CORTE DE CUENTAS DE LA REPÚBLICA

El Salvador, C.A.

XIV Concurso Anual de Investigación de OLACEFs 2011, denominado "Auditoria de Gestión a las Tecnologías de Información y Comunicaciones".

Tema:

"Manual de Auditoría de Gestión a las Tecnologías de Información y Comunicaciones".

SEUDÓNIMO: JEREMÍAS 333

Í N D I C E

RESUMEN EJECUTIVO i

I. INTRODUCCIÓN 1

CAPITULO I 2

GENERALIDADES DE LA INVESTIGACIÓN 2

1. MARCO TEÓRICO 2

1.1 Titulo de la Investigación 2

1.2 Definición del Problema 2

1.3 Objetivos de la Investigación. 2

1.4 Alcance. 3

1.5 Metodología de Investigación utilizada. 3

1.6 Antecedentes. 4

1.7 Definición de Auditoría de Gestión a las TICs. 4

CAPITULO II 6

DESARROLLO DE LA INVESTIGACIÓN 6

1. PROCESO DE LA AUDITORÍA 6

1.1 Objetivo del Manual. 6

1.2 Elaboración y Organización de Papeles de Trabajo Electrónicos. 6

1.2.1 Información mínima deben contener los papeles de trabajo electrónicos..... 7

1.3 Naturaleza de la Documentación de Auditoría. 9

1.4 Forma, Contenido y Extensión de la Documentación de Auditoría. 10

2. FASES DEL PROCESO DE AUDITORÍA 12

2.1 Objetivos de la Auditoria de Gestión a las Tecnologías de Información y Comunicaciones. 12

Objetivo General. 12

Objetivos Específicos 12

2.2 Estándares Internacionales que influyen en el proceso de una Auditoría de Gestión a las Tecnologías de Información

y Comunicaciones. 13

Mejores Prácticas 14

2.3 Supervisión en el Proceso de una Auditoría de Gestión a las Tecnologías de Información y Comunicaciones.....16

CAPITULO III 16

DE LA PLANIFICACIÓN 18

1. Conocimiento de la Entidad y Entorno del área de Tecnología de Información y Comunicación. 16

1.1 Organización de área TIC. 17

1.2 Infraestructura Tecnológica de la entidad auditada. 18

1.3 Plan Maestro de tecnología de información y comunicaciones..... 19

1.4 Planes Operativos 20

1.5 Planes de Continuidad 21

1.6 Planes de Mantenimiento. 21

1.7 Presupuesto Tecnológico. 22

1.8 Planificación de TACCs. 22

2. Seguimiento a Recomendaciones de Auditorías Anteriores. 23

3. Análisis, Evaluación e Incorporación de Hallazgos de Auditoría elaborados por la Unidad de Auditoría Interna y Firmas Externas de Auditoría.....24

4. Plan de Trabajo de Auditoria TIC´s. 25

5. Análisis Previo. 26

5.1 Áreas preliminares a examinar. 26

5.1.1 Organización y Planificación de TI..... 26

5.1.2 Procesamiento Electrónico de Datos..... 27

5.1.3 Evaluación de los Sistemas. 29

5.1.4 Controles de Sistema en Desarrollo y Producción..... 29

5.1.5 Evaluación de los equipos..... 31

5.1.6 Evaluación de la Seguridad de la Información. 33

5.2 Indicadores de Gestión (Eficiencia, Eficacia, Efectividad y Economía) aplicados al Área de Tecnología de Información y Comunicaciones 34

5.3 Evaluación de Riesgos Tecnológicos. 36

5.4 Evaluación de Control Interno Tecnológico. 38

5.5 Normativa Técnica de Control Interno y Fuentes de Información... 41

5.6 Comunicación de Asuntos de Importancia Relativa de TIC´s. 42

5.7 Informe Ejecutivo de Análisis Previo. 43

6. Conclusiones y Recomendaciones.....46

CAPITULO IV 47

DE EJECUCIÓN.....47

1. Pruebas de Auditoría asistidas por Computadora. 47

1.1 Pasos para desarrollar una TAAC. 48

1.2 Seguridad de datos y Técnicas de Auditoría Asistidas por Computadora. 48

2. Evaluación y recolección de Evidencia..... 49

3. Cumplimiento de Políticas y procedimientos. 51

4. Carta de Salvaguarda. 52

CAPITULO V 52

DE INFORME 52

1. Resultados Preliminares de Auditoría (Informe Previo)..... 52

2. Carta de Gerencia de Asuntos de Importancia Relativa. 53

3. Informe de Auditoría. 54

II. CONCLUSIONES 57

III. APLICABILIDAD EN EL CAMPO DEL CONTROL GUBERNAMENTAL. 58

IV. BIBLIOGRAFÍA 59

V. ANEXOS 60

ANEXO 1

Formato de Papeles de Trabajo 61

ANEXO 2 .....

Criterios Técnicos del Área de Tecnologías de la Información y Comunicaciones. 62

RESUMEN EJECUTIVO

El presente manual de auditoría de gestión a las tecnologías de información y comunicaciones describe procedimientos que los auditores deben utilizar para verificar el uso de los recursos tecnológicos, confidencialidad, confiabilidad, integridad, disponibilidad de la información procesada por los sistemas de información automatizados y apoyo en la automatización de los procesos operativos y administrativos de la entidad para llegar a medir los indicadores de gestión de eficiencia, efectividad y economía de las tecnologías de información y comunicaciones implementadas por la institución y presentar conclusiones y recomendaciones oportunas y acertadas que sirvan de guía para corregir las deficiencias que pueden llegar a existir y lograr mejorarlas.

El Capítulo I, describe las generalidades de la investigación como: título de la investigación, definición del problema, los objetivos de la investigación, el alcance de la investigación incluyendo el proceso de auditoría de gestión a las tecnologías de información y comunicaciones, la metodología utilizada, los antecedentes de las tecnologías de la información y comunicaciones en las diferentes entidades del sector público y municipal que trabajan continuamente con sistemas informáticos.

En el Capítulo II Desarrollo de la investigación, se describen los objetivos del manual, el diseño, preparación y conservación de papeles de trabajo y la naturaleza de la documentación de auditoría en formato electrónico en cada ente fiscalizador, además de los procedimientos que deben desarrollar los auditores en la fase de planificación de auditoría y de

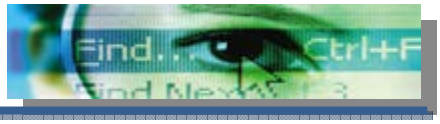
los estándares internacionales que intervienen en el proceso de una auditoría de gestión a las tecnologías de información y comunicaciones.

El Capítulo III de la Planificación, describe el desarrollo de una auditoría de gestión a las TIC´s, en la fase de planificación, obteniéndose un entendimiento y comprensión de los aspectos siguientes: entorno de la entidad y del Área de Tecnología de Información, procesos sistematizados, administración de riesgos, evaluación de indicadores de gestión, control interno y organización del área de tecnología de información y comunicaciones, pues dicho conocimiento le brinda un marco conceptual, que le permite evaluar si la organización sigue un enfoque estructurado de gestión informática y si el mismo es adecuado, además el seguimiento a recomendaciones de auditorías anteriores, la elaboración de un plan de trabajo de auditoría y de la ejecución de guía de procedimientos de análisis previo y la elaboración del informe ejecutivo de análisis previo que contendrá los asuntos de importancia identificados y agrupados por proyectos de las áreas vulnerables o de impacto determinados.

En el Capítulo IV de la Ejecución, se describen las pruebas asistidas por computadora que se pueden aplicar para investigación y la obtención de evidencia de las causas que originan una debilidad en gestión tecnológica, la evaluación y recolección de evidencia suficiente y apropiada que permitan emitir las conclusiones acerca de la operatividad de la gestión en tecnología de información y comunicaciones.

El Capitulo V de Informe, describe la estructura que debe de contener un informe de resultados preliminares, la carta de gerencia, que dará a conocer a la administración todos aquellos asuntos de menor importancia,

estos asuntos de menor importancia son riesgos que pueden ser administrados y que a juicio del auditor no son de impacto en la gestión de las tecnologías de la información y comunicaciones, al haber garantizado el derecho de defensa a la administración, analizado las respuestas y comentarios, se emite el informe de auditoría que sustenta las conclusiones del auditor sobre el uso de las tecnologías de información y comunicaciones y medición de los indicadores de gestión de eficiencia, eficacia y economía de la entidad pública.



INTRODUCCIÓN

La creciente disponibilidad de información electrónica y procesos soportados por recursos informáticos y de comunicación que son capaces de satisfacer las circunstancias tanto funcionales como económicas, de oportunidad y efectividad de las entidades públicas, hacen que el auditor se vea en la necesidad de poseer el conocimiento suficiente de los sistemas de información por computadora para planear, dirigir, supervisar, y revisar el trabajo a desarrollar.

La naturaleza especializada de la auditoría de gestión a las tecnologías de la información y comunicaciones (TIC´s), requiere de habilidades y conocimientos técnicos informáticos, para desarrollar este tipo de auditorías, además es necesario para el desarrollo de la auditoria, la implementación de normativa legal y técnica en el Área de Tecnología de Información y Comunicaciones de la administración pública y municipal y promulgación de normas generales para la auditoría a los sistemas de información.

Para realizar auditoría de gestión a las tecnologías de información y comunicaciones requiere realizar una adecuada planeación de la auditoría, se debe tener un conocimiento general razonable que permita determinar el alcance, tamaño y características de cada área de Tecnología de la Información y Comunicación dentro de la organización que se auditará, sus sistemas, procesos sistematizados, normativa técnica utilizada por la entidad, adopción e implementación de estándares internacionales relacionados con seguridad de la información, control interno y servicios tecnológicos, organización y equipo físico y lógico.

CAPITULO I
GENERALIDADES DE LA INVESTIGACIÓN

1. MARCO TEÓRICO

1.1 Título de la Investigación

Manual de Auditoría de Gestión a las Tecnologías de la Información y Comunicaciones.

1.2 Definición del Problema

Los Entes Fiscalizadores no poseen una metodología apropiada a seguir para el desarrollo de auditorías de gestión a las tecnologías de información y comunicaciones.

1.3 Objetivos de la Investigación.

1) Proponer criterios técnicos tecnológicos en el desarrollo de auditorías de gestión a las tecnologías de información y comunicaciones.
2) Estandarizar una metodología para el desarrollo de auditorías de gestión a las tecnologías de información y comunicaciones.
3) Implementar procedimientos para el desarrollo de las auditorias de gestión a las tecnologías de información y comunicaciones.

1.4 Alcance.

El alcance que tendrá la investigación comprende todo el proceso de auditoría de gestión a las tecnologías de información y comunicaciones, e incluye las fases de planificación, ejecución e informe.

La Auditoría de Gestión a las Tecnologías de Información y Comunicaciones, comprenderá un examen a los controles generales y específicos TIC's y procedimientos sustantivos y administrativos de la entidad, apoyados por recursos tecnológicos, para el cumplimiento de sus objetivos estratégicos y operativos, con el propósito de mejorar la efectividad, eficiencia, economía y confidencialidad de la información y la prestación de los servicios en las entidades públicas y municipales.

