San Salvador 30, de junio de 2011.

Señor
Presidente del Comité de Investigaciones
Técnico Científicas de la OLACEFS
San Salvador-El Salvador

Remitimos a usted el trabajo del XIV Concurso Anual de Investigación de OLACEFs correspondiente al año 2011, denominado "Auditoria de Gestión a las Tecnologías de Información y Comunicaciones", con el Tema **"Auditoria de Gestión a las Tecnologías de Información y Comunicaciones"**, este trabajo ha sido elaborado por los participantes con el Seudónimo **"Technica Impendi Nationi"** auditores de la Corte de Cuentas de la República de El Salvador.

Agradeciendo su amable atención a la presente nos suscribimos de usted.

Atentamente,

“Porque un día, todas las Auditorías serán TIC…”

XIV Concurso Anual de Investigación de la OLACEFS

Tema:
“Auditoría de Gestión a las Tecnologías de Información y Comunicaciones.”

Seudónimo:
Technica Impendi Nationi

Corte de Cuentas de la República de El Salvador
San Salvador, El Salvador, Centroamérica.

OLACEFS

CONTENIDO

RESUMEN EJECUTIVO

Debido al acelerado incremento y desarrollo de las tecnologías de información y comunicaciones (TIC), se han experimentado cambios trascendentales en la evolución de la forma de vida de la sociedad actual, y por consiguiente en la forma en que los gobiernos administran las naciones, de esta manera las entidades gubernamentales hacen uso de las tecnologías de información y comunicaciones para el desarrollo de sus procesos y la prestación de servicios a la los ciudadanos. Así mismo, este crecimiento de las tecnologías no solo nos enfrenta a un mundo nuevo de procesos automatizados, y servicios más eficientes y efectivos basados en TIC, sino también a la aparición de nuevas formas de "Corrupción"; por lo tanto, se vuelve imprescindible controlar y fiscalizar de manera especializada la administración de los recursos tecnológicos, razón por la cual, las Entidades Fiscalizadoras Superiores (EFS) deben estar preparadas para los desafíos que implica fiscalizar dichas tecnologías.

Considerando el planteamiento anterior, se realizó esta investigación en cumplimiento con las especificaciones señaladas en las Bases del XIV Concurso Anual de Investigación promovido por la Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores OLACEFS, estableciendo como tema "Auditoría de Gestión a Las Tecnologías de Información y Comunicaciones".

Por lo anterior se desarrolló una propuesta de solución para realizar la Auditoría de Gestión a las Tecnologías de Información y Comunicaciones, basada en estándares de aceptación mundial, y que sea adaptable a la realidad Tecnológica de cada país de Latinoamérica y

del caribe, a través de las Entidades Fiscalizadoras Superiores (EFS), así mismo que se constituya en un instrumento para unificar criterios en materia de la administración y fiscalización tecnológica de las entidades públicas, que permita identificar los riesgos en el proceso de la auditoria a la gestión TIC, para determinar constantemente el nuevo rumbo a seguir de las EFS, con el objetivo de que la capacidad de controlar y fiscalizar se mantenga al mismo ritmo en que avanzan las Tecnologías de información y comunicaciones.

La propuesta de solución presentada en el Capítulo III de este documento, establece ocho componentes integrados, que dependen uno del otro para funcionar, los cuales interactúan entre sí con el objetivo de crear una estructura estandarizada, ordenada, sólida, dinámica y actualizable en el tiempo, la cual se llamará "**Torre TIC de la Auditoria**".

El primer componente "**Unidad Especializada de Auditoria TIC**", ~~se~~ plantea la necesidad de crear un área/unidad especializada de auditoria TIC, como instancia para la planificación, desarrollo, monitoreo, coordinación, y en general la ejecución de la Auditoría de Gestión a las Tecnologías de Información y Comunicaciones.

El Segundo Componente "**Base de Datos TIC de las entidades Fiscalizadas**", plantea el desarrollo de una base de datos con información de las plataformas tecnológicas de cada entidad sujeta a fiscalización, esto con el fin de que la EFS cuente con información que sirva para la toma de decisiones en la ejecución de la Auditoria a la Gestión TIC.

El Tercer componente "**Perfil del auditor TIC**" define las capacidades, conocimientos y habilidades que un Auditor de TIC debe poseer, para el ejercicio de la Auditoria.

El Cuarto componente "**Desarrollo del conocimiento TIC**" determina la necesidad de desarrollar el talento humano de nuestro equipo de auditoria, bajo un esquema de "capacitación continua", basada en la especialización, con el fin de cubrir todas las áreas del conocimiento identificadas en el perfil del auditor TIC.

El quinto componente "**Estándares internacionales para la auditoría de gestión TIC**" exhorta a utilizar las mejores prácticas relacionadas las TIC, específicamente COBIT, ITIL, ISO 27002, para posibilitar un gobierno eficaz de las actividades de control y ordenamiento de la gestión TIC.

El Sexto componente "**Normativa TIC de las EFS**" propone crear la normativa que establezca los criterios básicos de control que deben observarse en la gestión TIC, las cuales se han convertido en un instrumento esencial en la prestación de los servicios y representan rubros importantes en los presupuestos del Sector Público, estos basados en estándares de aceptación mundial en materia TIC y que sea tropicalizada a la realidad tecnológica de cada Nación.

El Séptimo componente **"Metodología de auditoría de gestión TIC"**, plantea el proceso de la práctica de la auditoría de a la Gestión TIC.

El octavo componte "**Los N Vectores de la Auditoria de Gestión TIC",** determinan la dirección y sentido de la auditoria de gestión TIC, en la cual definimos los diferentes enfoques o áreas de importancia sobre las cuales se ejecutara la auditoria a las TIC.

Al final del documento se presenta la bibliografía consultada y los anexos que se consideraron precisos para fortalecer el contenido de la investigación.

INTRODUCCIÓN

El acelerado incremento y desarrollo de las tecnologías de información y comunicaciones (TIC), se ha convertido en el cimiento del rápido avance tecnológico mundial y con ello ha provocado un cambio trascendental en la evolución de la forma de vida de la sociedad actual, forzando a los Gobiernos a cambiar sus formas de administrar los países.

A pesar de que el avance tecnológico es considerado “La piedra angular” del crecimiento económico y la lucha contra la pobreza, los países latinoamericanos y del caribe necesitan continuar mejorando su infraestructura básica, además de los servicios de salud, la educación, la seguridad ciudadana y sus procesos para hacer un mejor Gobierno.

Es por esto que el papel protagónico de las tecnologías de información y comunicaciones, se vuelve importante en todos los órdenes de la sociedad, las cuales han obligado a las instituciones, tanto públicas como privadas, a adoptar estrategias para incorporarlas y utilizarlas como herramientas que le permitan administrar con mayor eficiencia el aparato estatal, así como desarrollar e implementar las tecnologías basadas en sistemas de información que apoyen tanto a sus procesos sustantivos como administrativos y faciliten sus formas de actuar y de dar respuestas a los problemas, con eficiencia, eficacia, y economía, incrementando así los beneficios de los ciudadanos a los cuales se debe cada gobierno.

Bajo esta perspectiva, los procesos críticos y servicios que prestan las entidades gubernamentales, hoy en día dependen de las TIC, las cuales, están soportadas en hardware, software, sistemas informáticos con sus bases de datos, técnicas y metodologías asociadas a la virtualización, audio, video, texto, imágenes, redes y telecomunicaciones manejables totalmente en tiempo real.

Es así como queda claro que cada vez más las entidades públicas se vuelven dependientes de las Tecnologías de Información y comunicaciones TIC, automatizando procesos que se realizaban de forma manual; cambiando de la información impresa en papel a un mundo digital, implementando proyectos TIC que apoyen al cumplimiento de los objetivos estratégicos que se han planificado, y cambiando la *velocidad* en el flujo de información.

Así mismo, este crecimiento rápido y dependiente de las tecnologías no solo nos enfrenta a un mundo nuevo de procesos automatizados, y servicios más eficientes y efectivos basados en TIC´s, sino también al desarrollo de nuevas formas de delincuencia, malversación y el mal uso del poder para conseguir una ventaja ilegítima de los recursos del estado "Corrupción"; por lo tanto, se vuelve imprescindible controlar y fiscalizar de manera especializada la administración de los recursos tecnológicos.

En este sentido se vuelve un compromiso de las Entidades Fiscalizadoras Superiores (EFS) el estar preparadas para actuar ante la incursión inminente que las Tecnologías de Información y comunicaciones tienen en las Instituciones gubernamentales y privadas. Por lo tanto, esta investigación tiene como objetivo proponer una solución para efectuar la Auditoría De Gestión a Las Tecnologías de Información y Comunicaciones, basada en estándares de aceptación mundial, y que sea adaptable a la realidad Tecnológica de cada país de Latinoamérica y del caribe, a través de las Entidades Fiscalizadoras Superiores (EFS), así mismo que se constituya en un instrumento para unificar criterios en materia de la administración y fiscalización tecnológica de las entidades públicas, que permita identificar los riesgos en el proceso de la auditoria a la gestión TIC, para determinar constantemente el nuevo rumbo a seguir de las EFS, para que la capacidad de controlar y

fiscalizar se mantenga al mismo ritmo en que avanzan las Tecnologías de información y comunicaciones.

Esta investigación se ha realizado en cumplimiento con las especificaciones señaladas en las Bases del XIV Concurso Anual de Investigación de la OLACEFS.

"Porque un día, todas las auditorias serán TIC…"

CAPÍTULO I.

MARCO REFERENCIAL

1.1 HISTORIA DE LAS TIC

Se pueden considerar a las tecnologías de información y comunicaciones (TIC) como un concepto dinámico. Por ejemplo, el teléfono podría ser considerado una nueva tecnología según las definiciones actuales a finales del siglo XIX. Esta definición también podría aplicarse a la televisión cuando apareció en la mitad del siglo XX.

El teléfono, la televisión y el ordenador se pueden considerar TIC, ya que favorecen la comunicación y el intercambio de información en la actualidad.

Los primeros pasos hacia una sociedad de la información estuvieron marcados por el invento del telégrafo eléctrico, teléfono, radiotelefonía, la televisión e internet. El móvil y el GPS han unido la imagen al texto y la palabra sin cables. Internet y televisión son accesibles en el móvil, que también puede hacer fotos.

A finales del siglo XX se dio un gran avance a la miniaturización de los componentes, que permitió crear aparatos con muchas funciones.

