdida de información y fraudes, para minimizar los riesgos de fraude, las empresas se requieren revisar, evaluar y fortalecer sus propios controles internos.

La ley Sarbanes-Oxley, emitida por el gobierno estadounidense el 30 de julio de 2002, fue preparada a partir de los escándalos financieros de los últimos años y establece una serie de nuevos requisitos tanto para las empresas estadounidenses como para las extranjeras, tenedoras y subsidiarias, que cotizan en la bolsa de valores estadounidense (New York Stock Exchange, NYSE), con la idea de regular el gobierno corporativo.



Normas Internacionales de Auditoría, NIA

Emitidas por el International Federation of Accountans (IFAC) a través del International Auditing and Assurance Standars Boards (IAASB). Son los requisitos mínimos de calidad relativos a la personalidad del auditor, al trabajo que desempeña y a la información que rinde como resultado de dicho trabajo.

Figura 3. Estructura general de las normas internacionales de auditoria

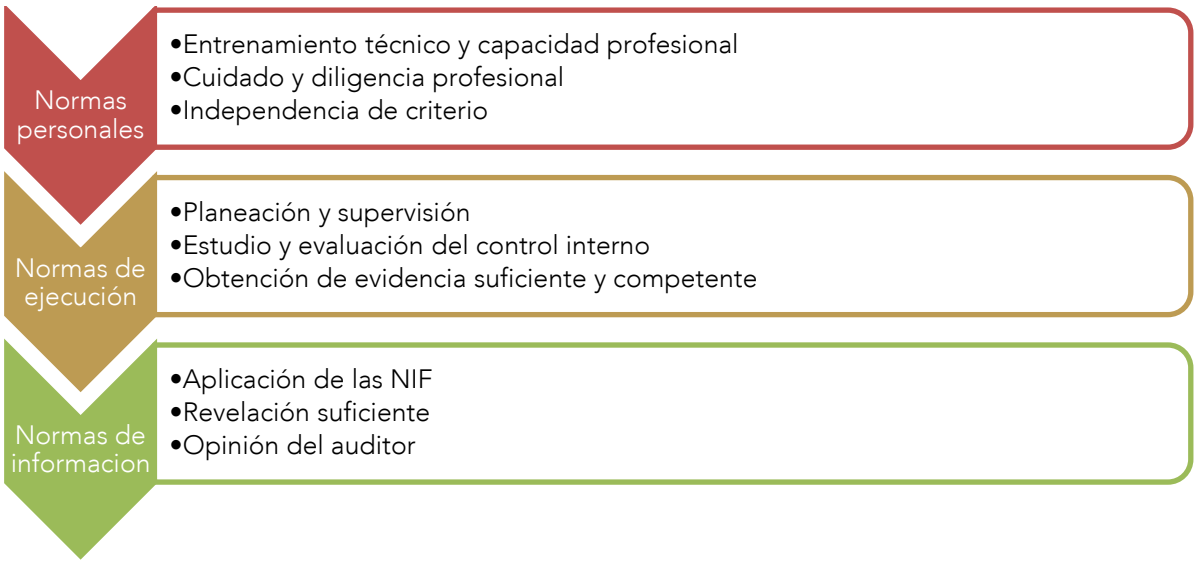
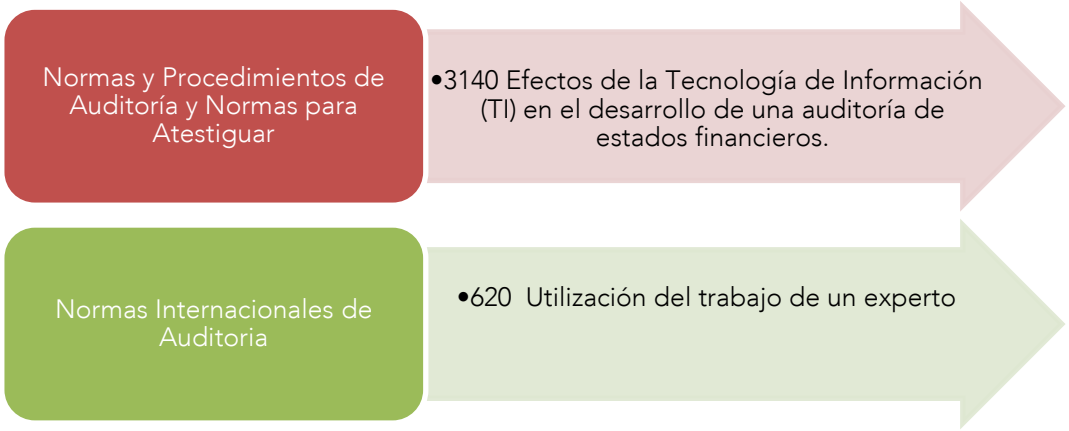


Figura 4. Normas donde se mencionan los expertos para las revisiones.



I.3. Objetivos de la Guía

Son objetivos de la presente Guía:

a. Establecer los Procedimientos que faciliten la realización de la auditoría de tecnologías de información
b. Establecer los procedimientos que permitan interactuar con las diversas áreas de la Auditoría Superior.
c. Estandarizar los procedimientos y alcances en la práctica de la auditoría de tecnologías de información.
d. Garantizar a los entes fiscalizables que la actuación de la Auditoría Superior del Estado en la auditoría de tecnologías de información se regirá, entre otros por lo principios de: Igualdad, Imparcialidad, Buena Fe, Transparencia y Confiabilidad.

I.4. Campo de Aplicación de la Guía

Esta guía se realizó para uso de la Auditoría Superior del Estado de Chihuahua, para su aplicación en el universo de entes públicos sujetos a auditar en el Estado, mismos que apliquen recursos públicos de manera directa e indirecta en acciones tecnológicas; así como en sus diferentes áreas, programas, planes, proyectos, operaciones y resultados que se generen en el proceso de gestión informática, y en sus aspectos administrativos, financieros y técnicos.

I.5. Alcance de la Guía

La presente guía está dirigida a los auditores de la Auditoría Superior que realicen funciones de auditoría de tecnologías de información a los diferentes entes públicos de la administración central, descentralizada ya sea estatal y municipal, autónomos,

fideicomisos y personas físicas o morales que manejen, recauden o administren recursos públicos. Además, el desarrollo de los procesos generales establecidos en la presente guía es de aplicación general y flexible de acuerdo a la naturaleza del ente.

I.6. Metodología Utilizada en la Elaboración de la Guía

La guía de auditoría de tecnologías de información, se nutre entre otros de los resultados y experiencias de los procedimientos de auditoría y acciones tecnológicas realizados en el ejercicio anterior y de la normatividad antes mencionada.

Para la elaboración de la presente guía, se consideraron los siguientes puntos:

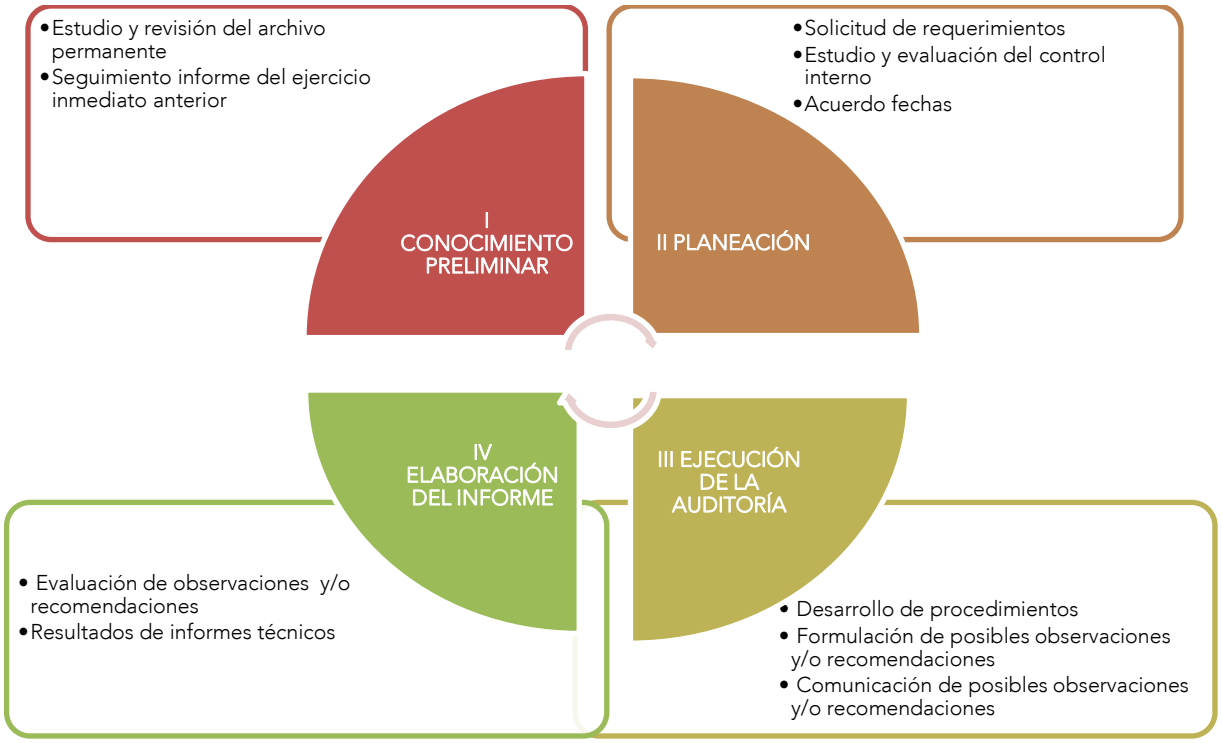
a. Planear: se convocó a un grupo de auditores involucrados en la ejecución de auditorías de tecnologías de información para evaluar y mejorar la metodología utilizada en esta área, para lo cual se recopiló información en la materia con los entes auditados, así como de procedimientos aplicables en otros países en relación a auditorías a las tecnologías de información.
b. Organizar: una vez concluida la fase de planeación, se define el plan de trabajo y los aspectos a considerar para el proceso de la auditoría, se procedió a elaborar la presente guía.
c. Verificar: se remitió el documento de trabajo al personal involucrado en el proceso de auditoría de tecnologías de información, a fin de que se comente y determine el contenido de la presente guía y se aporte un producto útil para la ejecución de las auditorías.
d. Control: con el propósito de evaluar y encontrar áreas de oportunidad para la mejora en los distintos procesos considerados en esta metodología, se procede a revisar anualmente los aspectos considerados en la "Guía de Auditoría de Tecnologías de Información"

La presente guía ha sido redactada bajo el *enfoque de procesos*, presentando el desarrollo de una secuencia lógica de actividades para la obtención de un producto final, el mismo que proporcionará información sobre posibles efectos tecnológicos.

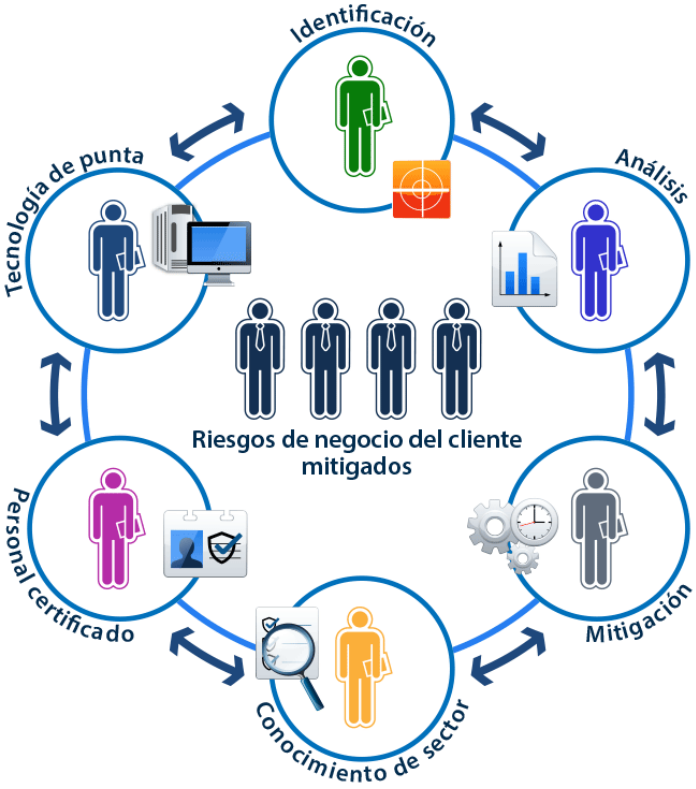
Las cuatro etapas del proceso de revisión de la auditoría de tecnologías de información son:

I. *El conocimiento preliminar*
II. *La planeación*
III. *Ejecución de la auditoría*
IV. *La elaboración del informe*

Figura 6. Desarrollo del Proceso de la auditoría de tecnologías de información



II. AUDITORÍA DE TECNOLOGÍAS DE INFORMACIÓN



II. AUDITORÍA DE TECNOLOGÍAS DE INFORMACIÓN

II.1. Tipos de Auditoría de Tecnologías de Información

Llevar a cabo una auditoría de tecnologías de información requiere un mínimo de conocimientos sobre temas tecnológicos y sus impactos.

Existen diferentes tipos de auditorías:

- Al ciclo de vida de sistemas
- A un sistema en operación
- A controles generales del computador
- A la administración de la función informática
- Auditoría a las microcomputadoras aisladas
- Auditoría de redes

Auditorías en las que pueden abordarse temas tecnológicos

1. **En la Auditoría financiera o de estados contables**, pueden incluirse, entre otros, los siguientes asuntos informáticos:

- Iniciativas para prevenir, disminuir o remediar daños a la información.
- La aplicación de recursos informáticos aprobados en los presupuestos correspondientes.
- Automatización de pruebas sustantivas.

2. **En la Auditoría de Normatividad**, los criterios que utilice el auditor deben ayudar a determinar si la entidad ha ejecutado las actividades relacionadas con el cuidado de los recursos informáticos. La auditoría de normatividad, en el contexto informático se encargará de evaluar:

- La verificación del cumplimiento normativo de aplicación a lo tecnológico.

II.2. Consideraciones para Establecer el Área de Auditoría de Tecnologías de Información

La Informática en la actualidad, está subsumida en la gestión integral de las organizaciones, por eso las normas y estándares propiamente informáticos deben estar, por lo tanto, sometidos a los estándares generales de la misma. En consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado gestión de la organización.

La Informática no gestiona propiamente a la organización, ayuda a la toma de decisiones, pero no decide por sí misma. Por ende, debido a su importancia en el funcionamiento de la misma, existe la *Auditoría Informática o de tecnologías de información*. Las organizaciones acuden a las auditorías externas e internas cuando existen síntomas perceptibles de debilidad. Estos pueden agruparse en clases:

a. Síntomas de descoordinación y desorganización:

- No coinciden los objetivos de la gerencia de TI con los de la propia organización.
- Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente.

b. Síntomas de mala imagen e insatisfacción de los usuarios:

- No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios de software en los terminales de usuario, variación de los archivos que deben ponerse diariamente a su disposición, etc.
- No se reparan las averías de hardware ni se resuelven incidencias en plazos razonables. El usuario percibe que está abandonado y desatendido permanentemente.
- No se cumplen en todos los casos los plazos de entrega de resultados periódicos. Pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario, en especial en los resultados de aplicaciones críticas y sensibles.

c. Síntomas de debilidades económico-financieras:

- Incremento desmesurado de costos.
- Necesidad de justificación de inversiones informáticas.
- Desviaciones presupuestarias significativas.
- Costos y plazos de nuevos proyectos.

d. Síntomas de Inseguridad:

- Evaluación de nivel de riesgos
- Seguridad lógica.
- Seguridad física.
- Confidencialidad.

II.3. Definición de Auditoría de Tecnologías de Información

Una auditoría a tecnologías de la información es un examen profesional, objetivo y sistemático de las operaciones y actividades efectuadas por una organización, proyecto o programa, para determinar el grado de cumplimiento y eficacia de:

- La planificación, el desarrollo y la implantación de los sistemas utilizados.
- La información producida por los sistemas, su pertinencia y confiabilidad.
- La documentación básica de cada sistema, su implantación y la divulgación de la misma entre los usuarios.
- Los mecanismos de control incorporados en los sistemas.
- Los recursos idóneos identificados y disponibles para garantizar la continuidad de las operaciones en caso de desastres.
- El programa de adiestramiento al personal de sistemas de información, sus usuarios y los auditores.

Entonces, se entiende por auditoría a tecnologías de la información a aquella actividad auditora que trata de evaluar la adecuada utilidad, eficiencia y fiabilidad de la información mecanizada que se produce en una determinada organización pública o privada, así como los servicios que la elaboran y procesan.