1.5 Metodología de Investigación utilizada.

La metodología de investigación será documental, la cual permite elaborar un marco teórico conceptual para formar un cuerpo de ideas sobre el tema investigado, incluye el uso de instrumentos definidos según la fuente documental a que hacen referencia.

Estas fuentes de información son los documentos que registran o corroboran el conocimiento inmediato de la investigación, dentro de los cuales están: libros, revistas, informes técnicos, tesis, internet, entre otros.

Elegido el tema de estudio se procede a la recopilación y lectura bibliográfica sobre la temática de interés, la cual permite fortalecer los conocimientos teóricos y conceptuales.

La investigación contará con el título de la investigación, definición del problema, los objetivos, el alcance de la investigación y los antecedentes.

1.6 Antecedentes.

En todas las áreas de la gestión pública y municipal, las tecnologías de información y comunicaciones han transformado la manera de prestar los servicios al público, optimizando los recursos y volviéndose más productivos, siendo capaces de producir mucho más, de mejor calidad, invirtiendo mucho menos tiempo.

Las Tecnologías de Información y Comunicaciones, también conocidas como TIC, son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Incluyen las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro, o procesar información para poder calcular resultados y elaborar informes.

Las Tecnologías de la Información y la Comunicación están presentes en nuestras vidas y la han transformado.

Esta revolución ha sido propiciada por la aparición de la tecnología digital. La tecnología digital, unida a la aparición de ordenadores cada vez más potentes, ha permitido a la humanidad progresar muy rápidamente en la ciencia y la técnica desplegando nuestro arma más poderosa: la información y el conocimiento.

1.7 Definición de Auditoría de Gestión a las TICs.

La Auditoría de Gestión a las Tecnologías de Información y Comunicaciones, consiste en el examen de carácter objetivo (independiente), crítico (evidencia), sistemático (normas) y selectivo (muestral) de las políticas, normas, funciones, actividades, procesos e informes de una entidad, con el fin de emitir una opinión profesional (imparcial) con respecto a: eficiencia en el uso de los recursos informáticos, validez y oportunidad de la información, efectividad de los controles establecidos y la optimización de los recursos tecnológicos.

Este enfoque es totalmente compatible con las prácticas y controles contenidos en COBIT, ITIL, estándares o normativa que relaciona el enfoque COSO, SAC, NIAS, Estándares de Seguridad de la Información (ISO 27000) entre otros, que hacen referencia a las pistas de auditoría en los sistemas informáticos, controles de acceso a los sistemas, bases de datos, Áreas de Tecnología de la Información y Comunicaciones (TIC´s) área de servidores, codificación de la información, prevención de virus, fraude,

detección y mitigación de intrusos, entre otros; estos estándares no proporcionan un criterio legal aplicable si no han sido adoptados por la entidad, pero sí procedimientos de auditoría para examinar la gestión tecnológica en las diferentes organizaciones del sector público.

CAPITULO II
DESARROLLO DE LA INVESTIGACIÓN

1. PROCESO DE LA AUDITORÍA

1.1 Objetivo del Manual.

Proveer a los auditores tecnológicos lineamientos para la realización de una auditoría de gestión a las tecnologías de información y comunicaciones que coadyuven a la buena gestión de la disponibilidad de los servicios sistematizados prestado a la población en general, con el uso de la tecnología proporcionando seguridad, disponibilidad, confiabilidad y oportunidad de la información procesada y resguardada dentro de la entidad.

1.2 Elaboración y Organización de Papeles de Trabajo Electrónicos.

Cada ente público diseñará e implementará formatos para elaboración de papeles de trabajo en medios magnéticos, el cual

se almacenará según las necesidades particulares de cada entidad fiscalizadora.

El auditor deberá preparar y conservar los papeles de trabajo adecuados, los cuales le ayudan en la planeación, desempeño, supervisión y revisión de la auditoría, y registran la evidencia obtenida para apoyar la opinión de auditoría.

La documentación de auditoría es conocida también como: **"papeles de trabajo"**. Y se refiere al registro de los procedimientos desarrollados en la auditoría, es decir, la evidencia más relevante obtenida en el transcurso de la misma; incluyendo las conclusiones a las que llegó el auditor.

1.2.1 Información mínima que deben contener los papeles de trabajo electrónicos.

Los papeles de trabajo electrónicos que elaborarán los auditores de sistemas informáticos serán en forma electrónica y deben ser completos, de tal forman que muestren: la información y los hechos concretos, el alcance del trabajo efectuado, las fuentes de la información obtenida y las conclusiones respectivas. **ANEXO 1.**

Como anteriormente se mencionó, la forma de documentar la evidencia va a depender del auditor, pero hay que tomar

en cuenta, las leyes que rigen cada país para presentar la documentación en forma electrónica o física.

1.2.2 Organización de Papeles de Trabajo.

A efecto de clasificar y organizar el archivo corriente y permanente de los papeles de trabajo originados en la auditoría de gestión a las TIC´s, a continuación se presenta un ejemplo de cómo realizarlo:

Archivo Permanente		
Legal	Administrativo	Técnico
Ley de Creación de la entidad	Organigrama TIC	Inventario de hardware y software
Manual de organización	Manual de Funciones	Sistemas operativos
	Manual de Descripción de Puestos	Bases de datos
	Políticas y procedimientos de TIC´s	Aplicaciones
	Contratos de nombramiento	Planes de contingencia
	Instructivos	Diagrama de Red
	Formularios	

Archivo Corriente	
Componente	Elementos
Marco Legal	Leyes y reglamentos
	Controles administrativos
	Normas y procedimientos
	Manuales de usuario
Percepción de usuarios	Percepción de usuarios
Niveles de seguridad	Seguridad física
	Seguridad lógica
	Panorama técnico
	Valores parametrizables
	Pistas de auditoría
Funcionamiento	Origen de datos
	Entrada de datos
	Proceso de datos
	Salida de información
Planes de contingencia	Back up
	Sitios de resguardo

1.3 Naturaleza de la Documentación de Auditoría.

La documentación de la auditoria puede hacerse en papel, medios electrónicos, u otros medios. Para este caso el medio será electrónico y documental respecto a la evidencia de respaldo sobre las deficiencias encontradas por el auditor, la cual debe de estar impresa (Físico) y con la suficiente seguridad razonable que es la

autorizada y proporcionada por el servidor público auditado, mientras no se tenga una legislación que avale la documentación en formato electrónico.

La documentación de auditoría debe ser preparada y archivada de tal manera que si en determinado momento otro auditor con experiencia necesite tener acceso a ella por cualquier motivo, pueda entender: la naturaleza, oportunidad y extensión de los procedimientos de auditoría desempeñados; los resultados y la evidencia de auditoría obtenida, así como las conclusiones obtenidas durante la auditoría.

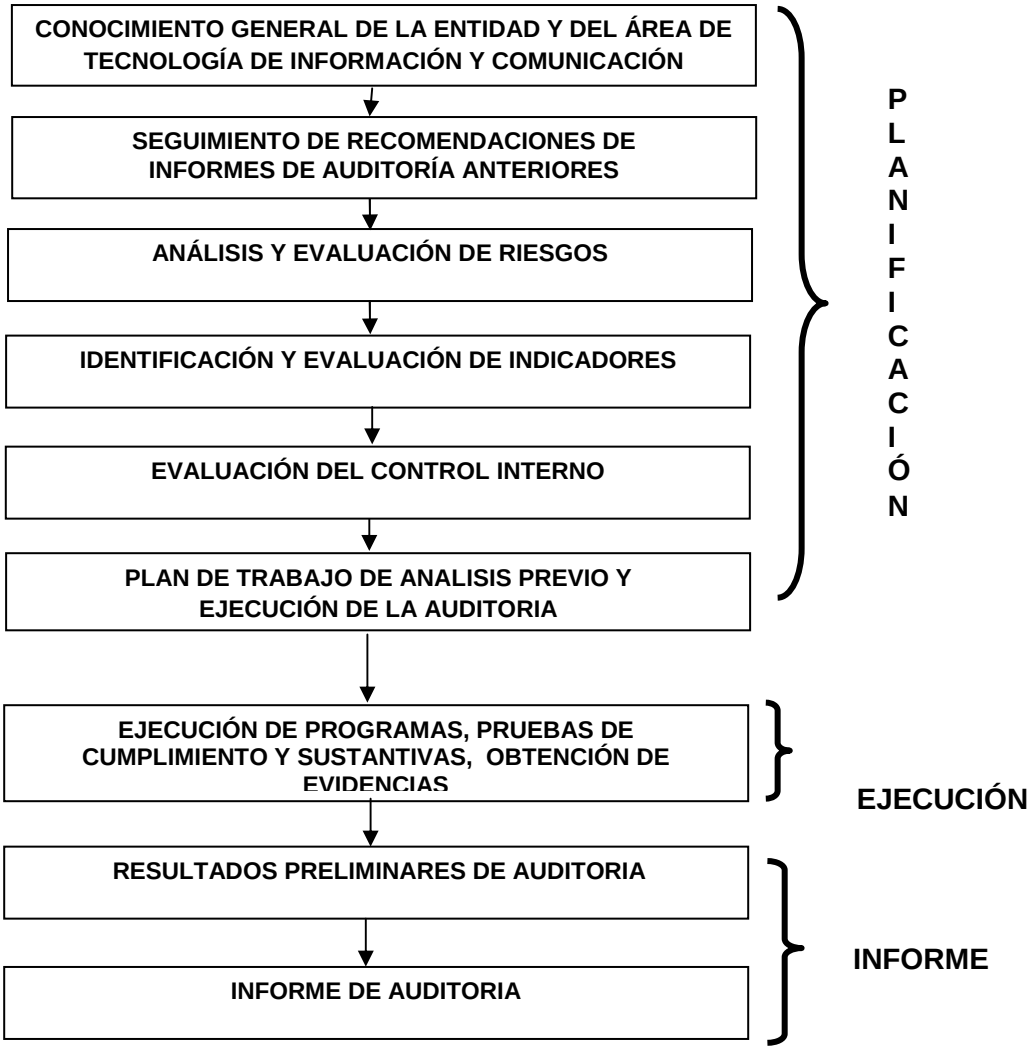
1.4 Forma, Contenido y Extensión de la Documentación de Auditoría.

Los papeles de trabajo deben ser preparados lo suficientemente completos y detallados con el fin de que haya una mejor comprensión de la auditoría.

Las Normas de Auditoría de la Organización Internacional de Entidades Fiscalizadoras (INTOSAI), en los acápites 153 a 158, destacan la importancia de la documentación del trabajo de auditoría, resaltamos lo señalado en los acápites 156 y 158: "**156.** Los auditores deben justificar documentalmente, de manera adecuada, todos los hechos relativos a la fiscalización, incluso los antecedentes, y la extensión de la planeación, del trabajo realizado y de los hechos puestos de manifiesto."; "**158.** El auditor debe tener en cuenta que el contenido y la disposición de los

documentos de trabajo reflejan su grado de preparación, experiencia y conocimiento. Los documentos de trabajo deben ser lo suficientemente completos y detallados como para permitir a un auditor experimentado, que no haya tenido previa relación con la auditoría, descubrir a través de ellos el trabajo realizado para fundamentar las conclusiones."

2. FASES DEL PROCESO DE AUDITORÍA



2.1 Objetivos de la Auditoria de Gestión a las Tecnologías de Información y Comunicaciones.

Objetivo General.