Inventos TIC	Año	Detalles
Pendrive/ Memoria USB	1998	Las unidades flash USB fueron inventadas en 1998 por IBM como un reemplazo de las unidades de disquete para su línea de productos ThinkPad
Ordenador	1936	arquitectura Von Neumann, electrónicas, basadas en la aritmética binaria y de programa almacenado en

		memoria
Portátil /Laptop	1981	El primer ordenador portátil considerado como tal fue el Epson HX-20, desarrollado en 1981
Televisión	1927	Las primeras emisiones públicas de televisión las efectuó la BBC en Inglaterra en 1927 y la CBS y NBC en Estados Unidos en 1930
Radio	1895	En 1895 el italiano Guillermo Marconi construyó el primer sistema de radio
Móvil /Telefonía Celular	1983	El modelo fue diseñado por el ingeniero de Motorola Rudy Krolopp en 1983
Internet	1960	Sus orígenes se remontan a la década de 1960, dentro de ARPA (hoy DARPA), como respuesta a la necesidad de esta organización de buscar mejores maneras de usar los computadores de ese entonces

"Las TIC han provocado un cambio trascendental en la evolución de la forma de vida de la sociedad actual."

1.2 DELIMITACIÓN DE LA INVESTIGACIÓN

La investigación se ha delimitado en los aspectos fundamentales siguientes:

TEÓRICAMENTE

Se ha estudiado una base teórica relacionada con las Tecnologías de Información y Comunicaciones, específicamente desde la perspectiva de estándares de aceptación mundial y buenas prácticas como COBIT, ITIL e ISO 27002, analizando la aplicabilidad de estas al ámbito de la auditoria y la forma en que las TIC sirven de apoyo a los procesos sustantivos de las entidades públicas, con el objetivo de proponer una solución para efectuar la Auditoría de Gestión a las Tecnologías de Información y Comunicaciones, en las Entidades del Sector Público sujetas a fiscalización.

TEMPORALMENTE

La investigación bibliográfica y de campo se desarrolló en un período de cuatro meses, a partir del 1 de marzo al 30 de junio del 2011.

GEOGRAFICAMENTE

La investigación de campo se ha realizado en países de Latinoamérica y el Caribe, así como de las experiencias obtenidas en el desarrollo de auditorías a las TIC en nuestro país.

1.3 JUSTIFICACIÓN DE LA INVESTIGACIÓN

Debido al acelerado incremento y desarrollo de las tecnologías de información y comunicaciones (TIC), y al impacto que estas ejercen sobre la productividad y el crecimiento económico de las naciones, las entidades gubernamentales utilizando TIC como instrumento de apoyo a sus procesos sustantivos y la prestación de los servicios a los

ciudadanos, razón por la cual las Entidades Fiscalizadoras Superiores (EFS) deben estar preparadas para los retos que implica fiscalizar dichas tecnologías.

1.4 OBJETIVOS DE LA INVESTIGACIÓN

Con la realización de esta investigación se persiguen los objetivos siguientes:

GENERAL

Proponer una solución para efectuar la Auditoría De Gestión a Las Tecnologías De Información Y Comunicaciones, basada en estándares de aceptación mundial, y que sea adaptable a la realidad Tecnológica de cada país de Latinoamérica y del caribe, a través de las Entidades Fiscalizadoras Superiores (EFS), Así mismo que se constituya en un instrumento para unificar criterios en materia de la administración y fiscalización tecnológica de las entidades públicas, que permita identificar los riesgos en el proceso de la auditoria a la gestión TIC, para determinar constantemente el nuevo rumbo a seguir de las EFS, para que la capacidad de controlar y fiscalizar se mantenga al mismo ritmo en que avanzan las Tecnologías de información y comunicaciones.

ESPECIFICOS

a) Lograr estandarizar la forma en que las EFS hacen la auditoria de gestión a las TIC en Latinoamérica y el Caribe.
b) Proponer una solución integral para que las EFS realicen las auditorías a la gestión TIC.
c) Impulsar a que las EFS desarrollen Normativas de gestión y control TIC, basadas en estándares de aceptación mundial y buenas prácticas relacionadas a las TIC.

d) Que a través de la implementación de los componentes de la Torre TIC, la OLACEFS cuente con un instrumento de medición que le permita verificar las áreas críticas o los problemas de las EFS para efectuar Auditoria de Gestión TIC de forma más precisa.

1.5 ALCANCE DE LA INVESTIGACIÓN

Como resultado de la investigación, se ha diseñado una solución integral que le permita a las EFS realizar la Auditoría de Gestión a las Tecnologías de Información y comunicaciones bajo estándares de aceptación mundial en materia TIC y que sea adaptable a la realidad Tecnológica de cada país de Latinoamérica.

1.6 DETERMINACIÓN DEL UNIVERSO, POBLACIÓN Y MUESTRA

A efecto de llevar a cabo esta investigación y obtener la opinión sobre el tema objeto de estudio, se definió como universo a las EFS de los 23 países miembros de OLACEFS. Cabe mencionar que de los 23 países consultados, no se recibió respuesta a las encuestas enviadas a través de nuestra EFS.

1.7 DEFINICIÓN DEL PROBLEMA DE INVESTIGACIÓN

Las Tecnologías De Información Y Comunicaciones (TIC en adelante), juegan un papel crucial en la innovación y la generación de conocimiento y nuevos negocios. Adicionalmente, son el instrumento que garantiza la transparencia en la administración que ejerce un Gobierno, fortalece la conexión entre las instituciones del Estado y especialmente, de éstas con los ciudadanos, a través de la ubicuidad, que significa estar en todas partes al mismo tiempo y con la disponibilidad de la información a cualquier hora, desde cualquier lugar y con una variedad de dispositivos tecnológicos, que modifican la forma de acceder a la información.

Es por esto que cada vez más las entidades públicas se vuelven dependientes de las Tecnologías de Información y comunicaciones, involucrándose cada vez más en todos los procesos sustantivos de las entidades gubernamentales.

En ese sentido el desarrollo de la Auditoria de gestión a las tecnologías de información y comunicaciones se vuelve imprescindible, para que las Entidades fiscalizadoras Superiores ejerzan el rol de fiscalización para el cual fueron creadas. Ya que la era de auditar sobre papel casi ha desaparecido, así que cada auditor independientemente de la auditoria que realice ya sea esta financiera, administrativa, operativa, de gestión, medio ambiente o Informática, deberá tener conocimientos sobre TIC, debido a que los procesos sustantivos de las entidades a auditar y su información, estará siendo administrada por diferentes componentes de las TIC.

De esta manera determinamos que nuestro problema reside en la falta de una organización bien estructurada para efectuar la auditoria de Gestión a las TIC, que nos permita planificar, desarrollar, monitorear, y coordinar la ejecución de la Auditoría, basada en un marco legal de la aplicación de mejores prácticas en la administración TIC y un adecuado desarrollo del perfil de los auditores en las TIC.

Además la rapidez con la que avanza la tecnología y los cambios a corto plazo que genera en instituciones del estado que suelen ir a la vanguardia en la implementación de tecnología de punta en apoyo a sus procesos sustantivos, convierte a los procedimientos de auditoria que no siguen el mismo ritmo dinámico de cambios tecnológicos, en auditorias con metodologías y técnicas desactualizadas, y por lo tanto incapaces de auditar las TIC de hoy.

CAPÍTULO II.

MARCO TEÓRICO

Para el desarrollo de esta investigación definiremos los conceptos de:

- TIC
- Gestión
- Gestión TIC
- Auditoria de Gestión a las TIC.

2.1 TIC

Las tecnologías de la información y la comunicación (TIC) son un conjunto de servicios, redes, software y dispositivos que tienen como fin la mejora de la calidad de vida de las personas dentro de un entorno, y que se integran a un sistema de información interconectado y complementario.

Las TIC se conciben como el universo de dos conjuntos, representados por las tradicionales Tecnologías de la Comunicación (TC) - constituidas principalmente por la radio, la televisión y la telefonía convencional - y por las Tecnologías de la información (TI) caracterizadas por la digitalización de las tecnologías de registros de contenidos (informática, de las comunicaciones, telemática y de las interfaces)". Las TIC son herramientas teórico conceptuales, soportes y canales que procesan, almacenan, sintetizan, recuperan y presentan información de la forma más variada. Los soportes han evolucionado en el transcurso del tiempo (telégrafo óptico, teléfono fijo, celulares, televisión) ahora en ésta era podemos hablar de la computadora y de Internet. El uso de las TIC representa una variación notable en la sociedad y las relaciones interpersonales y en la forma de difundir y generar conocimientos.

2.2 Gestión

Está caracterizada por una visión de las posibilidades reales de una organización para resolver determinada situación o arribar a un fin determinado. Puede asumirse, como la "disposición y organización de los recursos de un individuo o grupo para obtener los resultados esperados". Pudiera generalizarse como una forma de alinear los esfuerzos y recursos para alcanzar un fin.

2.3 Gestión TIC

El alineamiento y apoyo a la consecución de los objetivos de una organización, a través de las tecnologías de información y comunicaciones. Es una disciplina basada en procesos, enfocada en alinear los servicios de TI proporcionados con las necesidades de las empresas, poniendo énfasis en los beneficios que puede percibir el cliente final.

2.4 Auditoria de Gestión a las TIC

En este sentido ejecutar una Auditoría de Gestión a las Tecnologías de Información Y Comunicaciones, va más allá de un examen a los controles de los elementos de hardware y software de una plataforma tecnológica.

La Auditoría de Gestión a las Tecnologías de Información y Comunicaciones se enfoca desde dos perspectivas:

a) El examen de los elementos y las técnicas utilizadas en el procesamiento, tratamiento y la transmisión de las informaciones, principalmente de informática, internet y telecomunicaciones.

b) Como las TIC se encuentran alineadas a la consecución de los objetivos institucionales, en apoyo a la gestión de la organización, mejorando procesos y servicios en función de eficiencia, eficacia, productividad, y economía.

2.5 Auditoría en tiempo real.

La auditoría se realiza por lo general en sistemas manuales a posteriori. Se convocan auditores periódicamente para examinar las transacciones recientes de una organización y determinar si se han realizado actividades fraudulentas. La auditoría en TIC puede implicar un procesamiento inmediato en el computador para revisar las transacciones que se acaban de realizar, la tecnología es de hoy… y por ende en tiempo real. La auditoría de gestión TIC debe de efectuarse de manera, preventiva, en tiempo real y posterior. Preventiva y posterior dependerá de los factores que impacta a las TIC, como por ejemplo la seguridad y confiabilidad de la información.

2.6 Falta de indicadores de Gestión TIC.

Para hacer mediciones eficaces que permitan saber cómo estamos haciendo las cosas, qué estamos haciendo bien y qué debemos corregir hay que crear Indicadores de Gestión en TIC. No se desarrollan suficientes indicadores de gestión TIC. Es un reto para cada una de las EFS el determinar los indicadores de Gestión de las TICs, así mismo se puede hacer uso de los determinados por los estándares de aceptación mundial relacionados con las TICs, como ITIL, COBIT, ISO 27002.

CAPÍTULO III.