Engloba el análisis de la organización, seguridad, segregación de funciones y gestión de las actividades de proceso de datos.

II.4. Principios

La Auditoría Superior, en el ejercicio de sus atribuciones, se regirá por los principios de posterioridad, anualidad, legalidad, imparcialidad, eficiencia, eficacia, economía y transparencia.

a. Posterioridad: las acciones de la Auditoría se llevarán a cabo una vez que los entes públicos hayan presentado su cuenta pública anual, conforme lo establece la norma vigente aplicable.

b. Anualidad: el período de revisión debe estar acotado a un ejercicio fiscal de los entes, con salvedad de las hipótesis previstas en la propia normatividad.

c. Legalidad: la operación de los entes públicos se rige por la normatividad que establece el marco jurídico que le aplica.

d. Imparcialidad: las auditorías se realizarán a los entes públicos de una manera objetiva y veraz.

e. Eficacia: capacidad de lograr los objetivos y metas programadas con los recursos disponibles en un tiempo predeterminado.

f. Eficiencia: uso racional de los medios con que se cuenta para alcanzar un objetivo predeterminado; es el requisito para evitar o cancelar dispendios y errores.

g. Economía: la adquisición de bienes y servicios en mejores condiciones de precio, calidad, cantidad y oportunidad, así como la óptima aplicación de los recursos utilizados en la administración para la reducción al mínimo de los costos.

h. Transparencia: está referida a la difusión de la labor de auditoría, con la finalidad de sensibilizar y concientizar a funcionarios y pobladores sobre la necesidad de conservar el ambiente y propender a su desarrollo sostenible.

II.5. Objetivo de la Auditoría de Tecnologías de Información

II.5.1. Objetivo general

Promover y elevar la cultura del aprovechamiento en el uso de las Tecnologías de Información en los Entes a fiscalizar, constatando que se lleven a cabo las mejores prácticas y se sigan los procedimientos que aseguren la veracidad, confidencialidad, confiabilidad y disponibilidad de la información, garantizando de esta manera la prevención ante posibles contingencias que puedan impedir la continuidad del uso de los recursos informáticos.

Realizar las actividades correspondientes a la verificación de los controles internos establecidos en el área de Sistemas, así como el estudio de seguridad física y lógica, el análisis de los riesgos a que está expuesta la información y los equipos de cómputo.

II.5.2. Objetivos específicos

- Determinar la situación actual del área informática, las actividades y esfuerzos necesarios para lograr los objetivos propuestos.
- Minimizar existencias de riesgos en el uso de tecnología de información.
- Evaluar la dependencia de los sistemas y las medidas tomadas para garantizar su disponibilidad y continuidad.
- Revisar la seguridad de los entornos y sistemas.

- Evaluar la suficiencia y eficacia de los planes de contingencia.
- Analizar la garantía de calidad de los Sistemas de Información
- Brindar una opinión y recomendaciones sobre la utilización eficiente de los recursos informáticos.
- Analizar los controles y procedimientos tanto organizativos como operativos.
- Apoyar a las demás áreas de auditoría con la realización de pruebas sustantivas y de cumplimiento con el uso de las herramientas informáticas.

II.6. Características del Proceso de Auditoría

El proceso de auditoría debe cumplir las siguientes características:

a. Objetividad: el auditor debe contar con actitud mental independiente sin influencias personales, debiendo prevalecer en todo momento el juicio profesional para analizar, interpretar y evaluar el cumplimiento normativo y el registro de las operaciones realizadas.

b. Sistematicidad: porque a través de una metodología, se permite que el auditor exprese y sustente una opinión sobre la gestión desarrollada por la entidad.

c. Especialización: contando con los conocimientos en auditoría, tecnologías de información y disciplinas afines, respaldados por la experiencia.

d. Oportunidad: la ejecución de la auditoría, así como la presentación del Informe Técnico de Resultados, que integra las observaciones y recomendaciones al ente auditado, deberán presentarse en los tiempos establecidos por la Legislación aplicable.

III. GUÍA DE AUDITORÍA DE TECNOLOGÍAS DE INFORMACIÓN

III. GUÍA DE AUDITORÍA DE TECNOLOGÍAS DE INFORMACIÓN

La auditoría de tecnologías de información es un proceso que comprende cuatro fases: Conocimiento Preliminar, Planeación, Ejecución de la Auditoría y Elaboración del Informe de Resultados. Adicionalmente, se considera una fase de seguimiento posterior a la conclusión de la auditoría; tal como se muestra a continuación:

Figura 7. Proceso de auditoría de tecnologías de información

La secuencia del proceso de actividades que comprende cada fase, es flexible y aplicable de acuerdo a la naturaleza de la entidad, así como al plan, programa, proyecto, obra, actividad o problema informático que se va a auditar. El proceso completo de la auditoría se grafica en el **Anexo 1 "Diagrama de Flujo del Proceso de auditoría de tecnologías de información"**.

A continuación, se analiza cada fase del proceso de auditoría de tecnologías de información.

Enfoque metodológico

El enfoque metodológico propuesto integra el conocimiento aportado por las organizaciones que lideran el desarrollo de los estándares y mejores prácticas en el ámbito de las tecnologías de la información reconocidas a nivel internacional, entregando un marco referencial para realizar auditorías a las tecnologías de información centradas en los procesos de la organización, los sistemas de información que los soportan y sus actividades de control.

III.1. Conocimiento Preliminar

Es la fase inicial del proceso de auditoría de tecnologías de información, se considera el archivo permanente que contiene la información general para el estudio y comprensión de los entes a revisar en caso de que se hayan realizado auditorías en años anteriores, así como, revisar el informe del ejercicio anterior para darle seguimiento a las observaciones.

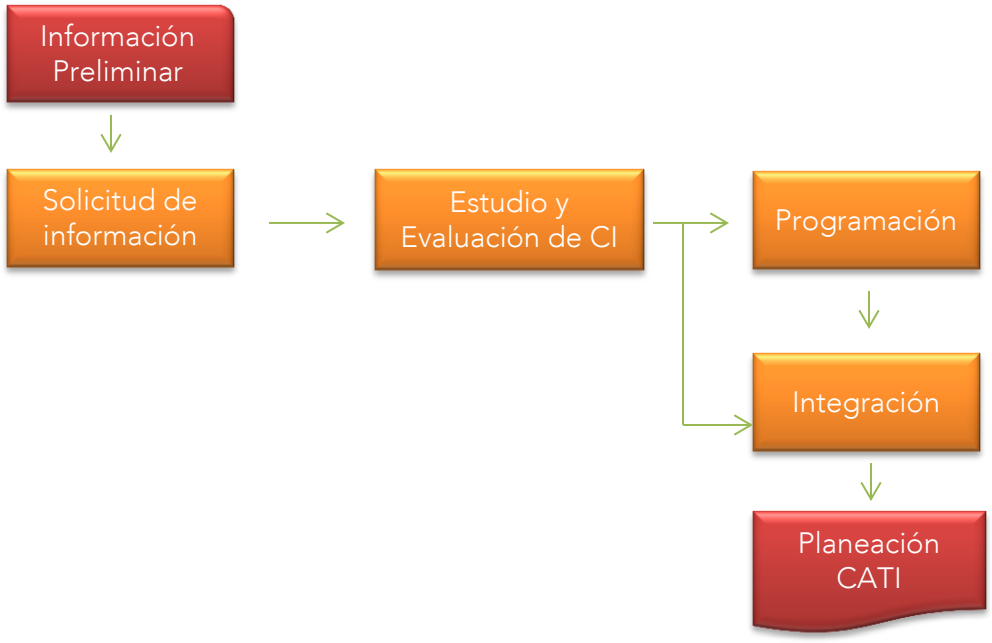
III.2. Planeación

La Planeación es la primera fase del proceso de auditoría, en ella se identifican las áreas críticas e información del área de tecnologías de información, a partir del cual se determina el alcance, procedimientos de revisión y el equipo auditor comisionado, con el propósito de definir los objetivos de auditoría teniendo como resultado la Planeación de la Auditoría.

Para el desarrollo de la planeación de auditoría de tecnologías de información, se deberán considerar el desarrollo de los siguientes procesos:

- Solicitud de información al área del Índice de Rendición de Cuentas (IRC) y validación de la misma.
- Estudio y evaluación del control interno en las áreas de tecnologías de información del ente a auditar, se aplica a través de la herramienta SIDATI.
- Solicitar información del contenido tecnológico mediante instrumentos de recopilación como son: cuestionarios, entrevistas, inspección, etc.
- Coordinarse con el resto de las áreas de la ASE a efecto de compartir información del tipo informática que éstas hayan considerado en sus procedimientos de revisión.
- Bases de datos de los sistemas a revisar.
- Procedimientos a revisar por las diferentes áreas de la ASE.
- Coordinación con el Síndico Municipal para el desarrollo de procedimientos técnicas e inspecciones de auditoría de tecnologías de información.