El objetivo de la auditoría de gestión a las tecnologías de información y comunicaciones es evaluar la eficiencia, economía, efectividad y confiabilidad de la información, para la toma de decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación.

Objetivos Específicos.

- Asegurar la integridad, confidencialidad, confiabilidad y oportunidad de la información.
- Seguridad de los datos, el hardware, el software y las instalaciones.
- Minimizar existencias de riesgos en el uso de tecnología de información en los procesos sistematizados.
- Conocer la situación actual del área informática para el logro de objetivos estratégicos y operativos de la institución.
- Apoyo de función del área de tecnología de información y comunicaciones a las metas y objetivos de la organización.
- seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente tecnológico.

- Incrementar la satisfacción de los usuarios que reciben los servicios sistematizados.
- Buscar una mejor relación costo-beneficio de los sistemas automatizados.

2.2 Estándares Internacionales que intervienen en el proceso de una Auditoría de Gestión a las Tecnologías de Información y Comunicaciones.

El auditor de las tecnologías de información y comunicaciones, deberá de tener conocimientos de los diferentes estándares que ayudan al control, operación y administración de los recursos tecnológicos, control de inversiones en tecnología de información y comunicaciones a nivel físico y lógico y procesos documentados de tecnología de información y comunicaciones. Dichos estándares inciden en el proceso de la auditoria, ya que las entidades de gobierno los implementan según sus necesidades de resguardo, uso y protección de la información, que es un activo importante dentro de la organización para asegurarse que la información se encuentre disponible, oportuna y utilizada por los funcionarios autorizados.

Para la realización de una auditoría de TICS, existen Normas de relacionadas a la Auditoría de Sistemas las cuales son emitidas por el Consejo Normativo de la Asociación de Auditoría y Control de Sistemas de Información (Information Systems Audit and Control Association – ISACA®).

Para documentar el proceso de auditoría, la Organización Internacional de Entidades Fiscalizadoras (INTOSAI), ha emitido lineamientos generales que destacan la importancia de documentar el trabajo de auditoría.

Mejores Prácticas

ITIL Esta metodología es la aproximación más globalmente aceptada para la gestión de servicios de tecnologías de información en todo el mundo, ya que es una recopilación de las mejores prácticas tanto del sector público como del sector privado que se apoyan en herramientas de evaluación e implementación.

El objetivo de usar ITIL

ITIL como metodología propone el establecimiento de estándares que ayudan al control, operación y administración de los recursos. Plantea hacer una revisión y reestructuración de los procesos existentes en caso de que estos lo necesiten (si el nivel de eficiencia es bajo o que haya una forma mas eficiente de hacer las cosas), lo que nos lleva a una mejora continua.

Otra de las cosas que propone es que para cada actividad que se realice se debe de hacer la documentación pertinente, ya que esta puede ser de gran utilidad para otros miembros del área, además de que quedan asentados todos los movimientos realizados, permitiendo que toda los usuarios estén al tanto de los cambios y no se tome a nadie por sorpresa.

COBIT conjunto de mejores prácticas para la seguridad, la calidad, la eficacia y la eficiencia en TIC que son necesarias para alinear TIC con el negocio, identificar riesgos, entregar valor al negocio, gestionar recursos y medir el desempeño, el cumplimiento de metas y el nivel de madurez de los procesos de la organización y tiene como propósito "investigar, desarrollar, publicar y promocionar un conjunto de objetivos de control generalmente aceptados para las tecnologías de la información que sean autorizados (dados por alguien con autoridad), actualizados, e internacionales para el uso continuo de los gestores de negocios (también directivos) y auditores." Gestores, auditores, y usuarios se benefician del desarrollo de COBIT porque les ayuda a entender sus sistemas de información (o tecnologías de la información) y decidir el nivel de seguridad y control que es necesario para proteger los activos de sus compañías mediante el desarrollo de un modelo de administración de las tecnologías de la información.

ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha

información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

2.3 Supervisión en el Proceso de una Auditoría de Gestión a las Tecnologías de Información y Comunicaciones.

Los entes fiscalizadores deberán contar con procedimientos autorizados para efectuar la supervisión y control de calidad del proceso de auditoría que incluya las fases de planificación, ejecución e informe, con el objetivo de identificar y corregir errores en el proceso y agregar valor a los resultados que deberán presentarse a la entidad auditada.

La supervisión puede ser conducida por funcionarios independientes al equipo de auditoría instalado en la entidad auditada, a efecto de recomendar mejoras objetivas e imparciales, acertadas, oportunas y que brinden calidad al proceso de auditoría, lográndose cumplir con las expectativas del ente auditado.

CAPITULO III
DE LA PLANIFICACIÓN

1. Conocimiento de la Entidad y Entorno del área de Tecnología de Información y Comunicación.

Para el desarrollo de una auditoría de gestión a las TIC´s, es muy importante que el auditor, conozca el entorno de la entidad y del Área de Tecnología de la Información, procesos sistematizados, organización

del área de tecnología de información y comunicaciones, planes estratégicos de TIC, planes operativos, planes de contingencia y/o continuidad del negocio relacionado con la tecnología de la información, planes de mantenimiento preventivo y correctivo de la plataforma tecnológica con la que cuenta la entidad, de manera que le permita una adecuada planificación de su trabajo, pues ese conocimiento le brinda un marco conceptual, que le permite evaluar si la organización sigue un enfoque estructurado de gestión informática y si el mismo es adecuado.

1.1 Organización de área TIC.

El auditor debe de conocer, comprender y analizar la arquitectura organizacional de la Entidad de manera general, identificando las ideas rectoras, organización, instrumentos administrativos, recursos humanos (principales funcionarios), productos y servicios de la entidad, así como la relación que mantiene con otras organizaciones y del conocimiento de la función del área de Tecnología de Información y Comunicaciones principalmente en aspectos como: Arquitectura Organizacional, Ideas Rectoras, Objetivos y metas operativas, Instrumentos Administrativos, Organización y función, Procesos, Productos y/o Servicios, Insumos y el entorno de la función de Tecnología de Información y Comunicaciones (clientes), aplicando procedimientos generales tales como:

- ✓ Revisar y evaluar si la función de TIC está alineada con la misión, visión, valores, objetivos y estrategias de la

organización y deberá revisar el desempeño esperado por la empresa (eficacia y eficiencia) y evaluar su cumplimiento.

- ✓ Revisar y evaluar la eficacia de los recursos de TIC y el desempeño de los procesos administrativos.
- ✓ Se debe utilizar un enfoque basado en riesgos para evaluar la función de TIC.
- ✓ Se deberá revisar y evaluar el ambiente de control de la organización.
- ✓ Se deberá de revisar las áreas físicas de TIC´s, con el propósito si está en condiciones para la operatividad de las Tecnologías de la Información y Comunicaciones.
- ✓ Se deberá de revisar las funciones de cada uno de los técnicos para comprobar si estos cuentan con herramientas y condiciones necesarias para realizar su trabajo y de la optimización de los recursos tecnológicos.
- ✓ Se deberá de verificar y analizar el Manual de funciones sea aplicable y acorde a la realidad de las funciones desarrolladas por el capital humano del Área de Tecnología de Información y Comunicaciones.

1.2 Infraestructura Tecnológica de la entidad auditada.

El auditor debe conocer, comprender y analizar de forma general la Gestión en Tecnología de la Información, la infraestructura o plataforma tecnológica y los sistemas de información aplicados a la entidad, tales como:

- ✓ Granja de Servidores y sus características
- ✓ Seguridad Perimetral

- ✓ Estructura de redes
- ✓ Sistemas Operativos
- ✓ Software y hardware de seguridad
- ✓ El inventario de Hardware y Software con el propósito de establecer el nivel de obsolescencia o actualización.
- ✓ Servicios tercerizados contratados por la entidad y vinculados con la tecnología de la información y comunicaciones.
- ✓ Adquisiciones (Inversiones) en recursos de Tecnología de la información.
- ✓ Infraestructura eléctrica, entre otras.

Sistemas de Información (Aplicaciones)

- ✓ Procesos y/o funciones (sustantivos, apoyo y administrativos) de la entidad, que están soportados con tecnología de información y comunicaciones.
- ✓ La Administración de Sistemas y Bases de Datos.
- ✓ Adopción de Metodologías de Análisis y desarrollo de Sistemas.
- ✓ Lenguajes de programación
- ✓ Aplicaciones en producción y desarrollo
- ✓ Gestores de bases de datos.

1.3 Plan Maestro de tecnología de información y comunicaciones.

Como producto del proceso de gestión, el área de tecnología de información y comunicaciones debe elaborar un plan maestro, definido como un documento a largo plazo que contenga la estrategia de proyectos de modernización de los procesos

institucionales a través de los recursos tecnológicos, con el objetivo de brindar con calidad el servicio ofrecido a los usuarios (Clientes) de la entidad, entre los aspectos mínimos que conforman dicho plan se encuentran los siguientes:

- ✓ Objetivos estratégicos institucionales
- ✓ Misión
- ✓ Visión
- ✓ Acciones estratégicas
- ✓ Procesos que serán automatizados
- ✓ Usuarios que intervienen en el proceso
- ✓ Recursos humanos, materiales, financieros y técnicos
- ✓ Cronograma de implementación de proyectos

1.4 Planes Operativos

Los planes operativos son un instrumento de control a corto plazo que el auditor debe revisar, y que éstos contengan el desgloce de las actividades y acciones a desarrollar que conforman cada línea estratégica del plan maestro, plasmándose lo siguiente:

- ✓ Objetivo general
- ✓ Objetivos específicos
- ✓ Líneas estratégicas y acciones a corto plazo
- ✓ Responsables de los proyectos a desarrollar.
- ✓ Recursos humanos, materiales, financieros y técnicos
- ✓ Cronogramas de actividades a desarrollar en el periodo.

1.5 Planes de Continuidad

Es un conjunto de tareas que el área de TIC debe realizar en caso de fallas en los sistemas impidan el normal funcionamiento de los servicios TIC, el fin es recuperar a la brevedad las operaciones de la organización.

El auditor debe conocer y analizar el plan de contingencia implementado por la entidad para poder auditarlo, con el propósito de determinar el grado de efectividad y eficiencia para brindar continuidad en los servicios de TIC y minimizar la probabilidad y el impacto de interrupciones en los servicios, funciones y procesos claves del negocio.

Además se debe de conocer y comprender que el área de TIC´s ha requerido procedimientos para los planes de contingencia de servicios tecnológicos y de comunicaciones contratados con terceros con el propósito garantizar la continuidad del negocio, alinear los procesos de recuperación y determinar el impacto de la contingencia; para esto deberá de realizar con los proveedores pruebas de contingencia para determinar la veracidad del plan presentado.

1.6 Planes de Mantenimiento.

El auditor debe comprender y analizar los planes de mantenimiento de la Infraestructura o plataforma Tecnología (hardware y software) implementado por el área de TIC, con el objetivo de verificar que la plataforma tecnológica garantice un

funcionamiento continuo, disponibilidad y oportunidad de la información.

1.7 Presupuesto Tecnológico.

El auditor debe revisar que las inversiones en recursos tecnológicos hechas por las entidades del sector público, han contribuido a maximizar el desempeño de la organización y si éstas fueron administradas adecuadamente.