DESARROLLO DE LA PROPUESTA

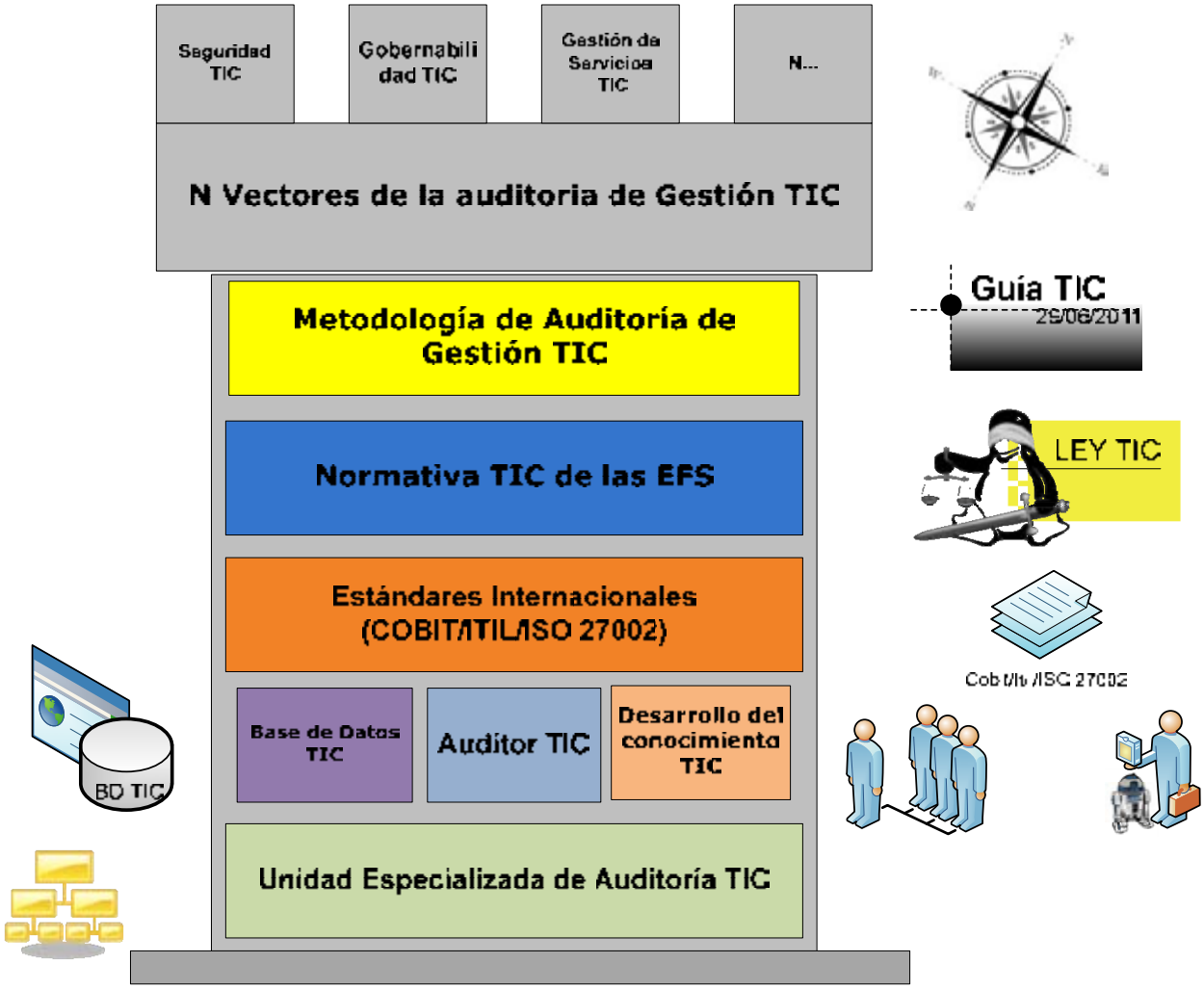
La OLACEFS, en conjunto con las Entidades Fiscalizadoras Superiores (EFS) han realizado esfuerzos significativos en cimentar las bases para el desarrollo de la auditoria TIC, logrando que muchas EFS sean hoy en día líderes en la fiscalización de dicha especialidad tecnológica, sin embargo, aún existen brechas entre las EFS de los países miembros de la OLACEF en el tema de la auditoria de gestión a las TIC. Por esta razón la propuesta se enfoca en plantear una solución para realizar la Auditoría de Gestión a las Tecnologías de Información y Comunicaciones, basada en estándares de aceptación mundial, y que sea adaptable a la realidad Tecnológica de cada país de Latinoamérica y del caribe, a través de las Entidades Fiscalizadoras Superiores (EFS), Así mismo que se constituya en un instrumento para unificar criterios en materia de la administración y fiscalización tecnológica de las entidades públicas, que permita identificar los riesgos en el proceso de la auditoria a la gestión TIC, y determinar constantemente el nuevo rumbo a seguir de las EFS para que la capacidad de controlar y fiscalizar se mantenga al mismo ritmo en que avanzan las Tecnologías de información y comunicaciones.

La presente propuesta está basada en el desarrollo de componentes integrados, que dependen uno del otro para funcionar, los cuales interactúan entre sí con el objetivo de crear una estructura estandarizada, ordenada, sólida, dinámica y actualizable en el tiempo, la cual llamaremos “TORRE TIC DE LA AUDITORIA”.

Los componentes que la integran son:

1. Unidad Especializada de Auditoria TIC.
2. Base de Datos TIC de las entidades Fiscalizadas.
3. Auditor TIC.
4. Desarrollo del conocimiento TIC.
5. Estándares Internacionales TIC (COBIT/ITI/ISO27002).
6. Normativa TIC de las EFS.
7. Metodología de Auditoría de Gestión TIC.
8. N Vectores de la auditoria de Gestión TIC.

DISEÑO DE LA TORRE TIC DE LA AUDITORIA



La Torre TIC, es una estructura que integra componentes que dependen cada uno del otro para poder funcionar de forma efectiva, para dar respuestas reales. Cada uno de los ocho componentes que la integran se describe en los apartados siguientes.

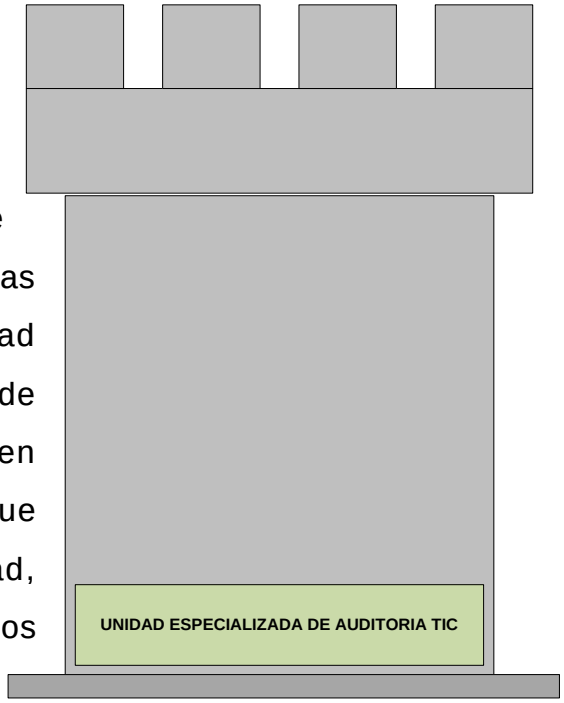
Porqué LA TORRE? Porque La torre simboliza:

a) Edificio fuerte, más alto que ancho, y que sirve para defenderse de los enemigos desde él, o para defender una ciudad o plaza.
b) Torre situada en un lugar alto para vigilancia: las atalayas se construían en zonas de costa para prevenir ataques de piratas.
c) Torre de control: construcción existente en los aeropuertos, con altura suficiente para dominar las pistas y el área de aparcamiento de los aviones, en la que se encuentran todos los servicios de radionavegación y telecomunicaciones para regular el tránsito de aviones que entran y salen.

Estos conceptos se apegan a la posición que debe tener la EFS para efectuar una auditoria de gestión a las TIC. Desde esta visión es que determinamos que nuestro enfoque para realizar la Auditoría De Gestión a las Tecnologías de Información Y Comunicaciones, debe ser ejecutada bajo una estrategia que nos permita mantener una superioridad tecnológica sobre las entidades sujetas a fiscalización, para vigilar, controlar, regular, monitorear y actuar ante los avances de las TIC.


ESTAS PREPARADO
PARA AUDITAR MI
GESTION TIC ?

3.1 UNIDAD ESPECIALIZADA DE AUDITORIA TIC



Si bien es cierto que las Tecnologías de Información y Comunicaciones constituyen parte de la forma de vida de la sociedad actual, la mayoría de personas son usuarios finales de dichas TIC, por lo tanto se vuelve una especialidad su administración, la cual está en manos de una minoría formada profesionalmente en áreas afines a las TIC. Es por esto que auditar TIC, se vuelve una especialidad, debido a que no solo se examinan los niveles de utilización como usuario final y los beneficios que estas generan, sino también su administración.

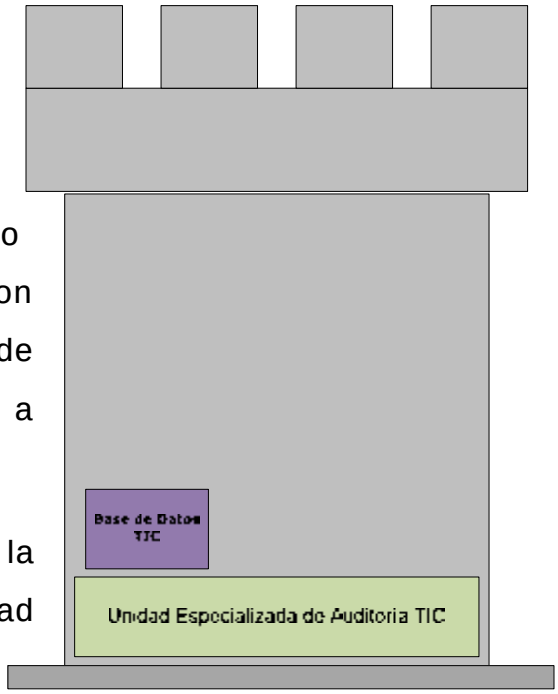
Por lo tanto se deberá crear la unidad especializada de auditoria TIC, como instancia para la planificación, desarrollo, monitoreo, coordinación de la Auditoría de Gestión a las Tecnologías de Información y Comunicaciones.

Facultades de la Unidad especializada de Auditoría TIC.

- Coordinación de la ejecución de la Auditoría de Gestión a las Tecnologías de Información
- Investigación de las nuevas tendencias de gestión de las TIC
- Desarrollar e implementar un proyecto de capacitación continua en el área de TIC para sus Auditores.
- Desarrollar y administrar las leyes, Normas y políticas de administración TIC de las EFS.

- Desarrollar una guía o manual de auditoria de gestión TIC.
- Mantener actualizada la base de datos TIC de las Entidades Fiscalizadas.
- Asesorar al gobierno en la dirección tecnológica del país.

3.2 BASE DE DATOS DE LA PLATAFORMA TECNOLÓGICA DE LAS ENTIDADES FISCALIZADAS.



Cada EFS deberá desarrollar una base de datos con información de las plataformas tecnológicas de las entidades públicas, esto con el fin de que la EFS cuente con información que sirva para la toma de decisiones en la ejecución de la Auditoria a la Gestión TIC.