Figura 8. Proceso de planeación de la auditoría de tecnologías de información



III.2.1.1 Riesgo y materialidad de la auditoría

Se puede definir los riesgos de auditoría como aquellos riesgos de que la información pueda tener errores materiales o que el auditor de TI no pueda detectar un error que ha ocurrido. Los riesgos en auditoría pueden tener diversas clasificaciones.

El auditor puede llegar a la conclusión de que no existen errores materiales cuando en realidad los hay. La palabra material utilizada con cada uno de los riesgos evaluados, se refiere a un error que debe considerarse significativo cuando se lleva a cabo una auditoría. En una auditoría de TI, la definición de riesgos materiales depende del tamaño o importancia del objeto auditado así como de otros factores. El auditor de TI debe tener una cabal comprensión de los riesgos de auditoría al planificar.

Una auditoría tal vez no detecte cada uno de los potenciales errores en un universo, pero, sí el tamaño de la muestra es lo suficientemente grande, o se utilizan procedimientos estadísticos adecuados, se llega a minimizar la probabilidad del riesgo de detección.

De manera similar al evaluar los controles internos, el auditor de TI debe percibir que en un sistema dado se puede detectar un error mínimo, pero ese error combinado con otros, puede convertirse en un error material para todo el objeto auditado.

a. Técnicas de evaluación de riesgos

Al determinar que áreas funcionales o temas de auditoría que deben auditarse, el auditor de TI puede enfrentarse a una gran variedad de temas candidatos a ser auditados, el auditor debe evaluar esos riesgos y determinar cuáles de esas áreas de alto riesgo debe ser auditada.

b. Objetivos de controles y objetivos de auditoría

El objetivo de un control es anular el riesgo siguiendo alguna metodología, el objetivo de auditoría es verificar la existencia de estos controles y que estén funcionando de manera eficaz, respetando las políticas del ente y los objetivos del ente.

III.2.2. Solicitud de información

Este procedimiento deberá realizarse de manera formal utilizando las herramientas como son: oficios, cuestionarios, entrevistas, layouts, entre otros, con la finalidad de documentar y soportar la auditoría de tecnologías de información.

III.2.2.1. Documentación e información

a. **Normatividad:** los auditores, entes auditados y el mismo proceso de auditoría; están sometidos a un marco normativo que debe ser considerado a lo largo de toda la auditoría.

b. **Lineamientos** establecidos en la que contiene: el objetivo general, objetivos específicos, metas y acciones, número de integrantes, planeación general de la auditoría de tecnologías de información. A partir del plan se establece el personal responsable. Cualquier otra acción no contemplada en la planeación estratégica se adicionará a los procedimientos aplicables para su ejecución.

c. **Archivo Permanente:** está integrado por información general como es: ley orgánica o decreto de creación del ente, informes de auditorías y cédulas de

seguimiento, nombre del titular, domicilio, colindancia, teléfono, etc., normativa y documentos de gestión desarrollados por el ente auditado.

d. Información General: comprende el conocimiento del ente auditar, es decir, su naturaleza, actividades y operaciones, obtenido a partir de decreto de creación y regulación normativa que le aplique.

e. Antecedentes: incluye informes de auditorías anteriores, internos o externos, denuncias de ciudadanos por aspectos tecnológicos, requerimientos del titular de la ASE, así como cualquier otra documentación relacionada con la auditoría.

f. Restricciones: tales como personal, tiempos, disponibilidad de equipos, comunicaciones y otras que puedan interferir en la realización del proceso de planificación.

III.2.2.2. Procedimientos

El auditor de TI responsable, deberá incluir de manera escrita o medios magnéticos los métodos que utilizará para el desarrollo de los trabajos correspondientes de acuerdo con el programa detallado de actividades y los alcances definidos para la Auditoría.

a. Revisión del archivo permanente:

   De existir una auditoría realizada con anterioridad a la entidad o área a evaluar, se debe contar con un archivo permanente que contiene normas generales, específicas y documentos de gestión de la entidad que pueden ser revisados inicialmente como referencia. Es el archivo con los antecedentes que reflejan el estado de organización y funcionamiento de los procesos y sistemas auditados en una entidad. Este archivo contiene información de la organización que es poco cambiante y, por consiguiente, tiene validez continua a través del tiempo.

b. Reuniones interinstitucionales:

Como parte del ente público a auditar y de la problemática a ser considerada en el diagnóstico inicial, los auditores realizarán reuniones, de ser posible, con los funcionarios del ente, con el fin de conocer su forma de trabajo, establecer el contacto inicial con los responsables de área, con la finalidad de obtener una mayor eficiencia en la revisión.

c. Sistematización y búsqueda de la información:

Comprende la revisión de información que se obtiene a partir de publicaciones, estudios de investigación, Internet, sistemas de información y otras adicionales a la información obtenida del ente a auditar.

d. Análisis de hechos:

Para identificar el problema principal o área crítica objeto del desarrollo de la auditoría, es necesario que los auditores se basen en hechos y no se dejen guiar solamente por el sentido común, la experiencia o la habilidad; lo cual podría ocasionar un resultado contrario al esperado.

e. Levantamiento de la información básica y detallada:

El levantamiento de información que se realiza en esta etapa, tiene como finalidad asegurar que el auditor comprenda la filosofía y las características de funcionamiento de los procesos de negocio y sistemas de información en estudio. Esto es imperativo dentro del proceso de la auditoría, puesto que toda la pericia y el conocimiento técnico del auditor serían inaplicables si antes no obtiene la comprensión de aspectos claves del universo que será auditado.

Como resultado de esta actividad, el auditor obtiene la siguiente información:

1. *De los procesos de negocio*
    - Estructura organizacional.
    - Estructura de las áreas propietarias de la información de los procesos de negocio.
    - Clientes internos y externos.
    - Dependencias de la organización.
    - Tareas o actividades que realiza cada dependencia.
    - Terceros que intervienen en el manejo de la información.
    - Cuantificación de las cifras de operaciones que manejan los procesos de negocio (promedio durante un año).
    - Políticas y procedimientos establecidos en la organización relacionados con los procesos de negocio.
    - Normas legales e institucionales que rigen el funcionamiento del servicio.
    - Información sobre fraudes y otros antecedentes en las operaciones del servicio.

2. *De las tecnologías de información que soportan los procesos de negocio*
    - Funciones y operaciones del negocio que ejecutan los sistemas.
    - Modelo entidad/relación de las bases de datos de los sistemas.
    - Diccionario de datos de los modelos entidad/relación.
    - Inventario de documentos fuentes y otros medios de entrada de datos.
    - Personas claves que dan soporte técnico a la operación y mantenimiento de los sistemas para cada dependencia.
    - Terceros que prestan servicios de tecnologías de información para los procesos de negocio.

- Inventario de informes que producen los sistemas y destinatarios de los mismos.
- Interfaces entre sistemas (información que reciben o proporcionan a otros sistemas).
- Manuales existentes con la documentación técnica y del usuario.
- Plataforma en la que funcionan los sistemas de información (sistema operativo, software de desarrollo y motor de base de datos utilizados).
- Si el sistema de información fue adquirido; datos del proveedor, año de adquisición, versión en producción, cantidad de usuarios con licencia, poseen programas fuentes y contrato de mantención).
- Si el sistema de información fue desarrollado internamente (tipo de lenguaje utilizado, archivos fuentes y ejecutables, fecha de ingreso a producción, versión actual en producción).

f. Ficha técnica de los sistemas de información

La ficha técnica es un documento con el resumen gerencial de las principales características del proceso de negocio y de las tecnologías de información que soportan sus operaciones.