El área de Tecnología de Información y Comunicaciones debe concentrar un presupuesto tecnológico institucional que considere todas las necesidades de (hardware y software), para lo que, el auditor debe verificar que toda contratación se incluya y se autorice en el plan anual de compras.

El auditor con base a este plan debe evaluar el proceso de contratación, priorizando en el cumplimiento de las especificaciones técnicas, recepción del bien o servicio y utilidad de los mismos de acuerdo a las necesidades requeridas por las unidades solicitantes.

1.8 Planificación de TAACs.

Se debe evaluar una combinación apropiada de técnicas manuales y TAACs. Al determinar que se utilizarán Técnicas de Auditoría Asistidas por Computadora, debe considerarse lo siguiente:

- Conocimientos de computadoras, destreza y experiencia del auditor de TICs.

- Eficiencia y efectividad para el uso de las Técnicas de Auditoría Asistidas por Computadora y técnicas manuales.
- Nivel de riesgo de auditoría.

2. Seguimiento a Recomendaciones de Auditorías Anteriores.

El auditor de TIC´s deberá obtener informes de auditorías anteriores relacionadas con la gestión de las tecnologías de información y comunicación con el propósito de efectuar el seguimiento al cumplimiento de recomendaciones. En este caso, el auditor solicitará a los funcionarios actuantes los comentarios y las acciones implementadas para comprobar el cumplimiento de las recomendaciones y la evidencia que las respaldan, y se analizará para establecer una base de estos y el grado de cumplimiento de las referidas recomendaciones.

El auditor al comprobar que las recomendaciones se encuentran cumplidas, comunicará por escrito los resultados del seguimiento a los funcionarios involucrados con el cumplimiento, haciéndoles mención que se han implementado acciones tendientes al mejoramiento del control interno o de la gestión tecnológica en la entidad y deberá incluir en el informe final de auditoría un párrafo estableciendo que la entidad cumplió con las recomendaciones plasmadas en el informe de auditoría anterior.

En el caso que al realizar el análisis de las acciones implementadas en la entidad, éstas no son suficientes para cumplir con las

recomendaciones hechas en el informe auditoria anterior, se deberá de desarrollar un asunto de importancia relativa, que deberá incluirse en el informe final de auditoría, en un apartado donde se haga referencia a los resultados sobre el seguimiento a las recomendaciones de la auditoría anterior; detallando lo siguiente:

a) Identificación.

   Hará referencia al informe y período auditado al que se le está efectuando seguimiento.

b) Condición.

   Incluir la situación encontrada en la auditoría anterior.

c) Recomendación.

   Incluir la recomendación planteada en la auditoría anterior.

d) Comentarios de la administración.

   Debe describir la situación actual de las acciones tomadas por la administración, para cumplir con la recomendación.

e) Grado de cumplimiento

   Debe indicarse el grado de cumplimiento actual.

3. Análisis, Evaluación e Incorporación de Hallazgos de Auditoría elaborados por la Unidad de Auditoría Interna y Firmas Externas de Auditoría.

El auditor debe obtener de la entidad auditada los informes y papeles de trabajo de auditoría de tecnologías de información y comunicaciones emitidos por la Unidad de Auditoría Interna y las Firmas Externas de Auditoría, con el objetivo de analizar y evaluar los hallazgos con los respectivos atributos, su impacto, importancia relativa y la evidencia

de soporte, y así determinar los hallazgos que serán incorporados en el informe de auditoría.

El proceso de análisis y evaluación deberá plasmarse en papeles de trabajo que elaborará el auditor informático.

4. Plan de Trabajo de Auditoria TIC´s.

Después que los auditores han conocido la entidad y el área de tecnología de información y comunicaciones e identificado posibles asuntos de importancia (líneas preliminares a examinar) que hayan llamado la atención, se listan y se agruparán por proyectos, deberá de incluir su conocimiento y análisis en un documento metodológico que evidencia la estrategia y alcance de la auditoría, el contenido se describe a continuación:

- Antecedentes la entidad y el área TIC
- Organigrama de TIC
- Objetivos general y específicos de TIC
- Naturaleza y alcance de la auditoria
- Estrategia de la auditoría
- Enfoque de la auditoria
- Fundamento de la auditoría
- Agrupación de Asuntos de Importancia y Determinación de Proyectos a Examinar en la Fase de Análisis Previo.
- Leyes aplicables al proceso de la auditoria
- Recursos (humanos, materiales y técnicos) del equipo de auditoria
- Cronograma de trabajo
- Programa de auditoría para iniciar la etapa de análisis previo.

5. Análisis Previo.

Como resultado de los procedimientos aplicados al conocimiento y comprensión del área de Tecnología de Información y Comunicación y de la Plataforma Tecnológica de la entidad, se elaborarán programas de auditoría dirigidos a examinar lo que a criterio del equipo de auditoría les llamó la atención, para dirigir de forma adecuada los procedimientos que desarrollarán los objetivos de la auditoria.

5.1 Áreas preliminares a examinar.

5.1.1 Organización y Planificación de TI

El auditor debe de realizar una evaluación y análisis de la estructura organizativa y la planificación del Área de TIC, con el propósito obtener una definición clara de las funciones, líneas de autoridad y responsabilidad de las diferentes unidades que conforman el Área de Tecnología de Información y Comunicaciones, además se debe analizar si es recomendable la ubicación actual dentro del organigrama institucional o amerite que el Área de tecnología de información y comunicaciones debe estar al más alto nivel de la pirámide administrativa para cumplimiento de sus objetivos y cuente con el apoyo necesario de la máxima autoridad.

El auditor debe de constatar y analizar que el área de TIC ha implementado y está cumpliendo con los controles siguientes:

- ✓ Se debe evitar que una misma persona tenga el control de toda una operación.

- ✓ Las funciones de operación, programación y diseño de sistemas deben estar claramente delimitadas.
- ✓ Deben existir mecanismos necesarios a fin de asegurar que los programadores y analistas no tengan acceso a la operación del computador y los operadores a su vez no conozcan la documentación de programas y sistemas.
- ✓ Debe existir una unidad de control de calidad, tanto de datos de entrada como de los resultados del procesamiento.
- ✓ El manejo y custodia de dispositivos y archivos magnéticos deben estar expresamente definidos por escrito.
- ✓ Las instrucciones deben impartirse por escrito.

5.1.2 Procesamiento Electrónico de Datos.

Los auditores deberán revisar los controles en las operaciones del procesamiento electrónico de datos en los siguientes aspectos:

1.- Revisión de controles en el equipo.

Se hace para verificar si existen formas adecuadas de detectar errores de procesamiento, prevenir accesos no autorizados y mantener un registro detallado de todas las actividades del computador que debe ser analizado periódicamente.

2.- Revisión de programas de operación.

Se verificará que el cronograma de actividades para procesar los datos, asegure la utilización efectiva del computador.

3.- Revisión de controles ambientales.

Se hace para verificar si los equipos tienen un ambiente físico adecuado, es decir si se cuenta con aire acondicionado, fuentes de energía continua, extintores de incendios, etc.

4.- Revisión del plan de mantenimiento.

Se verificará que todos los equipos principales tengan un adecuado mantenimiento que garantice su funcionamiento continuo.

5.- Revisión del sistema de administración de archivos.

Se hace para verificar que existan formas adecuadas de organizar los archivos en el computador, que estén respaldados, así como asegurar que el uso que le dan es el autorizado.

6.- Revisión del plan de contingencias.

En esta sección se verificará si el plan de contingencia es apropiado para garantizar la continuidad del negocio, las operaciones y la recuperación de información ante contingencias humanas o naturales que puedan poner en peligro las operaciones, pérdida de información, infecciones de virus entre otras, el cual debe de contener como requisitos mínimos los siguientes:

- ✓ Considera requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TI.
- ✓ Cubre los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas.

- ✓ Considera los requerimientos de respuesta y recuperación para diferentes niveles de prioridad, por ejemplo, de una a cuatro horas, de cuatro a 24 horas, más de 24 horas y para periodos críticos de operación del negocio.
- ✓ Se ha centrado la atención en los puntos determinados como los más críticos en el plan de continuidad para construir resistencia y establecer prioridades en situaciones de recuperación.
- ✓ Procedimientos de control de cambios, para asegurar que el plan de continuidad se mantenga actualizado y que refleje de manera continúa los requerimientos actuales del negocio.

5.1.3 Evaluación de los Sistemas Informáticos.

- ✓ Evaluación de los diferentes sistemas informáticos en operación (flujo de información, procedimientos, documentación, redundancia, organización de archivos, estándares de programación, controles, utilización de los sistemas).
- ✓ Evaluación del avance de los sistemas informáticos en desarrollo y congruencia con el diseño general.
- ✓ Seguridad física y lógica de los sistemas informáticos, su confidencialidad y respaldos.

5.1.4 Controles de Sistema en Desarrollo y Producción

El auditor debe de verificar y asegurarse que el Área de Tecnología de Información y Comunicaciones ha justificado que los sistemas

informáticos adquiridos a terceros y desarrollados internamente han sido la mejor opción para la entidad y que proporcionen oportuna y efectiva información, y se han desarrollado bajo un proceso planificado y se encuentren debidamente documentado.

Procedimientos a seguir:

Asegurarse que los usuarios han participado en el diseño e implantación de los sistemas informáticos, pues aportan conocimiento y experiencia de su área y esta actividad coadyuva a una mejor cultura tecnológica en el cambio de los procesos institucionales.

Verificar que el área de auditoría interna ha formado parte del grupo de diseño para sugerir y solicitar la implantación de rutinas de huellas de auditoría.

- ✓ Evaluar si el desarrollo, diseño y mantenimiento de sistemas obedece a planes específicos, metodologías del ciclo de vida de desarrollo de sistemas, procedimientos y en general a normativa escrita y aprobada.
- ✓ Evaluar si cada fase concluida esta aprobada y documentada por los usuarios mediante actas u otros mecanismos, a fin de evitar reclamos posteriores.
- ✓ Constatar si los aplicativos antes de pasar a producción son probados con datos que agoten todas las excepciones posibles.
- ✓ Comprobar si todos los sistemas informáticos están debidamente documentados y actualizados.

- ✓ Evaluar si han implantado procedimientos de solicitud, aprobación y ejecución de cambios a programas, formatos de los sistemas en desarrollo.
- ✓ Verificar si el sistema informático es entregado al usuario previo entrenamiento y elaboración de los manuales de operación respectivos

Para el procesamiento electrónico de datos en los sistemas informáticos el auditor debe de considerar:

- ✓ Evaluar la validación de datos de entrada, procesamiento y salida, este proceso es realizado en forma automática.
- ✓ Verificar que la preparación de los datos de entrada sea responsabilidad de los usuarios y consecuentemente su corrección.
- ✓ Verificar la adopción de acciones necesaria para correcciones de errores.
- ✓ Evaluación de la planificación del mantenimiento del hardware y aplicativos informáticos, tomando todas las medidas de seguridad para garantizar la integridad.

5.1.5 Evaluación de los equipos

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

El auditor debe de constatar que el Área de la Tecnología de Información y Comunicaciones ha implementado controles tales como:

Controles de Adquisición

El propósito es asegurar que el hardware y software adquirido a terceros proporcione mayores beneficios que cualquier otra alternativa y garantizar la selección adecuada de equipos y sistemas informáticos.