El contar con una base de datos de la plataforma Tecnológica de cada entidad sujeta a fiscalización, le permitirá a EFS, efectuar una planeación más precisa de la auditoria, así como integrar en el equipo de auditoria TIC, los profesionales idóneos para la ejecución de la auditoria.

Contenido mínimo de la base de datos de la Plataforma Tecnológica de las entidades sujetas a fiscalización.

a) Información General de la Entidad Fiscalizada:

a. Nombre de la Entidad (Dirección y teléfonos de contacto).
b. Nombre de la Máxima Autoridad de la Entidad fiscalizada.
c. Nombre del Gerente/Jefe del área de que administra las TIC en la entidad fiscalizada.
d. Estructura organizativa del Área de TIC.
e. Cantidad y características técnicas de las estaciones de trabajo/equipos desktop y laptops.
f. Cantidad y Características Técnicas de Equipos Servidores.
g. Detalle de las características de las redes (LAN, WAN, WiFi) y enlaces de comunicaciones (enlaces propios o outsourcing)

h. Descripción de los dispositivos de seguridad perimetral de la Red institucional.
i. Detalle de los sistemas /aplicativos informáticos.
j. Sistemas operativos.
k. Leguajes de desarrollo.
l. Detalle de las Bases de datos.
m. Entre otros.

Existen innumerables parámetros que podría contener la base de datos TIC, las cuales deberán ser definidas por cada EFS, de acuerdo a sus necesidades de información.

Dicha información deberá ser actualizada cada año o como mínimo en cada auditoria TIC, efectuada a la entidad fiscalizada.

Ejemplo de aplicación de la base de datos TIC:

La Unidad de auditoria TIC, planifica la ejecución de una auditoria a la entidad X, encargada de registrar a todos los ciudadanos del país, y de emitir los documentos de identidad únicos.

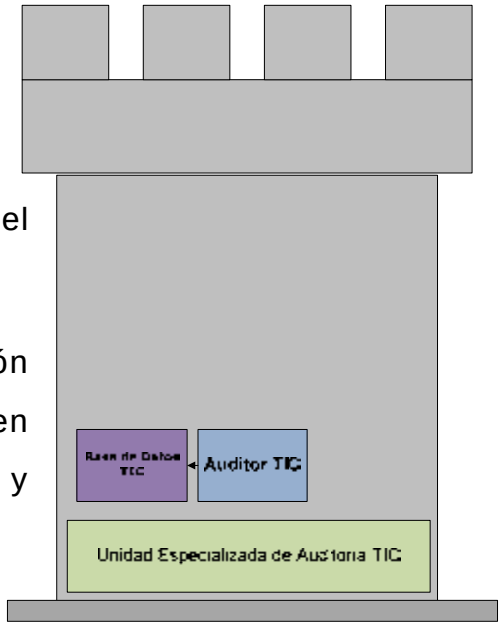
"En la planificación de la auditoria se consulta la base de datos TIC, con la información de la entidad X, encontrando que, cuentan con un sistema de apoyo al proceso sustantivo que es el de registrar ciudadanos y emitir documentos únicos de identidad, dicho sistema fue desarrollado por outsourcing, una base de datos Oracle versión 11g, y una granja de servidores con tecnología RISK. Así mismo, cuenta con enlaces de comunicación a todos los Estados/Departamentos a nivel nacional, debido a las sucursales. En total poseen con 500 equipos informáticos (PC y laptops) en red, las cuales accesan al sistema. Cuentan con tres sitios con servidores y bases de datos redundantes. Los sistemas operativos, UNIX en los Servidores y estaciones de trabajo PC con Microsoft Windows."

Luego de verificar toda esta información en la Base de datos TIC, se tiene un panorama de la capacidad tecnológica de la entidad fiscalizada. Así como el volumen de transacciones que esta podría manejar. En fin plantea un escenario real al cual nos enfrentaremos en la ejecución de la auditoria.

Beneficios:

a) Se podrá conformar el equipo de auditoria TIC con los profesionales idóneos, para verificar las tecnologías mencionadas.
b) Además, se podrá definir los tiempos y alcance de la auditoria de manera más precisa.
c) El analizar la base de datos TIC, servirá de insumo en la toma de decisiones para el rumbo tecnológico que la EFS deberá tomar en cuanto a uso de estándares TIC, y capacitaciones en función de desarrollar el talento humano del auditor TIC, de acuerdo a productos de tecnología más utilizado en bases de datos, sistemas operativos y lenguajes de programación, redes, entre otras tendencias tecnológicas que surjan con el tiempo.
d) Así mismo servirá como un insumo para la función asesora, que las EFS deberán utilizar para regular y normar el uso y administración de las TIC en las entidades públicas.

3.3 PERFIL DEL AUDITOR TIC



Este componente de la Torre TIC, es de gran importancia, debido a que define las capacidades, conocimientos y habilidades que un Auditor de TIC debe poseer, para el ejercicio de la Auditoria.

El auditor TIC no solo debe tener formación profesional en Auditoria, sino también en Tecnologías de Información y comunicaciones.

El perfil del auditor de sistemas es complejo, debido a que tiene que poseer los conocimientos de un auditor "Puro" y un Técnico o profesional en tecnologías de información, ya que el auditor de sistemas debe tener conocimientos sobre:

- Auditoría
- Seguridad TIC
- Gobernabilidad TIC
- Bases de Datos
- Sistemas Operativos
- Redes y comunicaciones
- Infraestructura de servidores
- Ingeniería de software
- **Hacking ético**
- Y muchos más.

Sería difícil encontrar tantos auditores con el 100% de los conocimientos necesarios para el perfil del auditor TIC. Y es por esto que introducimos dentro de dicho perfil, el concepto de **"Especialización"**.

La EFS deberá, a través del área o Unidad de Auditoria TIC, identificar las especialidades a crear, de acuerdo a las características TIC de las Organizaciones fiscalizadas, el estándar o común denominador de los elementos tecnológicos que integran a las organizaciones Gubernamentales y Privadas, así como de la información de la base de datos TIC descrito en el apartado anterior.

Se ha identificado que una organización que cuenta con infraestructura y servicios de tecnología de información y comunicaciones, cuenta con al menos una unidad de TI, o servicios autsourcing, que administran las áreas siguientes:

- Soporte Técnico
- Sistemas o aplicativos informáticos
- Bases de Datos
- Redes y comunicaciones
- Infraestructura de servidores

La unidad de auditoría TIC, deberá definir las especialidades TIC de los auditores con el fin de desarrollar el talento humano enfocado a la especialidad del perfil, de los cuales se proponen los siguientes:

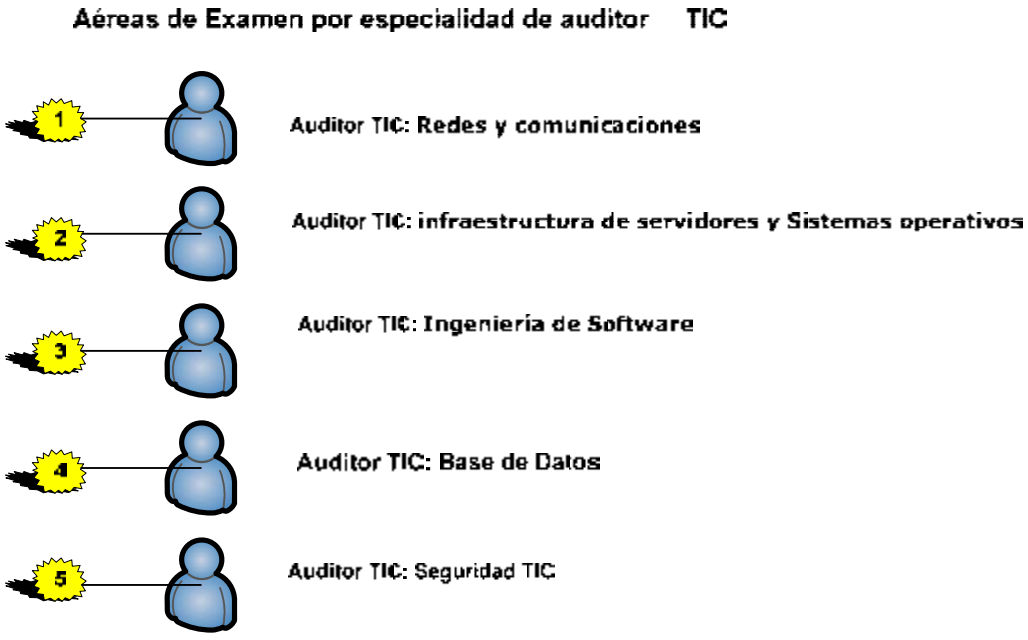
- Auditor TIC especializado en Redes y comunicaciones.
- Auditor TIC especializado en infraestructura de servidores y Sistemas operativos.
- Auditor TIC especializado en ingeniería de Software.
- Auditor TIC especializado en Bases de datos.
- Auditor TIC especializado en Seguridad de la información.

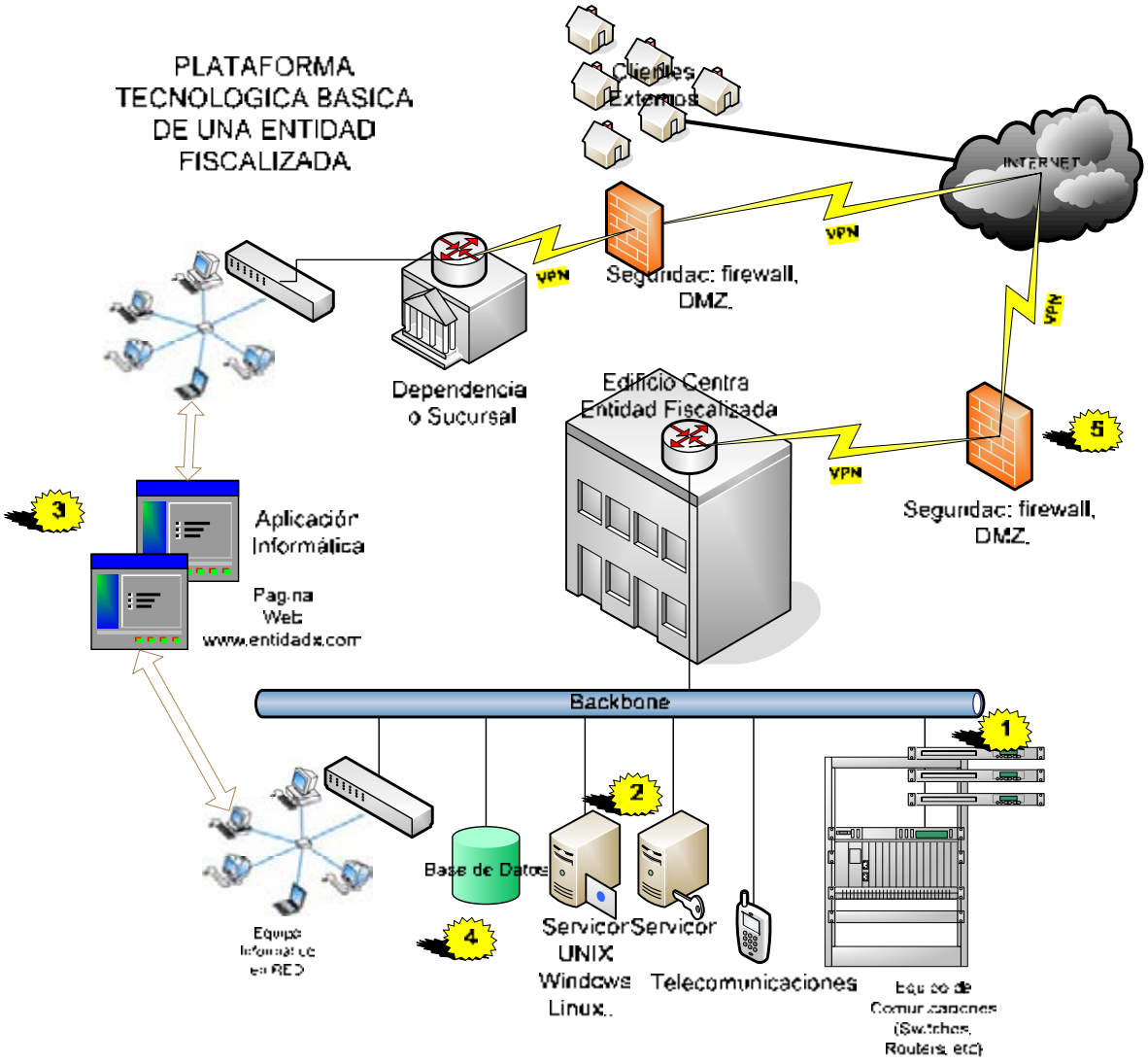
3.3.1 Esquema TIC de una entidad X y sus elementos tecnológicos a auditar:

Para el ejemplo supondremos que existe una entidad de gobierno a fiscalizar, la cual proporciona servicios de salud a sus ciudadanos, dicha entidad cuenta con una Dirección de TI, la cual administra su plataforma tecnológica integrada por una Intranet institucional con enlaces remotos, y servicios de telecomunicaciones contratados a terceros (outsourcing), para diferentes sucursales, infraestructura de servidores con diferentes sistemas operativos, sistemas informáticos y servicios web, así como dispositivos de seguridad perimetral de la red, y toda una red de equipos informáticos estacionarios y laptops. Todo para apoyar a los procesos sustantivos de la entidad y proveer servicios más eficientes y efectivos a la población.

Aplicando el concepto de "Especialidad del Auditor TIC", en la auditoria de gestión TIC, se cubrirán todos los elementos tecnológicos posibles a examinar, minimizando el riesgo de auditoria.

Hay que ejecutar una Auditoria TIC, para lo cual se deberá contar con :





Existen muchas más especializaciones que podrían ser consideradas, pero creemos básicas (en la actualidad) las expuestas en este documento, para que una EFS cuente con equipos de auditoria que hagan frente a la mayoría de elementos tecnológicos que integran una plataforma tecnológica de una entidad fiscalizada.

Lo que se pretende no es que un auditor lo sepa todo Tecnológicamente hablando, sino que la EFS, sea capaz de conformar “equipos de auditoria” que cubran al 100% el perfil del auditor TIC. Así podemos introducir otro concepto, el cual llamaremos “Equipo de auditoria TIC”.

Por lo que en la planificación de la auditoria, La Dirección de Auditoria TIC, deberá conformar el “Equipo de auditoria TIC”, más idóneo a enviar a la Entidad fiscalizada.

3.3.2 Certificaciones TIC

¿Qué es Certificación?

“La certificación, es el procedimiento mediante el cual una tercera parte diferente e independiente del productor y el comprador, asegura por escrito que un producto, un proceso o un servicio, cumple los requisitos especificados, convirtiéndose en la actividad más valiosa en las transacciones comerciales nacionales e internacionales. Es un elemento insustituible para generar confianza en las relaciones cliente-proveedor.”

Conforme al concepto de certificación expuesto en el párrafo anterior, podemos decir que es un elemento que genera confianza, y que asegura que los requisitos se cumplen. En las TIC la mayoría de procesos, productos y servicios son certificados por un tercero, ya sea por sus fabricantes o desarrolladores y por organismos certificadores.

Es por esto que se vuelve necesario que Los auditores TIC, posean certificaciones que le garanticen tanto a la EFS como a la entidad fiscalizada que se cuenta con los conocimientos y las habilidades requeridas para efectuar auditoria TIC.

Beneficios:

- Realza el reconocimiento Profesional y el crecimiento personal.
- Incrementa la credibilidad con las empresas y clientes.
- Incrementa la competencia en la ejecución de funciones de trabajo.
- Acceso a un mejor soporte Técnico.
- Habilidad para estar actualizado en las últimas tecnologías.

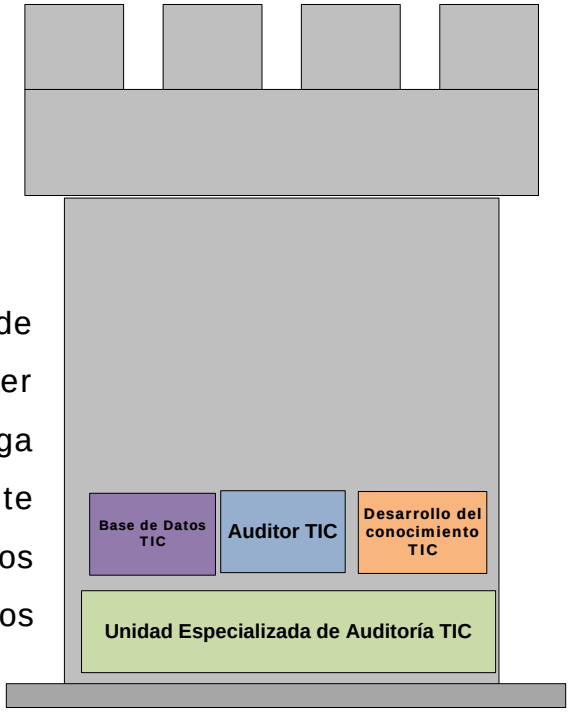
Para nuestro ámbito de acción son necesarios dos tipos de certificaciones:

a) **Certificaciones relacionadas a auditoria TIC**: Se recomienda La certificación internacional como Auditor de Sistemas de Información (Certified Information Systems Auditor - CISA™) está reconocida a nivel mundial como uno de los estándares más prestigiosos en las áreas de auditoria, control, seguridad y gobernabilidad de Sistemas de Información.

b) Y certificaciones Técnicas del profesional en TIC:

- CISCO
- VMware
- Microsoft
- Oracle
- ITIL
- COBIT
- ISO 27002
- Entre otras.

3.4 DESARROLLO DEL CONOCIMIENTO TIC



Las EFS pueden contratar personas talentosas para ocupar los cargos de auditor TIC, pero es mejor desarrollar por sí mismas el talento de sus Auditores.

Cuando se entra a analizar el área de capacitación del recurso humano en cualquier empresa o entidad de gobierno (que tenga diseñada esta área), resulta sorprendente encontrar que son muy escasos los recursos destinados al área, tal vez porque los empleadores piensan que el talento brota innatamente de su personal o porque no entienden que cuanto más desarrollado es su recurso humano, mayores serán los beneficios institucionales en términos de sentido de pertenencia y obviamente de desempeño.

El rápido avance de las tecnologías, obliga a los profesionales en TIC a mantenerse actualizados, con los cambios que se generan tanto en los procesos, como en los nuevos productos que la industria de tecnología desarrolla.

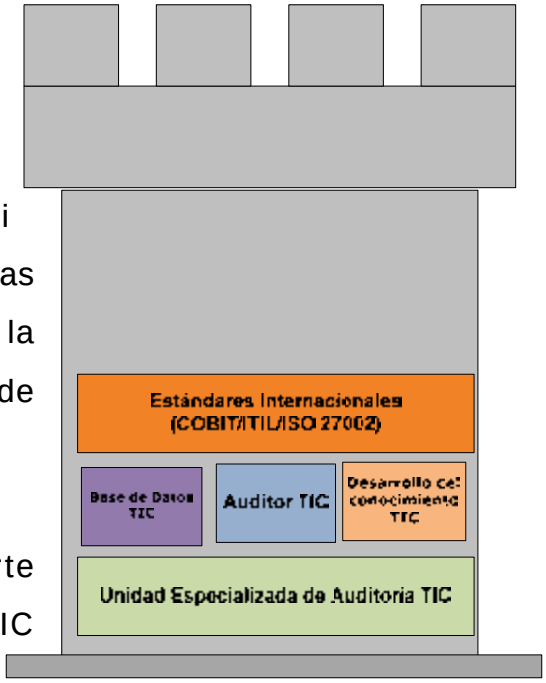
El profesional en auditoria TIC, debe poseer conocimientos superiores o como mínimo, estar al mismo nivel, que el de los profesionales administradores de las plataformas tecnológicas en las entidades sujetas a fiscalización.

Esto debido a que la EFS debe generar confianza en sus auditados, de que las personas que los auditan son competentes y “saben lo que hacen”.

En vista de la necesidad de desarrollar el talento humano **“Conocimiento TIC”** de nuestro equipo de auditoria, se recomienda, crear un esquema de **“capacitación continua”,** basada en **la especialización**, con el fin de cubrir todas las áreas del conocimiento identificadas en el **perfil del auditor TIC.**

Así mismo que dicho proyecto de capacitación continua en TIC incorpore un proceso de investigación, para identificar nuevas tecnologías que requieran de capacitación, para que en el momento en que las entidades públicas las implementen, los auditores TIC tengan la capacidad de auditarlas.

3.5 ESTÁNDARES INTERNACIONALES PARA LA AUDITORIA DE GESTIÓN TIC.



Las Tecnologías de Información y Comunicaciones se han hecho casi omnipresentes en la mayoría de las organizaciones, independientemente de la actividad de éstas, de sus dimensiones, o de su carácter público o privado.

Esto ha provocado una dependencia tan fuerte de estas tecnologías, debido a que las TIC han, pasado a ser un "commodity" (en economía es cualquier producto destinado a uso comercial), como es la luz eléctrica.

Es por esto que si se mira alrededor en el ámbito de trabajo de la auditoría y se reflexiona sobre la posibilidad de un apagón tecnológico momentáneo que dejase inoperativos todos los sistemas informáticos (Servidores, ordenadores, impresoras, programas de gestión, sitios Web etc.) y de comunicaciones (redes, Internet, plantas de telefonía digitales, etc.), será difícil imaginar la actividad de la organización en el día a día, y seguramente se concluya que un incidente de este tipo abocaría a un colapso en el funcionamiento de la misma.