III.2.2.3. Resultados de la planeación

a. Diagnóstico de Materialidad en la Auditoría, según el punto III.2.1.1:

Documento donde los auditores responsables de la planeación efectúan un primer análisis de la problemática a ser evaluada, identificando las áreas de oportunidad, provenientes de la aplicación de las herramientas de identificación de problemas, de la revisión de la documentación y realización de las reuniones interinstitucionales. Este diagnóstico ayudará a identificar la problemática tecnológica del ente para establecer los procedimientos a aplicar. Dicho

documento es aprobado por el equipo supervisor e instancia superior correspondiente.

b. Determinación de áreas de oportunidad:

Los pasos anteriores ayudan a definir las unidades de la entidad y los temas de interés a ser examinados. Esto no exime la posibilidad de que el auditor revise otras áreas no consideradas en la planeación.

c. Información adicional:

Si existe la necesidad de información complementaria se procede a requerirla de manera formal, utilizando medios telefónicos y correo electrónico. Asimismo, a través de la ASE mediante formatos internos de requerimientos del Índice de Rendición de Cuentas (IRC).

d. Inspecciones:

Extraordinarias: igualmente y solo de ser necesario, el auditor responsable de la planeación elaborará un documento proponiendo y justificando estas visitas, dicho documento deberá contener como mínimo lo siguiente:

- Justificación: la necesidad de la realización de la inspección.
- Objetivo: qué se desea obtener como resultado de la inspección.
- Puntos de interés: qué se requiere revisar durante la inspección.
- Actividades: rutas, tiempos, responsables etc.
- Necesidades: movilidad, equipos logísticos, costos (viáticos en el caso de realizarse fuera del ámbito geográfico de la entidad auditora).

El documento final será remitido a la instancia superior correspondiente para su aprobación y posterior archivo en los papeles de trabajo de la fase de planeación.

III.2.3. Estudio y evaluación del control interno

El estudio y evaluación del control interno se efectuará con el objeto de cumplir con la norma de ejecución del trabajo que requiere el auditor, que le sirva de base y determine el grado de confianza que va a depositar sobre el control interno y que esto le permita determinar la naturaleza, el alcance y la oportunidad en los procedimientos de auditoría.

Esta etapa tiene como objetivos conocer y comprender el ambiente de organización, tecnológico y operativo de los procesos de negocio y los sistemas de información que los soportan. Implica para el auditor realizar un levantamiento de la información detallada a través de entrevistas con las personas apropiadas, de observación de la forma como se ejecutan las operaciones y de la comprensión de la lógica del negocio, los flujos de información, el rol de las personas y dependencias que intervienen en el manejo de las operaciones y otros aspectos que el auditor considere importantes.

Cuando se realiza por primera vez la auditoría en un servicio, la información relevante obtenida en esta etapa se organiza en un documento conocido como archivo permanente o expediente continuo de auditoría. Si el archivo ya existe, es necesario su revisión y actualización con los cambios efectuados desde la última auditoría.

Este documento contiene información sobre los objetivos y procesos que soportan los sistemas de información y sobre los recursos de tecnología utilizados (instalaciones de procesamiento, infraestructura, personal, contratos, etc.) y la importancia relativa de las cifras que se procesan y otros datos de interés.

III.2.4. Programación

El Programa Anual de Auditoría que al efecto se elabore por la ASE, establecerá el universo de entes públicos a auditar durante el ejercicio fiscal que corresponda, asimismo establece la calendarización dentro de la programación de las auditorías.

De igual forma se comisiona al equipo de auditores de TI para llevar a cabo las auditorías del Programa Anual de Auditoría. El programa de trabajo se formula en papeles o medios magnéticos en los cuales generalmente se anotarán los siguientes encabezados:

- Procedimiento: Para describirlo lo más claro y breve posible.
- Extensión: Deberá incluirse y describirse su técnica.
- Oportunidad: Donde se aclara la época o fecha que debe efectuarse el trabajo específico.
- Auditor: Donde se asigna el responsable y equipo auditor de la revisión.
- Tiempo estimado: Donde se anota el tiempo en horas que se estima concluir la revisión.
- Tiempo real: Para anotar el tiempo realmente empleado
- Variación: Para anotar los tiempos reales respecto a los estimados y hacer las explicaciones pertinentes.
- Observaciones: Para aclarar aspectos especiales en relación con el trabajo o la cuenta a revisar.

III.2.5. Integración

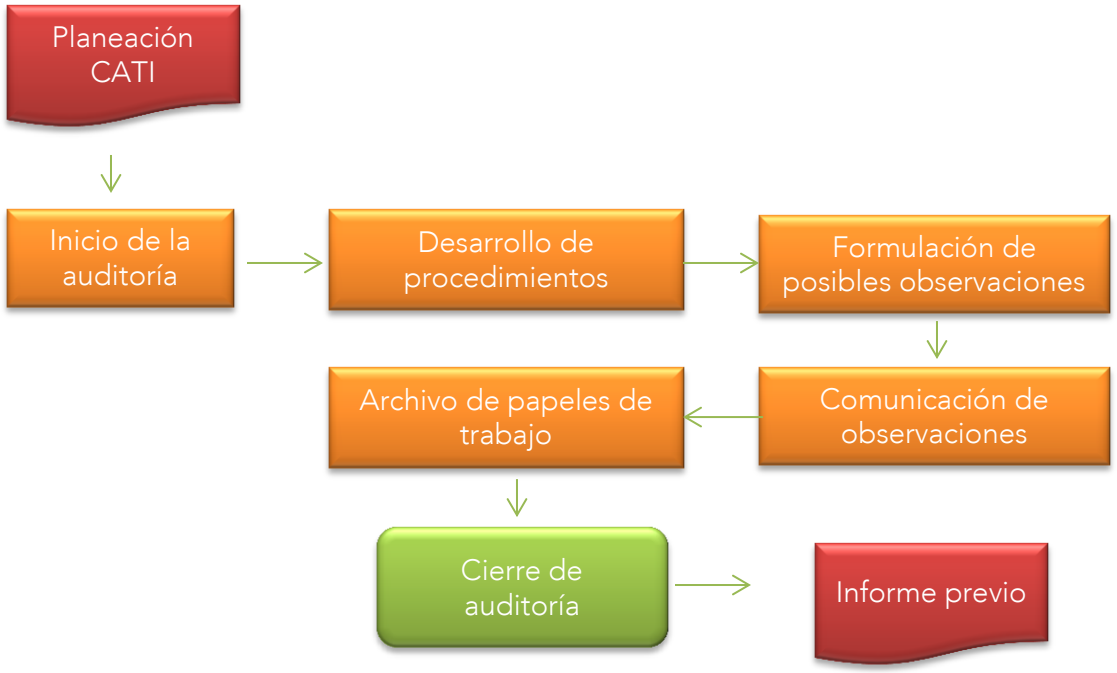
Considerado como el último de los procesos en la fase de planeación. Es aquí donde se consolida la información generada y que documentalmente establece la evidencia del

proceso de planeación, del estudio y evaluación del control interno, de los procedimientos a aplicar en la auditoría, de la supervisión a realizar, así como la programación de las auditorías.

III.3. Ejecución de la Auditoría

La fase de ejecución de la Auditoría se lleva a cabo en dos vertientes, el trabajo de campo que se realiza generalmente en el domicilio del ente, y otros procedimientos de la auditoría se realizan de gabinete en las oficinas de la Auditoría Superior. En la etapa de ejecución se realizan las pruebas de evaluación de cumplimiento normativo, el examen documental y la obtención de evidencias suficientes, competentes y relevantes que permitan cumplir los objetivos generales y específicos considerados en la planeación de auditoría de tecnologías de información.

Figura 9. Proceso de Ejecución de Auditoría



En esta fase, el equipo auditor realizará de ser necesario los ajustes al programa de auditoría, con el fin de lograr el objetivo de la misma, registrando los cambios.

III.3.1. Inicio de la auditoría

III.3.1.1. Acreditación

Es aquí donde se apersonan los auditados comisionados del área informática ante el titular y/o funcionario facultado, para dar inicio a la auditoría en el domicilio del ente a quienes se le presenta el Oficio de Comisión emitido por funcionario facultado de la Auditoría Superior para la realización de la auditoría procediendo a acreditarse los auditores comisionados con las credenciales de identificación correspondiente y el oficio de comisión. Posteriormente se solicita el nombramiento de testigos y la identificación y/o acreditación de los funcionarios y testigos con la finalidad de levantar el acta de inicio respectiva, firmando en dicho documento las partes que en ella intervienen.

III.3.1.2. Actividades

a. Reunión inicial:

   La reunión inicial es presidida por el auditor encargado, haciendo la presentación del equipo de auditoría a los funcionarios del ente auditado, ante quien exponen los objetivos, alcance y naturaleza de la misma y hacen entrega del documento original de acreditación ante el titular de la entidad.

b. Acta de inicio:

   Posterior a la presentación del oficio de comisión y explicado el objeto del mismo, se procederá a solicitar al titular la designación de dos testigos a afecto

de elaborar el acta de inicio, firmando al término de la misma los actuantes en el proceso de inicio de la auditoría.