Procedimientos a seguir:

- ✓ Revisión de un informe técnico en el que se justifique la adquisición del equipo, software y servicios informáticos incluyendo un estudio costo-beneficio.
- ✓ Formación de un comité que coordine y se responsabilice de todo el proceso de adquisición e instalación
- ✓ Elaborar un instructivo con procedimientos a seguir para la selección y adquisición de equipos, programas y servicios informáticos. Este proceso debe enmarcarse en normas y disposiciones legales.
- ✓ Revisar el respaldo de mantenimiento y asistencia técnica de los equipos informáticos.

Controles en el uso de Computadoras de Escritorio y Portátiles.

Es la tarea más difícil pues son equipos más vulnerables, de fácil acceso, de fácil explotación pero los controles que se implementen

ayudarán a garantizar la integridad y confidencialidad de la información.

Por lo que, el auditor mediante sus procedimientos de auditoría debe asegurase que el área de tecnología de información ha realizado lo siguiente:

- ✓ Adquisición de equipos de protección como reguladores de voltaje y de ser posible UPS.
- ✓ Vencida la garantía de mantenimiento del proveedor del equipo se debe proporcionar mantenimiento preventivo y correctivo.
- ✓ Establecimiento de procedimientos para la realización de respaldos de la información.
- ✓ Procedimientos e informes de revisión del software contenido en el computador, para asegurarse que el software instalado cuente con la respectiva licencia de uso.
- ✓ Mantener programas y procedimientos de detección e inmunización de virus en copias no autorizadas o datos procesados en otros equipos.
- ✓ Procesos de estandarización de sistemas operativos, software de ofimática, manejadores de base de datos y mantener actualizadas las versiones respectivas.

5.1.6 Evaluación de la Seguridad de la Información.

Los equipos informáticos son instrumentos que estructuran grandes cantidades de información, la cual puede ser confidencial para la entidad y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta; además pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de las

actividades de procesamiento electrónico de datos. Esta información puede ser de suma importancia, y al no contar con ella en el momento preciso puede provocar retrasos sumamente costosos.

Al auditar los sistemas informáticos, el auditor debe verificar y constatar lo siguiente:

- ✓ Que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión de virus.
- ✓ Que se hayan implementado procesos físicos y lógicos para la protección del hardware y datos procesados, así como a las instalaciones de ingreso al área de procesamiento de datos y servidores. Contemplando las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc.
- ✓ Implementación de mecanismos para garantizar la seguridad lógica del software, a la protección de los datos e información, procesos y programas, así como la restricción de usuarios no autorizados al acceso de la información.

5.2 Indicadores de Gestión (Eficiencia, Eficacia, Efectividad y Economía) aplicados al Área de Tecnología de Información y Comunicaciones

Los indicadores son semáforos de alarma, contienen información vital que alertan si la entidad gubernamental está administrando en forma deficiente sus objetivos estratégicos e identifica áreas débiles que pueden sujetas a una mejora continua.

Estos indicadores deben ser diseñados e implementados por las entidades públicas, la responsabilidad del auditor, es medirlos e interpretar los resultados obtenidos, para mejorar la gestión del Área de Tecnología de la Información y Comunicaciones (TIC´s).

La información utilizada para el desarrollo de indicadores incluye tanto elementos del plan estratégico de la entidad como aspectos operativos, mejor si se identifican con los puntos claves de la cadena causal interna: obtención de insumos e insumos, procesos o transformación de insumos, productos y servicios, efectos e impactos.

El auditor deberá evaluar el cumplimiento de la estructura de los indicadores de gestión, a la vez desarrollara una matriz de medición de los mismos, con el propósito de comprobar si estos están cumpliendo con los propósitos de implementación.

Estructura de un indicador adecuadamente compuesto:

Un indicador adecuadamente compuesto tiene la siguiente estructura:

1. **Nombre:** La identificación y diferenciación de un indicador es vital, y su nombre, además de concreto, debe definir claramente su objetivo y utilidad.
2. **Forma de cálculo:** Generalmente, cuando se trata de indicadores cuantitativos, se debe tener muy claro la fórmula matemática para el cálculo de su valor, lo cual implica la

identificación exacta de los factores y la manera como ellos se relacionan.

Esto, sin embargo, no es exclusivo de parámetros cuantitativos.

3. **Unidades de medida:** La manera como se expresa el valor cuantitativo de determinado indicador está dado por las unidades de medida, las cuales varían de acuerdo con los factores que se relacionan (horas laborales-funcionario, valor monetario, cantidad, días hábiles, etc.).
4. **Status, umbral y rango de gestión:** Esto requiere conocer las metas de objetivos estratégicos o de alcance institucional (qué, cuánto, cómo y cuándo), que serán a su vez el referente para la definición de las metas de los objetivos operativos.

5.3 Evaluación de Riesgos Tecnológicos

Riesgo

Evento fortuito e incierto resultante de acciones humanas o por la acción de una causa externa, que puede intervenir en el cumplimiento de la misión, visión, objetivos y metas que han sido definidos por la entidad gubernamental, causando perjuicios directos o indirectos.

El auditor debe cerciorarse que los riesgos tecnológicos han sido identificados por el área de tecnología de información y comunicaciones, estableciéndose el impacto y la ocurrencia de los mismos, la probabilidad o frecuencia de tal ocurrencia.

El auditor comprobará a través del análisis de riesgos que la unidad de TIC garantice, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, acceso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales, tanto por parte del personal interno como de terceros, para ello debe acatar lo dispuesto en las Políticas y Normas Institucionales de Seguridad Informática.

Como resultado del análisis y gestión de riesgos el auditor obtendrá el riesgo residual, orientando su examen a las acciones tomadas por la entidad para reducirlo, aceptarlo o transferirlo, implementándose controles internos para mitigarlo.

El auditor solicitará al área de tecnología de información y comunicaciones la identificación, análisis y gestión de riesgos tecnológicos que afecten el cumplimiento de los objetivos y metas del área y la entrega de servicios en la entidad.

Componentes del riesgo:

a) **Probabilidad:** Posibilidad de ocurrencia de un riesgo, medible a través de criterios de frecuencia o considerando la existencia de factores internos y externos, que propician el riesgo aún si éste no ha sucedido.
b) **Severidad:** Magnitud de los efectos o consecuencias que ocasionaría a la institución la ocurrencia de un riesgo.

c) **Nivel de riesgo:** Resultado de confrontar la severidad y la probabilidad con los controles existentes.

d) **Riesgos de Tecnología:** Se asocian con la capacidad de la entidad para que la tecnología disponible satisfaga las necesidades actuales y futuras de la institución y soporten el cumplimiento de la misión.

e) **Administración de Riesgos:** Proceso estructurado, consistente y continuo, implementado a través de toda la entidad para identificar, evaluar, medir y reportar amenazas y oportunidades que afectan el logro de los objetivos institucionales, a fin de proponer soluciones o alternativas para minimizar el impacto de los riesgos en el rendimiento institucional.

5.4 Evaluación de Control Interno Tecnológico.

El auditor debe evaluar y supervisar los controles de TIC que son parte integral del entorno de control interno de la organización, proponiendo al Área de Tecnología de Información y Comunicaciones consejos con respecto al diseño, implementación, operación y mejora de controles de TIC´s.

El control interno del Área de tecnología de información y comunicaciones está comprendido por **controles generales** (CPD, organización, implementación, seguridad de programas y datos, operación del computador, seguridad de comunicaciones y sistema operativo) diseñados para asegurar que los aplicativos

informáticos funcionan adecuadamente y **controles de aplicación** (Control de acceso, origen, entrada, proceso y salida de información) procedimientos diseñados para asegurar que las transacciones sean administradas de acuerdo con los objetivos específicos de control; que la información conserve todos sus atributos y características, y que los sistemas informáticos cumplan con los objetivos para los cuales fueron creados.

El auditor debe asegurarse que los controles internos diseñados por la institución, mitiguen en gran medida los riesgos residuales obtenidos en el análisis de riesgos, siendo factible y con menor inversión la administración de éstos, valor agregado que podrá denotar el auditor de TIC's.

La evaluación de Control Interno aporta a la entidad elementos de medición de la gestión informática y de la cultura informática; al Área de TIC´s le brinda indicadores de satisfacción de usuarios, tanto por las aplicaciones, como por el nivel de servicio que proporciona de la seguridad lógica y administración de plataformas tecnológicas, que los alerta sobre las posibles fallas de seguridad y le brinda retroalimentación sobre políticas y medidas de control, que podrían mejorar el funcionamiento de los equipos.

Esta revisión permite a la alta gerencia reforzar el Área de tecnología de información y comunicaciones, para que cumpla sus objetivos y soporte, las estrategias del negocio, mientras que al Área de tecnología de información y comunicaciones le brinda la

oportunidad de definir acciones preventivas y adoptar alternativas de mejora continua de sus servicios.

El factor crítico en el proceso de la auditoría es el conocimiento y evaluación del Control Interno Tecnológico y la elaboración de los programas de auditoría, por tal motivo es importante que el auditor informático, realice una revisión y evaluación detallada del control interno en las Tecnologías de Información y Comunicaciones (TIC´s) de las entidades públicas, en los siguientes puntos de control:

- ✓ Gerenciales.
- ✓ Desarrollo y Mantenimiento de Sistemas Informáticos.
- ✓ Operación.
- ✓ Aplicaciones.
- ✓ Tecnología.
- ✓ Continuidad y Oportunidad del Servicio.
- ✓ Cumplimiento de Objetivos estratégicos y operativos

Se deberá realizar una revisión y evaluación de las condiciones de seguridad lógica y física, que garanticen que las medidas de seguridad en las plataformas tecnológicas estén siendo administradas de tal forma que cumplan con los propósitos para lo cual fueron diseñadas y gestión adecuada de los procesos sustantivos sistematizados de la entidad y las metas de la organización y los objetivos de los proyectos tecnológicos implementados.

Esta evaluación tiene un enfoque técnico y es recomendable como medida preventiva, para reducir el riesgo de los ataques externos e internos hacia la información de la entidad, que puede afectar la continuidad de las operaciones.

El auditor debe asegurarse que el control interno haya sido implementado por la administración de la entidad y monitoreado periódicamente como medida preventiva, para anticiparse a situaciones que pongan en peligro la información o la continuidad de las operaciones de las entidades públicas; así como para identificar a tiempo oportunidades de mejora o desviaciones de las estrategias de TIC´s.

5.5 Normativa Técnica de Control Interno y Fuentes de Información.

En la nueva era de la información electrónica y de los recursos tecnológicos en las operaciones y prestación de servicios de las entidades públicas, es necesario contar con un marco normativo técnico que regule el uso, seguridad, administración y gestión de la información y de los recursos tecnológicos, con el propósito de resguardar la información ante ataques cibernéticos, usurpación de archivos confidenciales o bien detener por completo los sistemas de la organización, dañando el software o el hardware de la misma. Estas y otras muchas amenazas forman parte del peligro a los que se ven expuestas las entidades públicas, no solo por parte de personas ajenas a la institución, sino que hasta los

mismos trabajadores de la entidad podrían infringir las políticas implementadas y hacerle daño.