En este sentido, es inmediato concluir que es necesaria una buena administración de las TIC con el objeto de que no ocurran incidentes de tal magnitud e, incluso, de magnitudes menores que dejen inoperativos, por ejemplo, sólo una parte de los sistemas.

Siguiendo el mismo razonamiento, podemos también deducir que si la dependencia de una organización de las TIC es tal, una adecuada administración de estas tecnologías no sólo evitará desastres como los mencionados, sino que puede ayudar a que mejoren muchos aspectos como la calidad o la eficiencia en nuestra organización y, en definitiva, mejoren los resultados finales de la misma. En definitiva, se concluye que una adecuada administración de las TIC aportará valor al negocio de la organización, sea éste del tipo que sea y ayudará a ésta a conseguir sus objetivos, minimizando los riesgos.

Con buenos procesos de gestión es posible, además, empezar a medir de manera individual aspectos relevantes de las TIC.

Las Compañías, Corporaciones e Instituciones gubernamentales han implementado controles, roles y responsabilidades, orientados a garantizar la integridad, seguridad y confiabilidad de la información, que requieren que sean revisados y/o auditados en base a modelos de control tales como COSO, COBIT, ITIL, ISO27002.

La creciente adopción de mejores prácticas de TI se explica porque la industria de TI requiere mejorar la administración de la calidad y la confiabilidad de TI en los negocios y para responder a un creciente número de requerimientos regulatorios y contractuales.

Sin embargo, existe el peligro de que las implementaciones de estas mejores prácticas, potencialmente útiles, puedan ser costosas y desenfocadas si son tratadas como guías puramente técnicas.

Para ser más efectivos, las mejores prácticas deberían ser aplicadas en el contexto del negocio, enfocándose donde su utilización proporcione el mayor beneficio a la organización.

El desarrollo del tema "**Estándares internacionales para la auditoria de gestión tic",** aplica en general a todas las mejores prácticas TIC pero se enfoca en tres prácticas y estándares específicos, los que están siendo ampliamente adoptados a nivel global:

• ITIL v3: Publicado por la OGC (Office of Government Commerce) del gobierno británico para proporcionar un marco de referencia de mejores prácticas para la gestión de servicios de TI.

• COBIT ® 4.1: Publicado por el ITGI y posicionado como un marco de referencia de alto nivel para el control y el gobierno de TI.

• ISO/IEC 27002:2005: Publicado por ISO (International Organization for Standardization) y por IEC (International Electrotechnical Commission), derivado de la norma BS 7799 del gobierno británico, renombrada ISO/IEC 17799:2005, para proporcionar un marco de referencia del estándar para gestión de seguridad de información.

Las mejores prácticas y los estándares ayudan a posibilitar un gobierno eficaz de las actividades TIC

Incrementalmente, el uso de estándares y mejores prácticas tales como ITIL, COBIT e ISO/IEC 27002, está siendo conducido por requerimientos de negocio para mejoras de desempeño, transparencia y control sobre actividades de TI.

A inicios de la década de los 90, ISACA reconoció que los auditores, quienes tenían sus propios checklist para evaluar la efectividad de los controles de TI, hablaban en un lenguaje diferente a los profesionales de TI y a la plana gerencial. En respuesta a esta brecha en la comunicación, se creó COBIT como un marco de referencia de control de TI para la gerencia funcional, la gerencia de TI y para auditores, basado en un grupo genérico de procesos de TI significativo para la gente de TI

y, con el tiempo, para la gerencia. Las mejores prácticas en COBIT representan un enfoque común para un buen control de TI, a ser implementado por gerentes funcionales y de TI, y a ser evaluadas sobre la misma base por los auditores. A lo largo de los años, COBIT ha sido desarrollado como un estándar abierto, y es cada vez más utilizado como un modelo de control para implementar y demostrar un gobierno efectivo de TI.

COBIT está basado en marcos de referencia establecidos, tales como CMM de SEI (Software Engineering Institute), ISO 9000, ITIL e ISO/IEC 27002; sin embargo, COBIT no incluye tareas y pasos de procesos porque, aunque está orientado a procesos de TI, es un marco de referencia para gestión y control antes que un marco de referencia para procesos. COBIT se focaliza en lo que una empresa necesita hacer, no cómo lo tiene que hacer, y la audiencia objetivo es la alta gerencia, los gerentes funcionales, los gerentes de TI y los auditores. ITIL está basado en la definición de procesos de mejores prácticas para la gestión y el soporte de servicios de TI, antes que en la definición de un marco de control de amplio alcance. Se focaliza en el método y define un grupo más compacto de procesos. Existe material adicional en ITIL v3 que proporciona un contexto estratégico y de negocios para la toma de decisiones de TI, y empieza describiendo el mejoramiento continuo del servicio como una actividad integral, promoviendo el mantenimiento de la entrega de valor a los clientes. Debido a su alto nivel, a la amplia cobertura y porque está basado en muchas prácticas existentes, frecuentemente se refiere a COBIT como un 'integrador', ubicando diferentes prácticas bajo un solo paraguas, y tan importante como eso, ayudando a enlazar estas varias prácticas de TI con los requerimientos del negocio.

COBIT, ITIL e ISO / IEC 27002: Lo que ofrecen y consideran

COBIT

COBIT es un marco de referencia globalmente aceptado para el gobierno de TI basado en estándares de la industria y las mejores prácticas. Una vez implementado, los ejecutivos pueden asegurarse de que se ajusta de manera eficaz con los objetivos del negocio y dirigir mejor el uso de TI para obtener ventajas comerciales.

COBIT brinda un lenguaje común a los ejecutivos de negocios para comunicar las metas, objetivos y resultados **a los profesionales de auditoría, informática y otras disciplinas.**

COBIT brinda las mejores prácticas y herramientas para el monitoreo y la gestión de las actividades de TI.

Debido a que COBIT es un conjunto de herramientas y técnicas probadas y aceptadas internacionalmente, su implementación es una señal de buena gestión en una organización. Ayuda a los profesionales de TI y a usuarios de empresas a demostrar su competencia profesional a la alta dirección. Como ocurre con muchos procesos de negocio genéricos, existen estándares y mejores prácticas de la industria de TI que las empresas deberían seguir cuando utilizan las TI. COBIT se nutre de estas normas y proporciona un marco para implementarlas y gestionarlas.

ITIL

Hoy, las organizaciones dependen de las TI para satisfacer sus objetivos corporativos y sus necesidades de negocios, entregando valor a sus clientes. Para que esto ocurra de una forma gestionada, responsable y

repetible, la empresa debe asegurar que los servicios recibidos de alta calidad de TI deben:

• Satisfacer las necesidades de la empresa y los requisitos de los usuarios.
• Cumplir con la legislación.
• Asignarse y entregarse de forma eficaz y eficiente.
• Revisarse y mejorarse de forma continua.

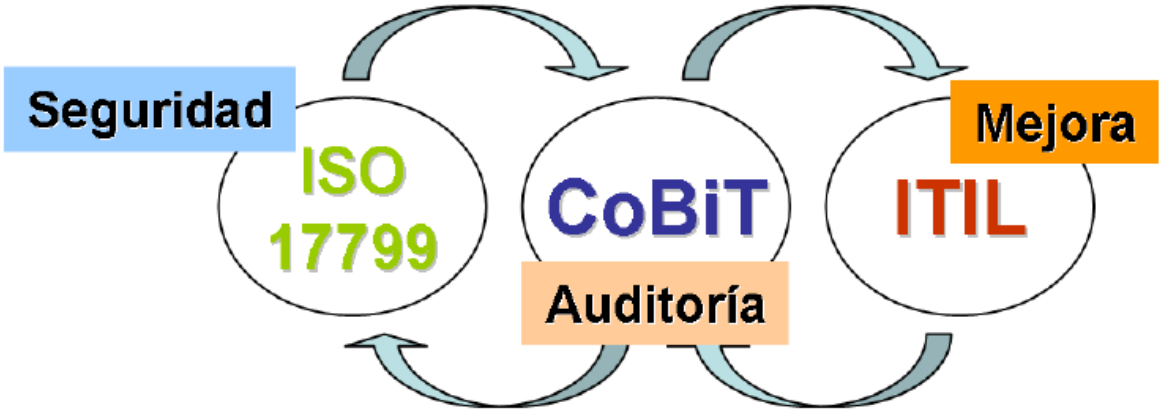
La gestión de servicios de TI se refiere a la planificación, aprovisionamiento, diseño, implementación, operación, apoyo y mejora de los servicios de TI que sean apropiados a las necesidades del negocio. ITIL proporciona un marco de trabajo de **mejores prácticas integra**l, consistente y coherente para la gestión de servicios de TI y los procesos relacionados, la promoción de un enfoque de alta calidad para el logro de la eficacia y eficiencia del negocio en la gestión de servicios de TI.

ISO/IEC 27002

El objetivo del estándar ISO/IEC 27002:2005 es brindar información a los responsables de la implementación de seguridad de la información de una organización. Puede ser visto como una buena práctica para desarrollar y mantener normas de seguridad y prácticas de gestión en una organización para mejorar la fiabilidad en la seguridad de la información en las relaciones interorganizacionales. En él se definen las estrategias de 133 controles de seguridad organizados bajo 11 dominios. La norma subraya la importancia de la gestión del riesgo y deja claro que no es necesario aplicar cada parte, sino sólo aquellas que sean relevantes.

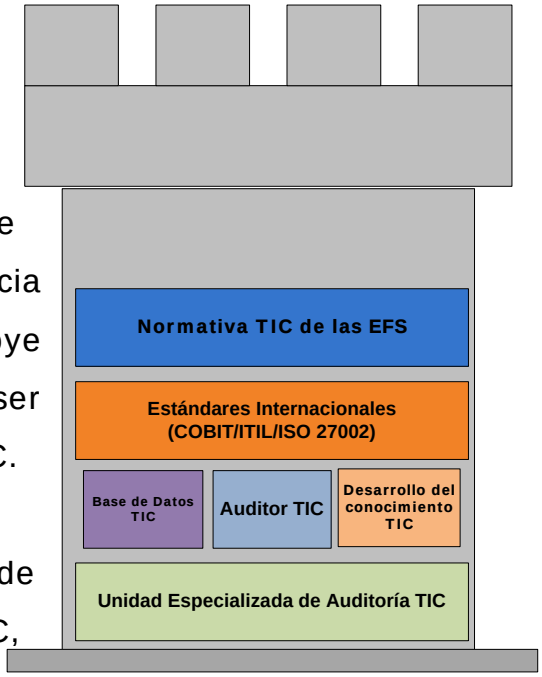
Es importante establecer que no existe una respuesta única a la hora de seleccionar los marcos a utilizar en cada momento. En principio diremos que no hay una aproximación que abarque todo, desde el gobierno de

las TIC a la implementación de los procesos concretos como el de seguridad, y más bien existe un conjunto de aproximaciones que se complementan unas con otras para abarcar todo el escenario, se deben tomar en cuenta las mejores prácticas para ser más efectivos en la ejecución de la auditoria TIC, no necesariamente adquiriendo y aplicando todos sus componentes al pie de la letra, si no enfocando donde su utilización proporcione el mayor beneficio a la auditoria y en el caso de las organizaciones privadas e Instituciones gubernamentales para implementar controles, roles y responsabilidades, orientados a garantizar la integridad, seguridad, confiabilidad de la información; alineando sus procesos sustantivos, hacia una buena gestión de las TIC.