En caso de no designar a los testigos antes citados, se hará constar dicha circunstancia en el acta de inicio, y se procederá al inicio de la auditoría.

c. Lugar de trabajo:

Solicitar al titular del ente auditado un espacio adecuado para el desarrollo de los trabajos de auditoría, asimismo las herramientas y equipo requerido por los auditores para el mejor desempeño de su comisión.

III.3.2. Desarrollo de procedimientos

De acuerdo a las tareas asignadas en la planeación de la auditoría, el equipo asignado se orientará al logro de los objetivos de la revisión, a través del examen documental, la inspección y la verificación de la información del ente en lo referente a programas, planes y acciones, aplicando los procedimientos y técnicas de auditoría necesarios.

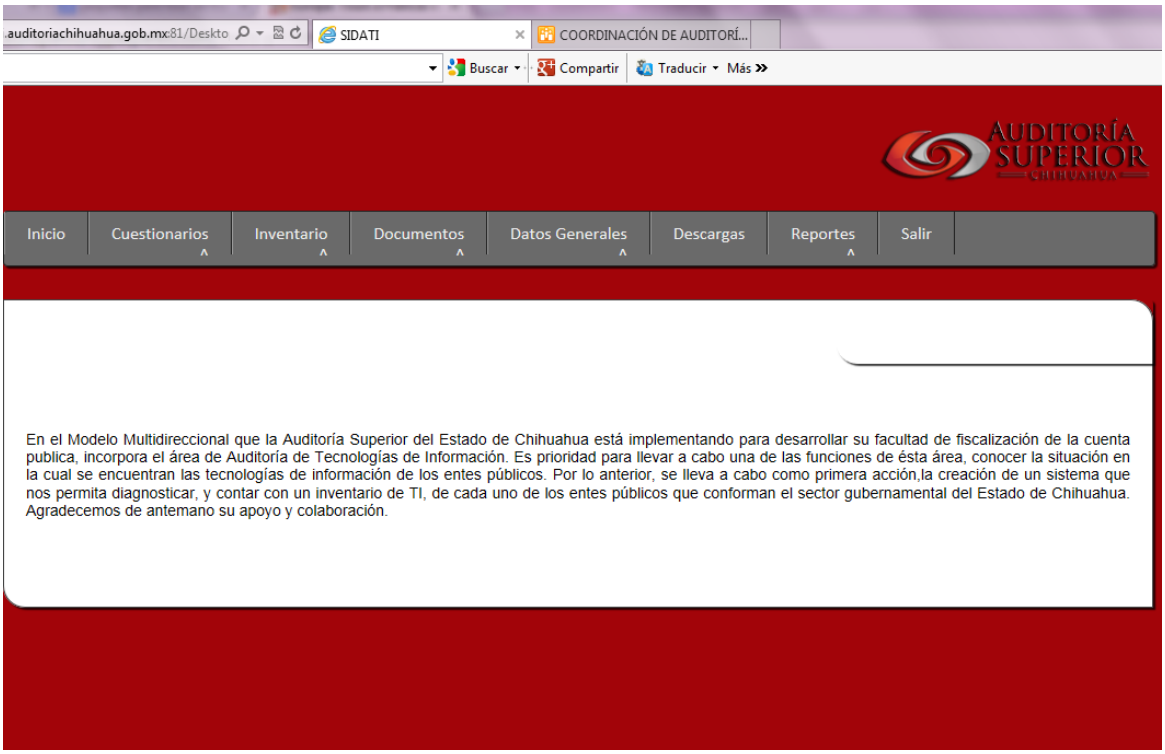
III.3.2.1. Actividades

a. Evaluación del control interno:

Todos los tipos de auditoría ejecutados en la ASE, deben evaluar la estructura de control interno de los entes a auditar, que sirva de apoyo en la toma de decisiones de los auditores y establecer los pronunciamientos normativos aplicables a su estudio y evaluación como un aspecto fundamental al establecer la estrategia de la auditoría.

Particularmente, el área de auditoría de tecnologías de información desarrolló un software en web que permitió la aplicación de un cuestionario de control interno y la solicitud de inventarios de tecnologías de información a cada uno de los entes que conforman el sector gubernamental con la finalidad de obtener un diagnóstico general de los recursos informáticos (humano, técnico, y de sistemas) del sector público del Estado de Chihuahua. Este sistema fue desarrollado y fundamentado en el Marco de Control COBIT.

Figura 10. Sistema WEB SIDATI



En esta etapa los auditores deben evaluar el sistema de control interno existente en los procesos de negocio y sistemas de información objeto de la auditoría, como base para determinar la naturaleza y extensión de las pruebas de auditoría que se requieran. Evaluar el sistema de control interno significa: "Determinar si los controles establecidos en los procesos de negocio y los sistemas de

información, ofrecen la protección apropiada para reducir los riesgos a niveles aceptables para la organización".

El propósito de la evaluación de control interno, es determinar si es suficiente y efectiva para proteger a la organización, contra los riesgos que podrían afectarla en los procesos de negocio y sistemas de información que se están auditando. Esto es, evaluar la confiabilidad de los controles utilizados para prevenir o detectar y corregir las causas de los riesgos y minimizar el impacto que estos tendrían en caso de llegar a materializarse.

La evaluación del sistema de control interno produce resultados intermedios, de valor importante para las etapas restantes del proceso de auditoría, estos son:

1) El auditor fundamenta su opinión sobre la confiabilidad que ofrecen los controles utilizados, para reducir la probabilidad de ocurrencia o el impacto de los riesgos. Los resultados de esta evaluación sirven al auditor como base para determinar la naturaleza y extensión de las pruebas de auditoría que se consideren necesarias y apropiadas a las circunstancias.

2) El auditor identifica y soporta debilidades y oportunidades de mejoramiento (observaciones de auditoría) en la estructura de los controles. Estas observaciones son insumos para el informe de auditoría.

3) El auditor identifica los controles que deberán verificarse en la etapa de ejecución de pruebas de auditoría, para determinar que realmente existen, están operando y son entendidos por las personas encargadas de ejecutarlos (pruebas de cumplimiento).

4) El auditor identifica los datos críticos y actividades sobre las cuales es necesario aplicar pruebas para verificar la exactitud y confiabilidad de los cálculos y de la información que producen los sistemas de información para apoyar el desarrollo de las operaciones del negocio (pruebas sustantivas).

5) El auditor documenta las observaciones de auditoría para los procesos de negocio y los sistemas de información que los soportan. Esta presenta las debilidades y deficiencias de control interno y seguridad identificadas en la evaluación de controles.

Los controles internos comprenden planes, métodos, procedimientos y otras medidas, incluyendo la actitud de funcionarios y demás personal de la entidad, encargados de lograr los objetivos de efectividad, eficiencia y economía; proteger y conservar los recursos públicos; y cumplir leyes, reglamentos y otras normas.

b. Obtención de pruebas de auditoría:

   Aplicando los procedimientos y técnicas de auditoría, el auditor debe obtener evidencia suficiente, competente, relevante y aplicar pruebas de control y procedimientos sustantivos, que le permitan fundamentar razonablemente los juicios y conclusiones que le formule al ente auditado.

c. Las pruebas a realizar son:

   De control: para confirmar que los programas o acciones han operado efectivamente durante el período examinado.

   De cumplimiento: Sobre la observancia de las disposiciones legales y reglamentarias vigentes. Todas las pruebas deben incorporarse en los papeles de trabajo de la comisión de auditoría, con su respectivo análisis y conclusión.

d. Las técnicas de auditoría son:

Verificación ocular: Los auditores se cerciorarán personalmente, sobre los hechos y circunstancias, cómo el personal de la entidad ejecuta las operaciones.

Verificación oral: Indagación, averiguaciones o conversaciones con el personal del ente auditado. Varias respuestas relacionadas entre sí, razonables y consistentes, suministran un elemento de juicio satisfactorio.

Entrevistas: Con beneficiarios de programas o proyectos, deberá prepararse apropiadamente, e identificar quiénes serán los entrevistados, así como definir el propósito y los puntos a abordar.

Verificación escrita: Radica en corroborar la verdad, certeza o probabilidad de hechos, situaciones, sucesos u operaciones mediante documentación certificada, datos e información obtenidos de manera directa de los funcionarios o terceros que participan o ejecutan las operaciones sujetas a verificación.