La carencia de aspectos técnicos jurídicos en la aplicabilidad de los procedimientos de auditoría en los procesos sistematizados hace que se vuelva vulnerable dicha auditoria, por tal motivo antes de realizar este tipo de auditoría, los Entes Fiscalizadores deben implementar en el sector público y municipal como primer paso las Normas Técnicas de Control Interno Tecnológicas, con el propósito de constituir el marco básico normativo técnico, para promover la eficiencia y eficacia en el desarrollo de las actividades y operaciones tecnológicas, obtención de confiabilidad y oportunidad de la información, y el cumplimiento con leyes, reglamentos, aspectos administrativos y otras regulaciones aplicables, para proporcionar seguridad razonable en la consecución de los objetivos establecidos y metas programadas.

La normativa técnica es elaborada internamente dentro del Área de Tecnología de Información y Comunicaciones, autorizada por la máxima autoridad de la entidad y divulgada a los usuarios de los servicios tecnológicos. **(ANEXO 2)**

5.6 Comunicación de Asuntos de Importancia Relativa de TIC´s.

El auditor en el transcurso de la auditoria, mantendrá constante comunicación con los servidores de la entidad u organismo

auditado, proporcionándoles oportunidad para que presenten pruebas o evidencias documentadas, con la finalidad de obtener mayores elementos de juicio, que nos permitan brindar conclusiones y recomendaciones adecuadas y que estos a la vez puedan ser utilizados por los tomadores de decisiones, para mejorar su gestión.

Mencionando en dicha comunicación que con base a los procedimientos y pruebas de auditoría aplicados, se han identificando asuntos de importancia relativa relacionados a los objetivos de nuestra Auditoría de Gestión, los cuales se hacen de su conocimiento, además se debe de hacer mención el nombre de la normativa relacionada a la comunicación con los funcionarios.

Además se hace con el propósito de obtener evidencia convincente de las causas que están originando los asuntos de importancia (condiciones, deficiencias, observaciones), para dirigir sus procedimientos de auditoría a la obtención de evidencia respectiva.

5.7 Informe Ejecutivo de Análisis Previo.

El producto que se obtendrá del **Análisis Previo,** será un informe ejecutivo que contendrá los asuntos de importancia identificados y agrupados por proyectos de las áreas vulnerables o de impacto determinados, al aplicar los procedimientos de auditoría de

análisis previo y donde se profundizará en la fase de ejecución de la auditoría.

El objetivo del informe ejecutivo es que el Director lo autorice y tenga una visión general del proceso de la auditoria, pueda comprender en una sola lectura en qué consisten los procedimientos aplicados y los ASUNTOS DE IMPORTANCIA RELATIVA DE TIC´s obtenidos, y deberá contener en su estructura como mínimo lo siguiente:

Introducción

En esta sección se presenta, brevemente, el objetivo general de cada proyecto de análisis previo, objetivos específicos y restricciones.

1. Datos Generales

La descripción del Área de Tecnología de ~~la~~ Información.

En qué consiste Área de Tecnología de Información, los productos o los servicios que ofrecen, cuáles son sus principales funciones.

Filosofía del Área de Tecnología de Información y Comunicaciones.

Esta sección incluirá misión, visión, principios y/o valores, objetivos estratégicos, acciones estratégicas, objetivos a corto plazo, metas, indicadores de gestión tecnológica y ubicación organizativa del Área de Tecnología de Información y Comunicaciones.

Proyectos Tecnológicos ejecutados o a ejecutar.

Aquellos que van a desarrollar que sea innovador y novedoso, y que van permitir a sistematizar los procesos de negocio.

El presupuesto de las Inversiones requeridas.

Se deben detallar los presupuestos de inversión que se ejecutarán en determinado periodo por parte del Área de tecnología de información y comunicaciones.

Principales logros de la entidad y del área de Tecnología de la Información y Comunicaciones.

Se deben resaltar las realizaciones sobre la implementación y el uso de las tecnologías de información y comunicaciones en los procesos de negocio y de soporte en el cumplimiento de metas y objetivos en el periodo de la auditoria que tenga la entidad o el Área de Tecnologías de Información y Comunicaciones.

2. Desarrollo

Se deben describir detalladamente los procedimientos de auditoría y cómo se fueron desarrollando. Pueden ser necesarias figuras para describir lo realizado en cada etapa. Si el trabajo lo amerita puede dividirse en más de un punto.

Áreas de Impacto o Vulnerables.

Se deberá describir y listar todas las áreas y procesos que impactan negativamente la gestión tecnológica de la entidad y que

no permiten alcanzar los objetivos y metas previstos en los planes del Área de Tecnología de Información y Comunicaciones, agrupándolas por proyectos, con el propósito de dirigir la auditoria a las áreas de impacto o vulnerables identificadas.

El equipo de trabajo de Auditoria

Detallar los auditores con las respectivas profesiones o especialidades que ejecutaran los proyectos o fases de la auditoria.

Anexos

Lo que los auditores consideren importante de anexar.

6. Conclusiones y Recomendaciones.

Las conclusiones deben redactarse de una forma clara y entendible y no ser interpretadas por un tercero. Los auditores sustentan su trabajo en las conclusiones basadas en indicadores de gestión del Área de Tecnología de Información y Comunicaciones.

Las recomendaciones son emitidas por el Director de Auditoria que tiene a cargo el equipo de auditoria, para agregar valor a la estrategia de auditoría, naturaleza y alcance y determinación de los procedimientos de auditoría que se realizarán en la fase de ejecución de la entidad auditada.

CAPITULO IV
DE EJECUCIÓN

1. Pruebas de Auditoría asistidas por Computadora.

Una vez concluido el análisis previo, el auditor debe diseñar un programa de auditoría dirigido a las áreas de mayor vulnerabilidad y/o impacto identificadas al confrontar los riesgos versus controles tecnológicos y se debe investigar a profundidad y obtener evidencia de las causas que originan una debilidad dentro de la Gestión a las Tecnologías de Información y Comunicaciones, para lo cual, el auditor podrá apoyarse en las Técnicas de Auditoría Asistidas por Computadora (TAACs).

Estas técnicas son utilizadas en el desarrollo de procedimientos de auditoría, incluyendo:

- Procedimientos de revisión analíticos
- Pruebas de cumplimiento de los controles generales de tecnología de información y comunicación
- Pruebas de cumplimiento de los controles de aplicación de tecnología de información y comunicación
- Pruebas de penetración
- Verificación Ocular (Observación, Comparación)
- Verificación Física (Inspección)
- Verificación Oral (Indagación, entrevista, encuestas)
- Verificación Escrita (Análisis, Confirmación, Tabulación, conciliación)

- Verificación Documental (Comprobación, Cálculo, Rastreo, Revisión Selectiva).

1.1 Pasos para desarrollar una TAAC.

1. Defina detalladamente el objetivo de lo que se va a examinar
2. Determine las técnicas de auditoria que deberá automatizar.
3. Identifique las fuentes de los datos.
4. Identifique sus atributos.
5. Solicite la documentación de sistema o confeccione el modelo "entidad – relación
6. Analice la forma como automatizara las técnicas de auditoria, solución lógica.
7. Seleccione la herramienta computacional que más se adecue a lo requerido.
8. Implemente la herramienta computacional siguiendo los pasos del modelo lógico
9. Prueba y verifique los resultados.
10. Ya tiene confeccionada su "TAAC"

1.2 Seguridad de datos y Técnicas de Auditoría Asistidas por Computadora.

Cuando las TAAC´s son utilizadas para extracción de información y análisis de datos, el auditor de TIC´s debe verificar la integridad del sistema de información y el ambiente tecnológico donde son extraídos los datos.

Las Técnicas de Auditoría Asistidas por Computadora pueden ser utilizadas para extraer programas o sistemas de información sensibles y datos en producción que deben ser mantenidos en forma confidencial.

El auditor de TIC´s debe entender la clasificación de información de la entidad y políticas llevadas para salvaguardar adecuadamente los programas y/o sistemas de información y datos en producción con un nivel apropiado de confidencialidad y seguridad.
El auditor de TIC´s debe considerar el nivel de confidencialidad y seguridad requerido por la organización propietaria de los datos y cualquier legislación pertinente, y debe consultar a otros, tanto como el consejo y administración sea necesaria.

El auditor debe utilizar y documentar los resultados de los procedimientos, para proveer sobre la marcha integridad, confiabilidad, utilidad y seguridad de la TAACs. Por ejemplo, esto debe incluir una revisión de programas de mantenimiento y control de cambio de programas sobre el software de auditoría para determinar que solo los cambios autorizados han sido hechos por las TAACs.

2. Evaluación y recolección de Evidencia.

El auditor deberá obtener la certeza (evidencia) suficiente y apropiada a través de la ejecución de sus procedimientos para permitirle emitir

las conclusiones para fundamentar su opinión sobre la operatividad de la Gestión en Tecnología de Información y Comunicaciones.

Evidencia Suficiente.

Se entiende por suficiente, aquel nivel de evidencia que el auditor debe obtener a través de sus pruebas de auditoría, para llegar a conclusiones razonables sobre el uso de las Tecnologías de información y comunicaciones que se someten a examen. Este profesional no pretende obtener toda la evidencia existente, sino aquella que cumpla, a su juicio profesional, con los objetivos de su examen.

Es necesario confiar en evidencias que son más convincentes que concluyentes, por tanto, con frecuencia puede buscar evidencia de diferentes fuentes o de distinta naturaleza para apoyar un mismo hecho o dato. La evidencia es adecuada cuando sea pertinente para que el auditor emita su juicio profesional.

El auditor en tal situación debe valorar que los procedimientos que aplica para la obtención de la evidencia sean los convenientes en cada circunstancia.

Evidencia adecuada.

El concepto de "adecuación" de la evidencia es la característica cualitativa, en tanto que el concepto "suficiencia" tiene carácter cuantitativo. La combinación de ambos elementos debe proporcionar al auditor el conocimiento necesario para alcanzar una base objetiva de juicio sobre los hechos sometidos a examen.

La evidencia es adecuada cuando sea pertinente para que el auditor emita su juicio profesional.

Documentación de la evidencia

La evidencia obtenida deberá recogerse en los papeles de trabajo del auditor como justificación y soporte del trabajo efectuado y para documentar todos aquellos asuntos de importancia relativa que no está conforme a la normativa técnica y legal en la operatividad y uso de las tecnologías de información y comunicaciones.

Protección y Conservación

La evidencia de auditoría deberá estar protegida contra el acceso no autorizado y la modificación.

La evidencia de auditoría debe mantenerse después de la finalización del trabajo de auditoría, mientras sea necesario para cumplir con todas las leyes aplicables, reglamentos y políticas.

3. Cumplimiento de Políticas y Procedimientos.

En el transcurso de la auditoría de gestión a las tecnologías de información y comunicaciones, el auditor debe cerciorarse mediante los procedimientos plasmados en los programas de auditoría, el cumplimiento de políticas y procedimientos para el uso de la información y de las tecnologías de información y comunicaciones (TICs) en la organización, y al determinar que no se están cumpliendo, el auditor lo evidenciará aplicando diferentes técnicas de auditoría y lo comunicará al funcionario público responsable del incumplimiento para

determinar las causales por las cuales no se están cumpliendo con lo plasmado en la normativa interna y externa aplicable, esto a su vez le sirve al auditor para obtener documentación que respalde su juicio y su opinión profesional con respecto al uso de la información y de la tecnología de información y comunicaciones.