“En la actualidad existen diferentes metodologías orientadas al control de las organizaciones, cada una de ellas abarca diferentes ámbitos, de forma que se complementan.”

3.6 NORMA O POLITICA TIC DE LAS EFS



En Auditoria está claro que "Sin Criterio, no hay hallazgo", y aunque no es el fin de la auditoria obtener el mayor número de hallazgos en un informe, es de suma importancia contar con el respaldo legal y técnico que apoye sus resultados, el control que debe ser observado en la gestión institucional de las TIC. Por consiguiente las EFS deberán crear la normativa que establezca los criterios básicos de control que deben observarse en la gestión TIC, las cuales se han convertido en un instrumento esencial en la prestación de los servicios y representan rubros importantes en los presupuestos del Sector Público.

Los encargados de la administración de las TIC deben contribuir al cumplimiento de dicho marco de control. Así mismo esta normativa deberá ser de acatamiento obligatorio para EFS y las instituciones y órganos sujetos a su fiscalización, y su incumplimiento generará las responsabilidades que correspondan de conformidad con el marco jurídico aplicable.

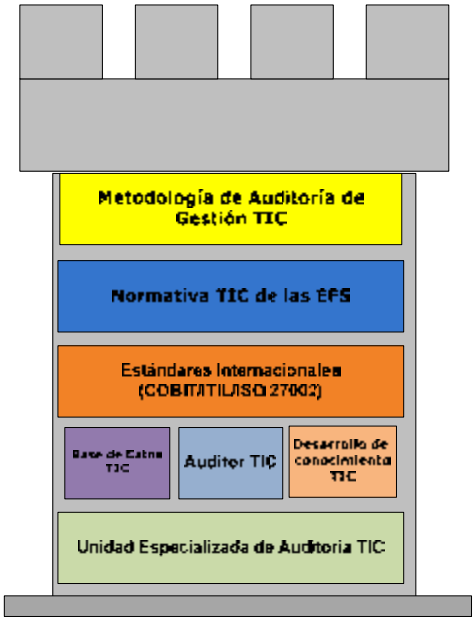
El contenido de la normativa TIC, deberá ser elaborado en base a estándares de aceptación mundial y mejores prácticas en la administración TIC, de los cuales se recomienda efectuar un hibrido basado en tres prácticas y estándares específicos, los que están siendo ampliamente adoptados a nivel global como lo son COBIT, ITIL e ISO

27002, debido a que juntos integran las características de seguridad de la información, gobierno de TIC y gestión de servicios, elementos necesarios para normar y controlar la gestión de las tecnología de información y comunicaciones en las entidades públicas. No obstante las EFS podrán adoptar cualquier otro estándar que se adapte a sus necesidades de control.

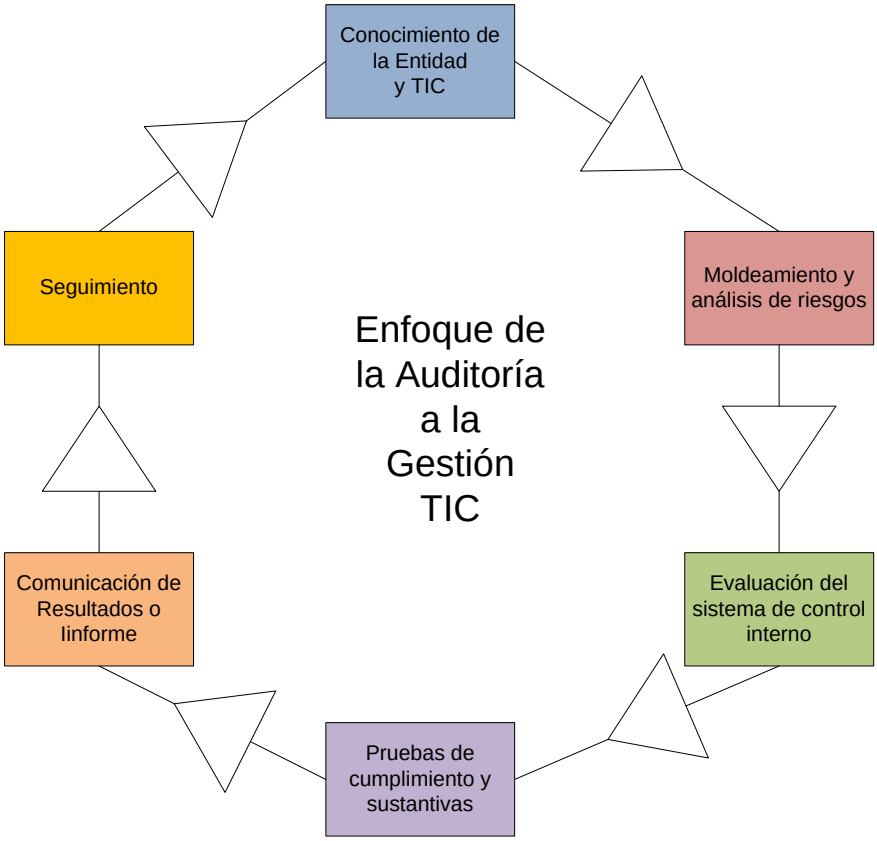
Cuando nos referimos a adoptar un estándar, no involucra aplicar todos sus componentes al pie de la letra, si no, enfocando donde su utilización proporcione el mayor beneficio a la auditoria, y sobre todo que sea tropicalizada a la realidad tecnológica de cada país.

3. 7 METODOLOGÍA DE AUDITORÍA DE GESTIÓN TIC

El Séptimo componente **"Metodología de auditoría de gestión TIC"**, plantea el proceso de la práctica de la auditoría a la Gestión TIC.



3.7.1 METODOLOGÍA DEL PROCESO DE AUDITORIA A LA GESTION DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES



Como en toda disciplina, según la fuente académica o profesional, se dan variaciones para establecer sobre los componentes y designaciones de un proceso de auditoría. De cualquier modo, éstos son muy similares a los de la auditoría financiera. En nuestra metodología, se presentarán fases, etapas y actividades principales, así:

1.- Fase de Planificación
1.1.- Etapa de Análisis General
1.1.1.- Conocimiento de la Entidad Auditada
1.1.2.- Comprensión de las Tecnologías de la Información y Comunicaciones
1.1.3.- Análisis de Sistemas Automatizados de Información (Aplicaciones)
1.1.4.- Modelamiento y Análisis de Riesgos
1.1.5.- Análisis de Índices e Indicadores de Gestión
1.1.6.- Resultados del Análisis General
1.2.- Etapa de Evaluación Preliminar
1.2.1.- Exploración y Esquema de Áreas Críticas para Examen Preliminar
1.2.2.- Evaluación del Sistema de Control Interno Áreas Críticas TIC
1.2.3.- Evaluación del Sistema de Control Interno Procesos Soportado TIC
1.2.4.- Riesgos Vrs Controles
1.2.5.- Resultados del Examen Preliminar
2.- Fase de Ejecución de Examen
2.1.- Pruebas de Control o Cumplimiento.
2.2.- Pruebas de Sustantivas.
2.3.- Pruebas Analíticas.
2.4.- Resultados de la Ejecución de Examen
3.- Fase de Comunicación de Resultados (Informe)
4.- Fase de Seguimiento.

1.- FASE DE PLANIFICACIÓN

La Auditoría a la Gestión de la Tecnología de la Información y Comunicaciones debe planificarse en forma técnica y profesional para alcanzar los objetivos de forma eficiente, eficaz, económica y oportuna. Se debe considerar aspectos como: Conocimiento de la Entidad auditada; comprensión de las tecnologías de la información y comunicaciones; el modelamiento y la gestión de riesgos; los índices e indicadores de gestión de la Entidad; el conocimiento, comprensión y

evaluación del sistema de control interno; la materialidad y el riesgo para determinar la estrategia de la auditoría.

1.1.- Etapa de Análisis General

La etapa de análisis general es obtener información base para formular un plan de trabajo, en ella, se debe obtener información de nivel general, sin entrar en detalles acerca de la entidad, la tecnología de la información, sus sistemas de información (aplicaciones); así también, sobre la gestión de riesgos y los indicadores de gestión.

1.1.1 Conocimiento de la Entidad Auditada

Los auditores deben explorar la Entidad auditada, de forma que puedan conocer y entender de manera general su naturaleza y operatividad. Para obtener un adecuado entendimiento de la Entidad, es importante considerar la información siguiente:

- Marco jurídico externo aplicable a la Entidad
- Normativa interna emitida por la Entidad
- Modelo de Gerenciamiento aplicado por la Entidad
- Misión, Visión, Principios y/o Valores Institucionales.
- Proceso de Planeación Estratégica.
- Plan Estratégico Institucional.
- Objetivos y Metas Institucionales (superiores e inferiores).
- Estructura Organizativa de la Entidad
- Productos y/o Servicios ofrecidos por la Entidad.
- Planes Anuales Institucional
- Planes Anuales de trabajo por unidades administrativas y operativas.
- Manuales de Funciones, Procesos, Procedimientos y Puestos de Trabajo
- Políticas y prácticas de Gestión del Talento y/o Capital Humano
- Indicadores de Gestión Aplicados por la Entidad.
- Funciones y/o Procesos claves de la Entidad
- Método y/o técnica para el Modelamiento y Gestión de Riesgos
- Situación financiera y Presupuestaria
- Entorno Institucional (relaciones con otras instituciones)
- Tratamiento de la Información (clasificación, tipificación, procesamiento)

- Sistema de Control Interno implementado por la Entidad

Como resultado de conocer y comprender la Entidad auditada, el equipo de auditores reflejara dicho entendimiento en matrices y/o diagramas, ejemplo:

Utilizando Herramienta de Diagnostico, TASCOI

Estructura de la herramienta TASCOI	Descripción correspondiente Entidad
Transformación: se refiere a las actividades que la organización hace en el día a día para producir sus bienes y/o servicios.	
Actores: son las personas o funcionarios de la organización que hacen la transformación.	
Suministradores o Proveedores: son las personas que proporcionan los recursos, información e insumos para hacer la transformación.	
Clientes o Usuarios: son todas aquellas personas a quienes van dirigidos los productos, bienes o servicios que transforma la organización.	
Owners (Dueños): son quienes pueden decidir cambios en la transformación de la organización, por ejemplo el gerente, el director, las juntas o consejos directivos, (aunque en las organizaciones estatales, éstos no siempre tienen dicha capacidad o competencia).	
Intervinientes: son aquellas instituciones del entorno, cuyo accionar tiene injerencia en las organizaciones, los efectos pueden ser positivos es decir, que transforman o agregan valor o negativos, en ese caso implican que el organismo tendrá que adaptarse.	