Confirmación: Permite comprobar la autenticidad de los registros y documentos a través de la información directa o escrita otorgada por una persona independiente del ente auditado y que se encuentre en posibilidades de conocer la naturaleza y condiciones de la operación y por lo tanto confirmar de una manera valida esta técnica.

Verificación documental: Se aplica para constatar la existencia, legalidad, autenticidad y legitimidad de las operaciones efectuadas por el ente, mediante la verificación de los documentos que las justifiquen.

Verificación física: La Inspección es el examen físico presencial de activos, obras, documentos, escenarios, con el objeto de establecer su existencia, estado y autenticidad.

Inspecciones: Si bien las inspecciones forman parte de las técnicas de verificación física, su realización debe ser selectiva. Deben contar con un plan que contenga como mínimo:

- Objetivo
- Actividades a desarrollar
- Lugares a visitar
- Recursos humanos
- Apoyo logístico
- Duración
- Responsable

Certificación: Obtención de un documento de que se asegura la verdad de un hecho, legalizado por la firma de una autoridad facultada para hacerlo.

Reuniones de avances de auditoría: Durante la fase de ejecución de la auditoría, se realizan reuniones de avances. Estas reuniones deben ser presididas y guiadas por la supervisión.

Cruce de información: En la auditoría de las tecnologías de información por ser parte de la estructura multidisciplinaria de la ASE, es necesario crear los canales y filtros de información entre comisiones de auditoría que ayuden al logro del éxito de la misma.

III.3.3. Formulación de posibles observaciones y/o recomendaciones

Las posibles observaciones y/o recomendaciones determinadas o formuladas como resultado de los procedimientos de auditorías de tecnologías de información aplicados al ente auditado, los cuales están referidos al incumplimiento de la normatividad aplicable, por desvió de recursos destinados a programas tecnológicos.

III.3.3.1. Documentación e información

Fuentes de criterio: Normativa general y específica, documentos diversos que sustenten el incumplimiento normativo y desviaciones detectadas.

Riesgos en el proceso de auditoría: Derivado de la supervisión en el proceso de ejecución de la auditoría, existen situaciones de irregularidad que pueden alterar o modificar el desarrollo de los procedimientos y alcances considerados en la planeación de la auditoría.

III.3.3.2. Procedimientos

Desarrollo: El auditor al momento de ejecutar los procedimientos de auditoría debe tener en cuenta las siguientes características:

- Debe estar basado en hechos y evidencias precisas debidamente documentadas.
- Debe ser objetivo y completo.
- Debe estar basado en una razón suficiente para respaldar las conclusiones.
- Debe ser convincente y claro para una persona que no haya participado en la auditoría.

De contener las características y atributos señalados, la observación se redacta según la estructura: rubro, cuenta o concepto, descripción de la falta normativa o determinación de diferencias encontradas, así como la fundamentación de la legislación que se incumplió.

Análisis de la observación: El auditor debe considerar los siguientes criterios para analizar la viabilidad de una observación. Materialidad: para que una observación sea significativa debe garantizar la recolección de evidencias. Asimismo se debe tener en cuenta la relevancia en la desviación de recursos.

Revisión y Supervisión: Las observaciones deben ser revisadas como mínimo en dos niveles, el de la jefatura de la auditoría y el de la supervisión, los cuales deben asegurar el cumplimiento de los puntos anteriores.

III.3.4. Comunicación de posibles observaciones y/o recomendaciones

El auditor encargado es el responsable de comunicar oportunamente las posibles observaciones y/o recomendaciones al jefe inmediato superior, a fin de que puedan presentar sus comentarios y aclaraciones sustentados documentadamente en el plazo fijado, para su oportuna evaluación y consideración en el informe final correspondiente.

III.3.5. Archivo de papeles de trabajo

Es el archivo con las hojas de trabajo que contienen las evidencias del desarrollo de cada una de las etapas de la auditoría. Los documentos de este archivo tienen validez por una sola vez, es decir, para cada auditoría realizada a las aplicaciones que están en proceso de evaluación. Por consiguiente, cada vez que se efectúe una auditoría se debe elaborar un nuevo archivo con la información recopilada.

III.3.6. Cierre de auditoría

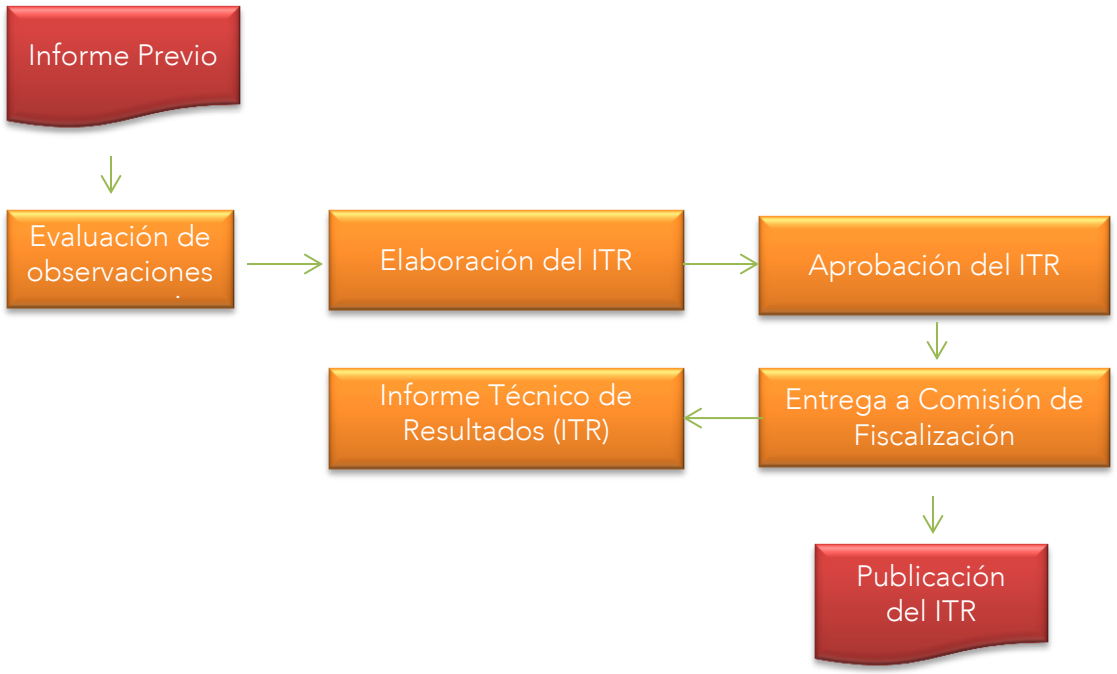
Es la culminación de la fase de ejecución o el trabajo de campo; aquí se sustentan los objetivos y procedimientos de las observaciones y/o recomendaciones, asimismo el auditor tiene que hacer uso de sus conocimientos del área y de su juicio profesional aplicando en gran medida la experiencia para lograr la evidencia de auditoría suficiente que permita determinar que el ente auditado cumplió con las expectativas.

Concluida la fase de ejecución, el equipo de auditoría se prepara para iniciar la etapa de la elaboración del informe técnico de resultados.

III.4. Elaboración del Informe de Resultados

El informe técnico de resultados es el documento más importante del trabajo de la auditoría de tecnologías de información, por presentar los resultados obtenidos en la revisión al ente. El informe de auditoría debe contener la expresión de razonamientos o juicios fundamentados en las evidencias obtenidas en relación a los objetivos de la auditoría.

Figura 11. Proceso de Informe Técnico de Resultados



III.4.1. Evaluación de observaciones y/o recomendaciones

El titular de la auditoría tecnologías de información deberá evaluar las observaciones y/o recomendaciones resultantes de la auditoría al ente. Dichos informes deben redactarse de manera clara para facilitar su comprensión, por lo tanto deben estar libres de imprecisiones y ambigüedades y conservar las características de independencia, objetividad, etc.

III.4.1.1. Documentación e información

Aclaraciones y Comentarios: producto de las observaciones, se procederá a la realización de las aclaraciones y comentarios correspondientes del ente auditado, dentro de los plazos establecidos en la Ley de la Auditoría Superior del Estado de Chihuahua.

III.4.1.2. Procedimientos análisis y evaluación de aclaraciones y comentarios

Permite diferenciar con la mayor objetividad, si lo plasmado en las observaciones y las aclaraciones o comentarios que efectúen los funcionarios del ente respecto de la observación. Lo realiza el equipo de auditoría bajo responsabilidad del auditor encargado.