4. Carta de Salvaguarda.

Antes que el equipo de auditoría se retire de la entidad, deberán obtener la carta de salvaguarda, relacionada con la gestión de tecnología de información y comunicaciones, suscrita por el Titular de la Entidad o por el funcionario a quien él designe, con la finalidad que el equipo de auditores se resguarden que toda la información relacionada con las tecnologías de información y comunicaciones solicitada, ha sido prevista por la administración.

CAPITULO V
DE INFORME

1. Resultados Preliminares de Auditoría (Informe Previo).

Esta etapa finaliza con los procedimientos de auditoría de la fase de ejecución, y comienza con la elaboración del Informe previo de Auditoría de resultados preliminares (en algunos países se le conocen como: informe previo, pre-informe, borrador de informe, entre otros), el jefe de equipo agrupa todos los asuntos de importancia (condiciones, deficiencias, observaciones) que incumplieron las

disposiciones relacionadas con aspectos de control interno y/o de cumplimiento con leyes, reglamentos legales y técnicos u otras disposiciones aplicables que dieron origen a la condición (Criterio), con la documentación que los respaldan y que los auditores determinaron al aplicar sus procedimientos de auditoría y se comunicarán a la máxima autoridad de la entidad y a los funcionarios actuantes responsables, esto se hace para garantizarse que dichos funcionarios tuvieron la oportunidad de defensa y convocándolos a una lectura de los resultados obtenidos y previos de auditoría para que emitan sus comentarios de defensa respectivos.

Para que un asunto de importancia (condiciones, deficiencias, observaciones), sea incluido en el Informe previo de Auditoría de resultados preliminares e Informe de Auditoría deberá estar estructurado con todos sus atributos (Condición, Criterio, Causa, Efecto, Comentarios de la Administración, Comentarios del Auditor y Recomendaciones).

Las recomendaciones y conclusiones hechas por los auditores deberán ser viables y factibles para que éstas sean atendidas por la administración y que sean de fácil comprensión y análisis para terceras personas y auditores que verificarán el cumplimiento en auditorias recurrentes.

El informe previo de Auditoría de resultados preliminares deberá tener un formato uniforme y estar dividido por secciones para facilitar al funcionario lector una rápida comprensión del contenido del informe, y contendrán los principios y estructuras descrita en el Informe de Auditoría.

2. Carta de Gerencia de Asuntos de Importancia Relativa.

Al finalizar la fase de ejecución, se elabora una carta de gerencia, en la cual se comunicará a la administración todos aquellos asuntos de menor importancia, estos asuntos de menor importancia son riesgos que pueden ser administrados y que a juicio del auditor no son de impacto en la gestión de las tecnologías de información y comunicaciones.

Este documento incluye la descripción de los asuntos de menor importancia (Condición) determinados y que no clasifican para constituirse como hallazgo y requieren de atención por parte de la administración para que en el futuro próximo no afecten el cumplimiento de la Misión, Visión, Objetivos y Metas de la entidad, al detallar estos asuntos menores, deberán incluir las disposiciones relacionadas con aspectos de control interno, leyes, reglamentos u otras disposiciones aplicables (Criterio) que se incumplieron y que originaron la condición, las cuales al ser superadas mejorarían la gestión tecnológica institucional, fortaleciendo el sistema de control interno, bajo responsabilidad de la máxima autoridad de esa Entidad.

3. Informe de Auditoría.

Posterior a la lectura del informe previo de Auditoría de resultados preliminares (Pre Informe, Borrador de Informe) se analizan los comentarios y documentación presentada por la administración, y se

elabora el Informe de Auditoría que contiene los resultados finales de la auditoría que no fuesen superados.

Se comunicarán los resultados al máximo nivel de dirección de la entidad auditada y otras instancias administrativas, así como a los funcionarios involucrados en los asuntos de importancia relativa (observaciones) que correspondan, cuando esto proceda.

El informe de Auditoría debe tener un formato uniforme y estar dividido por secciones para facilitar al funcionario lector una rápida comprensión del contenido del informe.

El informe de Auditoría debe cumplir con los principios siguientes:

- Que se emita por el jefe de grupo de los auditores actuantes.
- Por escrito.
- Oportuno.
- Que sea completo, exacto, objetivo y convincente, así como claro, conciso y fácil de entender.

  El hecho de que un Informe sea Conciso, no significa que su contenido sea corto, lo que se quiere es que su contenido sea breve, ya que muchos informes pueden ser amplios porque las circunstancias así lo requieren; sin embargo no deben incluir hechos impertinentes, superfluos o insignificantes.
- Que todo lo que se consigna esté reflejado en los papeles de trabajo y que responden a hallazgos relevantes con evidencias suficientes y competentes.
- Que refleje una actitud independiente.
- Que muestre la conclusión u opinión de los resultados o evaluación de la Auditoría.
- Distribución rápida y adecuada.

El informe de auditoría deberá ser estructurado y tendrá como mínimo requerido lo siguiente:

- Nombre de la organización
- Destinatario del Informe
- Alcance de la Auditoría
- Objetivos de la Auditoría
- Período auditado
- Naturaleza, plazo y extensión de las labores de auditoría
- Hallazgos
- Conclusiones
- Recomendaciones
- Seguimiento Recomendaciones de Informes de auditorías anteriores (acciones implementadas)
- Firma
- Fecha
- Distribución del Informe de acuerdo a los mecanismos de cada Contraloría

II. CONCLUSIONES

La auditoría de Gestión a las Tecnologías de Información y Comunicaciones, es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

La auditoría de Gestión a las Tecnologías de Información y Comunicaciones, deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específicos, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información, contribuye con la dirección al logro de una administración más eficaz, además de valorar los métodos y desempeño en todas las áreas orientadas a la informática, los factores de la evaluación abarcan el panorama económico, determinar deficiencias causantes de dificultades, sean actuales o en potencia, las irregularidades, descuidos, pérdidas innecesarias, actuaciones equivocadas, deficiente colaboración de lo que es una buena organización de la tecnología de información.

III. APLICABILIDAD EN EL CAMPO DEL CONTROL GUBERNAMENTAL.

Este manual de Auditoría de Gestión a las Tecnologías de Información y Comunicaciones, es aplicable al campo gubernamental por la creciente disponibilidad, transacciones económicas y uso de información en forma electrónica y de procesos sistematizados y de comunicación que son capaces de satisfacer las necesidades de los usuarios (ciudadanos) que hacen uso de las tecnologías de la información y comunicaciones (TIC´s), es decir, las instituciones gubernamentales dependen cada vez más de la tecnología de la información para la prestación de los servicios públicos y municipales, éstas tienen una importancia vital en la misión, visión y en los objetivos de las organizaciones públicas y municipales y su aplicabilidad dependerá del grado de madures en tecnología que se tenga en cada región.

Es importante mencionar que actualmente en algunas unidades de Auditoria Interna de las entidades públicas y gubernamentales no se practica como tal una auditoria de gestión a las tecnologías de información y comunicaciones, ya que únicamente realizan un tipo de examen de control interno y de cumplimento a leyes y reglamentos aplicables al área de tecnología de la entidad.

IV. BIBLIOGRAFÍA

- http://www.geocities.com/lsialer/NotasInteresantes.htm
- http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtm
- http://www.monografias.com/trabajos/maudisist/maudisist.shtml
- http://www.slideshare.net/alafito/niasauditsist.
- Propuesta de Criterios Técnicos de Control Interno del Área de Tecnología de la Información, publicado en la Revista - Transparencia año 3 No. 7 Enero 2008 y Publicorte No. 27 año 7 Diciembre de 2007-Enero 2008 de la Corte de Cuentas de la Republica de El Salvador
- www.intosai.org - Normas de Auditoría de la Organización Internacional de Entidades Fiscalizadoras (INTOSAI)
- http://www.geocities.com/lsialer/NotasInteresantes.htm.
- http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml.
- http://www.monografias.com/trabajos/maudisist/maudisist.shtml
- Directriz 3 emitida por ISACA, Uso de Técnicas Asistidas por Computadora (TAACs)
- Norma de Auditoría de SI, Documento S15, Controles de Tecnología de Información, emitida por ISACA.
- Norma de Auditoría Reporte, Documento S7, emitido por ISACA.
- Seminario de "Auditoría de Sistemas de Información Computarizados", impartido por el Instituto Salvadoreño de Contadores Públicos en septiembre de 2010.

V. ANEXOS

ANEXO 1

FORMATO DE PAPELES DE TRABAJO

En general, todo papel de trabajo electrónico debe contener como mínimo:

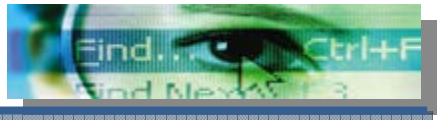
- ✓ *Título del Ente Fiscalizador y la unidad a la cual pertenece el auditor* que elabora los papeles de trabajo con sus respectivos logos de país y del ente fiscalizador.

- ✓ *Encabezado:* incluirá el nombre de la entidad pública, período de la auditoria, tipo de auditoría y área o componente específico, objeto de la auditoría.

- ✓ *Referencias:* cada papel de trabajo tendrá su propia referencia, y deberá indicar las hojas de trabajo relacionadas de acuerdo con un sistema de referencias cruzadas.

- ✓ *Fecha e Identificación de quién preparó el papel de trabajo:* Mediante rúbrica de la persona que ha contribuido a su elaboración, así como la fecha de realización.

- ✓ *Fecha e Identificación de quién supervisó el trabajo:* Mediante iniciales de la persona que revisó el trabajo realizado, como constancia de la supervisión efectuada.



- ✓ *Referencia al paso del programa de trabajo:* Para conocer el objetivo de preparación de la cédula.

- ✓ *El análisis realizado:* Estará en función a la ejecución de los procedimientos de auditoría para cumplir con lo definido en los programas de trabajo.

- ✓ *Método de muestreo:* Cuando sea aplicable será necesario hacer referencia al método de muestreo aplicado.

- ✓ *Explicación de las marcas de auditoría utilizadas:* En la parte inferior de la cédula se deberá realizar una descripción del significado de las marcas de auditoría utilizadas, en el caso de que esta explicación se encuentre en otra cédula se hará referencia a la misma.

- ✓ *Conclusiones:* Cuando corresponda, se realizará una exposición de los resultados logrados con el trabajo, una vez finalizado.

- ✓ La referencia de papeles de trabajo electrónicos en la auditoria operacional o de gestión se realizará, utilizando las herramientas automáticas de ofimática o bien referencia automatizada de un software específico.

ANEXO 2

Criterios Técnicos del Área de Tecnologías de Información y Comunicaciones.

Se proponen criterios técnicos iniciales para gestionar la Infraestructura Tecnológica y de los procesos sistematizados en el sector público y municipal.

ADMINISTRACIÓN DEL ÁREA DE TECNOLOGIA DE INFORMACION

El Área de TI debe realizar un proceso de panificación de TI de acuerdo con la planeación estratégica institucional, que facilite la consecución de sus de sus logros futuros.

La entidad debe procurar que a través del Manual de Organización, Funciones y Planes de Trabajo, se facilite la consecución de los objetivos planteados; para esto la entidad debe:

a) Velar porque la ubicación del área de TI, se encuentre en un nivel razonable de independencia funcional dentro de la estructura organizacional.
b) Definir y mantener actualizado el manual de puestos para el personal de TIC´s, de manera que las funciones y responsabilidades queden claramente establecidas.
c) Definir los procedimientos que permitan la contratación y adquisición de recursos de TIC´s.
d) Establecer una metodología que permita administrar adecuadamente los proyectos internos y externos (outsourcing), de acuerdo con los

recursos proyectados e invertidos.

e) Elaboración de Presupuesto del área de tecnología de la Información que incluyan los proyectos tecnológicos viables a desarrollar el cumplimiento de los objetivos estratégicos y operativos de la institución en el periodo financiero y debe de estar acorde con el plan de compras institucional.
f) Elaborar un plan de Trabajo diseñado de tal manera que defina los objetivos a cumplir y alineado con los objetivos estratégicos y/o operativos institucionales, actividades a desarrollar, programación, indicadores de cumplimiento.

La entidad debe procurar que los miembros de la organización actúen de modo que contribuyan al logro de los objetivos, establecer y comunicar los objetivos de la administración y las políticas de TIC´s, a los niveles pertinentes y contar con personal técnicamente capacitado o en su ausencia contratarlo externamente.

La entidad implantará los mecanismos de control necesarios para la supervisión y control de las tareas del área de TI; para ello deberá:

a) Verificar el cumplimiento de los controles y objetivos establecidos para los procesos de TIC´s.

b) Contar con un contrato vigente de prestación de servicios para el caso en que sus servicios de TIC´s no sean propios, verificando el cumplimiento del mismo.

c) Velar por el cumplimiento de sus obligaciones legales, regulatorias y contractuales, en los plazos y formas establecidas, así como las que terceros han establecido con la entidad.

La entidad que subcontrate parte o la totalidad de su procesamiento de datos en nuestro país, deberá incluir en los contratos que suscriba, una cláusula que permita a la entidad auditada la supervisión de las tareas contratadas en las instalaciones del proveedor.

SEGURIDAD LÓGICA Y ACCESO A LOS DATOS

El Área de TIC´s de la entidad administrará adecuadamente la seguridad lógica de sus recursos; para esto deberá:

a. Establecer políticas y procedimientos que permitan identificar, autenticar y autorizar el acceso a los sistemas de información, sistemas operativos y bases de datos.
b. Establecer políticas y procedimientos que permitan dar seguimiento a las transacciones que se ejecutan en los sistemas de información, bases de datos y sistemas operativos.

Se debe mantener una adecuada seguridad en todos aquellos puntos con acceso a redes públicas de datos; definiendo controles que permitan restringir el tráfico hacia dentro y fuera de la red institucional (Pared de fuego); Establecer políticas y procedimientos de prevención, detección y corrección de virus y Establecer políticas y procedimientos que regulen la utilización del correo electrónico.

SEGURIDAD FÍSICA

El Área de TIC´s debe establecer políticas y procedimientos relacionados con la ubicación, construcción, acceso físico a dicha Área.

El Área de TIC´s debe contar con procedimientos de control que regulen las condiciones ambientales del área, que proporcionen un ambiente físico conveniente para su funcionamiento y protejan los recursos materiales y al personal de TIC´s contra peligros naturales o fallas humanas.

El Área de TIC´s debe de elaborar y ejecutar un plan de Mantenimiento de Equipo Informático; debidamente diseñado con objetivos, políticas, prioridades, programación de actividades en el que se identifique a los responsables de ejecutarlas y la determinación de los costos estimados; además, la identificación de metas programadas formuladas de manera precisa, factible, viable y medible, para que se pueda ejercer un seguimiento y evaluación de objetivos sobre su cumplimiento, para la toma de decisiones a efecto de orientar adecuada y oportunamente los recursos asignados. Este plan deberá ser autorizado por la máxima autoridad de la entidad y ser comunicado a los niveles pertinentes.

El área de TIC´s deberá de contar con la documentación de soporte de las operaciones que realicen (Físicas o Electrónicas), ya que con ésta se justifica e identifica la naturaleza, finalidad y resultado de la actividad realizada; asimismo, contiene datos y elementos suficientes que facilitan su análisis. La documentación debe estar debidamente custodiada y contar

con procedimientos para su actualización oportuna.

SISTEMAS DE INFORMACIÓN

El Área de TIC´s debe procurar, a través de procedimientos, el diseño e implementación de sistemas de información sean eficaces, seguros, íntegros, eficientes y económicos, que impidan la modificación no autorizada; asimismo, se ajuste al cumplimento de las leyes, reglamentos y normativa vigente que les sean aplicables; para lo cual será necesario que se implemente:

a) Implementar una metodología para el ciclo de vida del desarrollo de sistemas, que asegure la calidad de los sistemas de información y satisfaga los requerimientos del usuario.
b) Definir una adecuada separación de los ambientes de desarrollo y producción, de forma que el personal de desarrollo no tenga acceso al ambiente en producción.
c) Se deberá definir procedimientos de actualización en los manuales de usuario y técnico, para el uso de los sistema en producción y que se se encuentra documentado el Control de cambios (versiones del Sistema) y los requerimientos se encuentren autorizados, realizados en el Sistema dentro del sistema.
d) Diseñar lineamientos para verificar que todas las transacciones efectuadas por los usuarios de los sistemas posean huellas o pistas de auditoría que permitan rastrear a los responsables de ingresar, eliminar y modificar los registros en las bases de datos.

El Área de TIC´s debe velar por la adecuada disponibilidad, capacidad y el

desempeño de los sistemas de información.

El Área de TIC´s debe contar con políticas y procedimientos relacionados con la captura, actualización, procesamiento, almacenamiento y salida de los datos, que asegure que los mismos permanezcan completos, precisos, confiables y válidos.

SOFTWARE Y BASES DE DATOS

El Área de TIC´s administrará adecuadamente sus bases de datos, y se requiere que se realice lo siguiente:

a) Definir la arquitectura de información para organizar y aprovechar de la mejor forma los sistemas de información.
b) Establecer políticas y procedimientos actualizados relacionados con la instalación, administración, migración, mantenimiento y seguridad de las bases de datos.
c) Definir mecanismos para controlar la integridad, disponibilidad, seguridad, capacidad y el desempeño de las bases de datos.
d) Elaboración de respaldos y definición de períodos de almacenamiento y eliminación de información, acorde con los requerimientos legales de la entidad.

El Área de TIC´s debe definir políticas y procedimientos para la adecuada instalación, mantenimiento y administración de software debidamente autorizado. Además, todo software deberá actualizarse con las últimas mejoras de seguridad publicadas por el proveedor, de la versión que están utilizando y que todavía cuenta con soporte por parte del proveedor. Lo anterior con el fin de reducir su vulnerabilidad, producto de las deficiencias

en los sistemas de seguridad, sistemas operativos, base de datos, antivirus, entre otros.

HARDWARE, REDES y COMUNICACIONES

La entidad debe administrar adecuadamente el hardware, las redes y las líneas de comunicación. Para lo cual deberá:

a) Realizar estudios de capacidad y desempeño del hardware y las líneas de comunicación, que permitan determinar en forma oportuna, necesidades de ampliación de capacidades o actualizaciones de equipos.
b) Establecer mecanismos para procurar que todas las redes instaladas, ya sean eléctricas, de voz o de datos, cumplan con los requerimientos mínimos vigentes de cableado estructurado. Entre estos deberán considerarse la documentación, el etiquetado, ductos para el cableado y el aterrizamiento del mismo.
c) Establecer políticas y procedimientos para la instalación y mantenimiento del hardware y su configuración base, que proporcionen la plataforma de TIC´s apropiada para soportar las aplicaciones de la entidad y reduzcan la frecuencia e impacto de las fallas de desempeño del hardware.

El Área de TIC´s debe administrar adecuadamente los puntos de red y switch es de red, para lo cual será necesario:

a) Establecer políticas y procedimientos para la ubicación, protección y mantenimiento de los puntos de red y switches.
b) Mantener en línea las estaciones de trabajo con los sistemas de

información de la entidad, de tal forma que en todo momento se cuente con la información oportuna, confiable y actualizada.

c) Establecer políticas y procedimientos para la comunicación al cliente (usuario) sobre el uso adecuado de las estaciones de trabajo y sistemas lógicos.

CONTINUIDAD DE LAS OPERACIONES

El Área de TIC´s debe establecer y mantener actualizadas políticas y procedimientos para el respaldo y recuperación de la información, que le permitan tener acceso a la misma durante periodos de contingencias, causados por desperfectos en los equipos, pérdida de información u otras situaciones similares.

El Área de TIC´s debe establecer un plan de continuidad o contingencia, viable donde se detallen acciones, procedimientos y recursos financieros, humanos y tecnológicos que considere los riesgos posibles, que afecten de forma parcial o total la operativa normal de los servicios de TIC´s categorizando el tipo de acción a realizar en cuanto a la medición en tiempo y recurso financiero para el restablecimiento de las operaciones tecnológicas. Este plan deberá ser autorizado por la máxima autoridad de la entidad y ser comunicado a los niveles pertinentes. Además, este plan debe probarse y actualizarse atendiendo la realidad tecnológica de la entidad al menos una vez al año.

El Área de TIC´s debe contar con una infraestructura tecnológica adecuada, que contemple el suministro de energía eléctrica para la

continuidad del negocio en caso de fallas temporales en la red eléctrica.

La entidad debe contar con cobertura de seguros para los principales equipos de cómputo y comunicaciones que permita mitigar el riesgo provocado ante cualquier tipo de contingencia y desastre natural (incendio, impacto de rayo, explosión, explosión, humo, gases o líquidos corrosivos, corto circuito, variaciones de voltaje, huelga, motín, robo, asalto y fenómenos naturales).

SERVICIOS POR INTERNET ~~y~~ Y CORREO ELECTRÓNICO INTERNO.

El Área de TIC´s debe administrar adecuadamente la seguridad lógica de los servicios por Internet y correo electrónico interno. Para esto se debe:

a) Implementar mecanismos de seguridad física y lógica que protejan la integridad y privacidad de la información sensible cuando el canal de transmisión sea internet.
b) Implementar y dar mantenimiento a los mecanismos de seguridad en todos aquellos puntos con acceso al servicio por internet. Estos mecanismos deberán probarse al menos dos veces al año.
c) Establecer procedimientos para uso y asignación del Internet y correo institucional.
d) Elaborar procedimientos para la estandarización para la creación y acceso de usuarios de red Institucional.

El Área de TIC´s debe considerar dentro de plan de continuidad o contingencia, un apartado donde se detallen acciones, procedimientos y recursos que consideren los riesgos posibles, que afecten de forma parcial

o total la operativa normal de los servicios por Internet y correo interno.

El Área de TIC´s debe asegurar la adecuada disponibilidad, capacidad y el desempeño de los servicios por internet.

El Área de TIC´s debe crear políticas y procedimientos para el mantenimiento y seguridad del Portal o página Web en donde se defina la responsabilidad del Área para la actualización, elaboración, creación y/o diseño de la página Web institucional.