III.4.1.3 Resultados de informes técnicos

Documentos Evaluados: es el resultado del análisis efectuado por el equipo auditor y deberá ser considerado en el resultado final de cada observación y/o recomendación e incluido en el informe de auditoría a manera de anexo.

III.4.2. Elaboración del informe

El informe técnico de auditoría de conformidad con la Ley de la Auditoría Superior, es el resultado de la auditoría practicada al ente auditado, dicho documento se estructura con los conceptos revisados, resaltando las irregularidades detectadas y la cuantificación de las mismas, asimismo se integrará con recomendaciones de acciones y programas encaminados a mejorar el desempeño del ente auditado.

De considerarse pertinente, se incluirán gráficos, fotos, tablas y cuadros que apoyen al informe Técnico de Resultados.

III.4.2.1. Documentación e información

Programa Anual de Auditoría: Que el ente auditado se encuentre integrado en el programa anual de auditoría de conformidad a lo que establece la norma.

III.4.2.2. Procedimientos

Desarrollo de la Estructura y Contenido del Informe: la elaboración del informe, está a cargo del equipo de auditoría conjuntamente con la supervisión y debe ser redactado en base al índice de áreas auditadas, integrando las observaciones encontradas, así como a las recomendaciones según las mejores prácticas.

Revisión del Informe: recae en el titular del área la revisión del informe realizado por el auditor encargado, para obtener un producto final de calidad.

III.4.2.3. Resultado de la elaboración del informe

Informe de Auditoría: es el producto principal de la auditoría de tecnologías de información y contiene las observaciones, conclusiones y recomendaciones orientadas a la mejora de los procesos y actividades de la entidad auditada.

Ficha Técnica: Es aquella que concentra los asuntos más importantes de la auditoría, debe ser breve y contener la posición de la ASE frente a la problemática evaluada.

III.4.3. Aprobación

Concluida la elaboración del informe del área de auditoría de tecnologías de información, es revisado por la instancia de normatividad para su aprobación legal y posteriormente remitirlo al ente auditado para la respuesta a las observaciones que integra el mismo, con la finalidad de agotar el derecho de audiencia del auditado.

III.4.3.1. Remisión a la entidad:

La remisión del informe de auditoría deberá estar acorde a los plazos establecidos en el programa anual de auditoría y disposiciones legales aplicables, permitiendo así que la información motivo del informe, sea utilizada oportunamente por el titular de la entidad

Anexo 1: Diagrama de Flujo de la auditoría de tecnologías de información

GLOSARIO

Aplicación: Aunque se suele utilizar indistintamente como sinónimo genérico de 'programa' es necesario subrayar que se trata de un tipo de programa específicamente dedicado al proceso de una función concreta dentro de la empresa.

Aplicación Web: Aplicaciones que los usuarios pueden utilizar accediendo a un servidor web a través de Internet o de una intranet mediante un navegador.

ASE: Auditoría Superior del Estado de Chihuahua.

Auditor: Persona que efectúa una auditoría

Auditoría: Examen de las operaciones de una empresa por especialistas ajenos a la operación y con objetivos de evaluar el ambiente de control y la situación de la misma.

Bases de Datos: Colección de datos organizados para que a través de las aplicaciones y programas la computadora pueda acceder rápidamente a ella.

COBIT: Objetivos de Control para la Información y las Tecnologías Relacionadas.

Confidencialidad: Se refiere a que la información solo puede ser conocida por individuos autorizados.

Control Interno: Conjunto de objetivos, políticas, procedimientos y registros con el propósito de:

I. Procurar mecanismos adecuados de operación, acordes con las estrategias y fines de las instituciones, que permitan identificar, dar seguimiento y evaluar los riesgos que puedan derivarse de las actividades del negocio, con propósito de

reducir las pérdidas en que puedan incurrir en la realización de actos o hechos voluntarios o involuntarios.

II. Delimitar las diferentes funciones y responsabilidades entre sus órganos sociales, unidades administrativas y personal, a fin de obtener eficiencia y eficacia en la realización de sus actividades.

III. Diseñar sistemas de información administrativa y financiera, correcta, precisa, íntegra, confiable y oportuna.

IV. Coadyuvar permanentemente a la observancia de la normatividad aplicable a las actividades de las instituciones.

COSO: Committee of Sponsoring Organizations of the Treadway Commission.

Costo: Desembolso en efectivo o en especie por algún beneficio.

Hardware: Conjunto de dispositivos físicos de los que consiste un sistema. Comprende componentes tales como el teclado, el mouse, las unidades de disco, el monitor, cada una de las partes físicas que forman un ordenador, incluidos sus periféricos, etc.

I.I.A: Institute of Internal Auditors.

I.M.A.I.: Instituto Mexicano de Auditores Internos, A.C.

Integridad: Totalidad, plenitud. La habilidad de determinar que la información recibida es la misma que la información enviada.

Investigación: Representa la obtención de información, datos y comentarios de los funcionarios y empleados de la empresa.

IRC: Sistema de Índice de Rendición de Cuentas ASE.

I.S.A.C.A: Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información).

ISO: (Organización Internacional para la Normalización) Organización de carácter voluntario fundada en 1946 que es responsable de la creación de estándares internacionales en muchas áreas, incluyendo la informática y las comunicaciones. Está formada por las organizaciones de normalización de sus 89 países miembro.

Lenguaje: En informática, conjunto de caracteres e instrucciones utilizadas para escribir programas de ordenador.

Management: La administración de empresas (Management), o ciencia administrativa es una ciencia social que estudia la organización de las empresas y la manera como se gestionan los recursos, procesos y resultados de sus actividades.

Medidas: Son medidas cuantitativas del desempeño del negocio utilizado por la alta gerencia para supervisar el negocio, obtener información y proporcionar retroalimentación. Una medida es efectiva cuando es parte de un proceso de supervisión que incluye objetivos y parámetros de acción o de excepción.

Metodología: Conjunto de pasos utilizados para lograr un objetivo.

NAGAS: Normas de Auditoría Generalmente Aceptadas.

Norma: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

Observación: Presencia física de cómo se realizan ciertas operaciones o hechos.

Papeles de trabajo: Registro del trabajo del auditor, el cual contiene la evidencia del trabajo realizado, sus observaciones y los resultados y conclusiones extraídas a la evidencia obtenida. Se utilizan para controlar el progreso del trabajo realizado y para respaldar la opinión del auditor. Los papeles de trabajo pueden estar constituidos por datos conservados en papel, película, medios electrónicos u otros medios.

Planeación: Consiste en prever cuales procedimientos de auditoria va a emplearse, la extensión y oportunidad en que van a ser utilizados y el personal que debe intervenir en el trabajo.

Política: Orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado.

Procedimiento: Método o sistema estructurado para la ejecución de actividades.

Proceso: Conjunto de operaciones lógicas y aritméticas ordenadas, cuyo fin es la obtención de resultados.

Programa: Secuencia de instrucciones que obliga al ordenador a realizar una tarea determinada.

Seguridad de la Información: Se refiere a la confidencialidad, integridad y disponibilidad de la información y datos, independientemente de la forma, los datos pueden ser: electrónicos, impresos, audio u otras formas.

Servidor o server: Ordenador que ejecuta uno o más programas simultáneamente con el fin de distribuir información a los ordenadores que se conecten con él para dicho fin.

SIDATI: Sistema de Diagnóstico de Auditoría de Tecnologías de Información.

Sistema de Información: Se denomina Sistema de Información al conjunto de procedimientos manuales y/o automatizados que están orientados a proporcionar información para la toma de decisiones.

Software: Componentes inmateriales del ordenador: programas, sistemas operativos, etc. Son aquellos programas que nos ayudan a tareas específicas como edición de textos, imágenes, cálculos, etc. también conocidos como aplicaciones.

SOX: La ley Sarbanes-Oxley.

TI: Tecnologías de Información. Conjunto de servicios, redes, software y dispositivos que tienen como fin la mejora de la calidad de vida de las personas dentro de un entorno, y que se integran a un sistema de información interconectado y complementario.

Auditoría de Tecnologías de Información: Se encarga de la verificación de los controles internos establecidos en el área de sistemas del ente, así como estudios de seguridad de la Información, Hardware y Software.

Recursos Informáticos: Son todos aquellos componentes de hardware y software, así como el personal que labora en él, o para el área de sistemas.