Utilizando Matriz Producto –-> Objetivos --> Impacto

Unidad Organizativa		Producto y/o Servicio	Objetivos y/o Efectos	Impacto
Nivel Decisorio				
1.	Junta Directiva			
2.	Titular de la entidad			
Nivel Asesor				
1.	Auditoría Interna			
2.	Planificación			
Nivel Apoyo				
1.	Oficina Financiera			
2.	Recursos Humanos			
3.	Tecnología de Información			
Nivel Operativo				
1.	Proceso sustantivo 1			
2.	Proceso sustantivo 2			

1.1.2.-Comprensión de la Tecnología de Información y Comunicaciones

Las tecnologías de información y comunicaciones (TIC) es la terminología moderna que se involucra en las Instituciones para facilitar la entrega de los productos y servicios que presta a la sociedad, haciendo uso de nuevos elementos, concepto y herramientas como son: la Internet, la Intranet, la Extranet, las Redes virtuales privadas, la integración de sistemas y plataformas, el portal web institucional, el E_commerce, el E_busines, el E_Services, el E_Gobierno, la Gestión del Conocimiento, el E_learnig, los ambientes virtuales entre otros. Las instituciones deberán contar con TIC para apoyar en forma efectiva su gestión.

Para obtener un adecuado entendimiento de las tecnologías de la información y comunicaciones, es importante considerar la información siguiente:

- Marco jurídico externo aplicable a las TIC's
- Normatividad interna emitida por la Entidad, aplicable a las TIC´s
- Modelo de Gerenciamiento para las TIC´s
- Plan Estratégico de Desarrollo de las TIC's.
- Objetivos y Metas Institucionales apoyados con TIC's.
- Estructura Organizativa de la Función de las TIC's.
- Productos y/o Servicios ofrecidos por la función TIC's.
- Planes Anuales de Trabajo del Área responsable de las TIC's.
- Procesos, procedimientos y Puestos del Área responsable de las TIC's
- Indicadores de Gestión Aplicados a los procesos de la función TIC's.
- Procesos claves del Área responsable de los Servicios TIC's
- Método y/o técnica para el Modelamiento y Gestión de Riesgos TIC's
- Administración de Inversiones de las TIC's
- Servicios TIC´s Tercerizados (Outsourcing)
- Clientes y/o Usuarios de los Servicios TIC's
- Plan de Desarrollo para el Talento Humano en el uso de las TIC's
- Modelo de Gestión a la Seguridad de la Información
- Políticas y Procedimientos de Monitoreo de las TIC's
- Hardware y Software de seguridad a las TIC's
- Plataforma tecnológica utilizada por la Entidad
- Estructura de redes y características de servidores
- Sistemas Operativos (Software Base)
- Inventario de Software y Hardware

- Base de Datos
- Herramientas de Desarrollo de Software Aplicativo
- Telecomunicaciones

El equipo de auditores debe de obtener un conocimiento y compresión de la administración TIC's: Sobre la planificación, que abarca la estrategia y la táctica que se vincula con la identificación de la forma en que la tecnología de información puede contribuir más adecuadamente con el logro de los objetivos Institucionales. Así también debe conocer como se realiza la estrategia de TIC, como se identifica, se desarrolla o adquieren soluciones de TIC y se implementan y se integran en el proceso de la Entidad. Se debe comprender la entrega o prestación de los servicios TIC's requeridos, como se establecen los procesos de soporte necesarios. Es preciso conocer como se monitorea los procesos de TIC a medida que transcurre el tiempo para determinar su calidad y el cumplimiento de los requerimientos de control.

Como resultado de comprender las TIC, el equipo de auditores refleja dicho entendimiento en matrices y/o diagramas, ejemplo:

Unidad o Proceso **Servicios TIC**	**Producto y/o Servicio**	**Objetivo y/o Efecto**	**Impacto**
Comité Técnico TIC	Decisiones Prioritarias	Desarrollo TIC	Incremento en nivel de madures en las TIC
Gerencia TIC	Lineamiento Administrativo	Cumplir Objetivos y metas	Desarrollo TIC Institucional
Desarrollo de Sistemas	Sistemas Automatizado de Información	Automatización de Procesos	Información ágil y oportuna para la toma de decisiones a todo nivel institucional
Administración de Base de Datos	Modelamiento Y disponibilidad de Datos	Distribución de datos a todo nivel	
Soporte técnico	Asistencia Técnica	Satisfacción de Clientes	Mejora Productividad Institucional
Administración de la Red	Funcionamiento de Red de Datos	Mejorar Comunicación	Integración de Funciones Institucionales
Comunicaciones	Funcionamiento medios comunicación	Mejorar metodología de trabajo	Comunicación entre grupos de trabajo
Seguridad y Gestión de Riesgos	Actividades de control	Seguridad Física y Lógica TIC	Seguridad razonable en cumplir objetivos
Capacitación	Conocimiento y Habilidades	Formación del Talento Humano	Personal Idóneo para los puestos de trabajo

Investigación y Desarrollo	Normativa Interna	Aseguramiento consistencia en actividades	Calidad en las operaciones Institucionales

1.1.3.- Análisis de Sistemas Automatizados de Información (Aplicaciones)

Una vez que el Equipo de auditoría se ha familiarizado con el funcionamiento de las operaciones de la Entidad y las TIC, las áreas de interés de la auditoría deben de emprender a ser reconocidas. Se debe de identificar qué sistema de información (aplicaciones) son importantes y críticos para el logro de los objetivos institucionales.

Deben también considerarse si la Entidad está usando las TIC's para aplicaciones significativas del proceso de negocios, su nivel de sofisticación y la extensión de su uso en la organización.

Se debe identificar los objetivos de los sistemas de información (aplicaciones), como también los objetivos a los diferentes niveles de la Entidad (Institucionales, funcionales, procesos, procedimientos), se debe establecer la concatenación entre ellos. Los objetivos de nivel inferior deben alinearse con los objetivos de nivel superior. Se desarrolla matrices que evidencien la identificación de la concatenación de los objetivos, así:

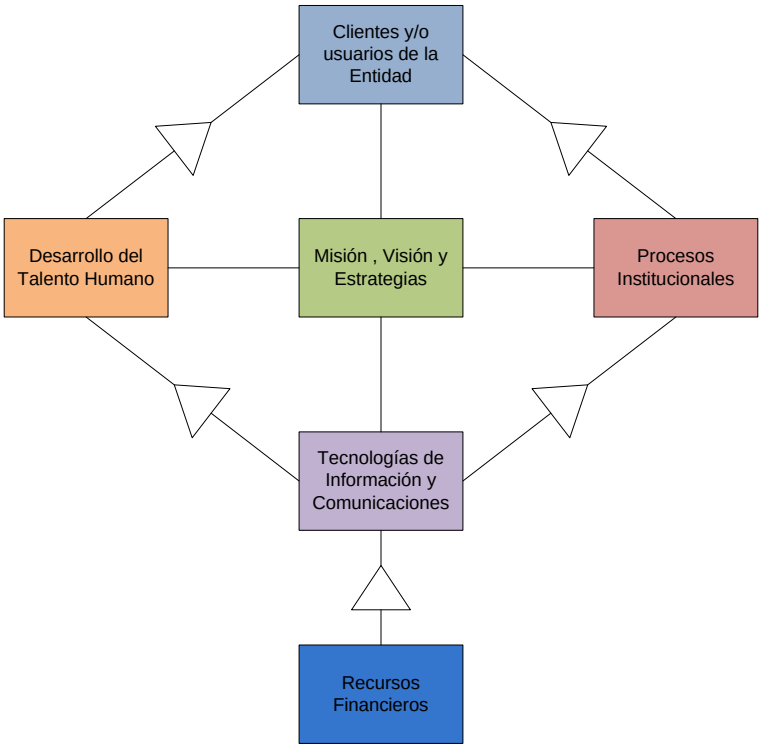
Objetivos Aplicaciones	**Objetivos de Procedimientos**	**Objetivos de Procesos**	**Objetivos Funcionales**	**Objetivos Institucionales**
Sistema de Información A	Pr1-P1-F1-A	P1-F1-A	F1-A	A
	Pr2-P1-F1-A			
	Pr1-P2-F2-A	P2-F2-A	F2-A	
Sistema de Información B				

Cuando las entidades utilizan las TIC's para aspectos significativos del negocio, se debe obtener información acerca de los sistemas automatizados, tales como:

- Descripción o diagrama general de sistema.
- Herramientas de Desarrollo (Lenguaje de programación).
- Normas de procesamiento de datos.
- Manuales de procedimiento usados en los sistemas.
- Procedimientos y medidas para respaldo, recuperación, restablecimiento de operaciones frente a eventos de falla de equipos o destrucción de datos.
- Datos y biblioteca de programas fuentes.
- Manual de normas de documentación.
- Descripción de transacciones de control de seguridad física.

1.1.4.- Modelamiento y Análisis de Riesgos

Modelar y analizar Riesgos de Perspectivas Estratégicas



Como resultado de un conocimiento general de la entidad y las TIC, se debe modelar los riesgos de las perspectivas estratégicas Institucionales, se desarrolla matrices. Ejemplo, aplicando enfoque del Cuadro de Mando Integral (Balanced Scorecard - BSC) así:

Perspectiva de Gestión	Objetivos Estratégicos	Amenazas	Procesos Claves	Áreas de Impacto
Recursos Financiero				
Clientes y/o Usuarios				
Procesos Institucionales				
Talento Humano				

Área de Impacto	Riesgo Primario	Análisis de Riesgos		Store (I*P)
		(I) Impacto o Consecuencia	(P) Probabilidad	

Modelar y Analizar Riesgos de Perspectivas de las TIC

El riesgo tecnológico responde a la probabilidad de que ciertas amenazas afecten en forma negativa a los sistemas de información y su tecnología asociada, y que impacten en los procesos sustantivos de la entidad, afectando el cumplimiento de los objetivos del negocio. El riesgo puede estar relacionado con un proceso clave de la entidad o con un criterio de información tales como: Calidad, Costo, Oportunidad, Efectividad, eficiencia operacional, Confiabilidad de la información, Cumplimiento de leyes y regulaciones, Confidencialidad, Integridad, Disponibilidad u otros criterios determinados en el marco jurídico aplicado y normativa internas de la entidad.

Como resultado del conocimiento de la Entidad y las TIC's, se modela los riesgos de perspectivas de las TIC, para lo cual se debe de identificar los objetivos de nivel superior (planes) de TIC. Se desarrolla matrices, Ejemplo aplicando enfoque COBIT:

Perspectiva de Gestión TIC's	**Objetivos**	**Amenazas**	**Procesos Claves**	**Áreas de Impacto**
Planeación y Organización				
Adquisición e Implementación				
Entrega de Servicios y Soporte				
Monitoreo				

Área de Impacto	**Riesgo**	**Análisis de Riesgos**		**Store (I*P)**
		(I) Impacto	(P) Probabilidad	
Gerencia TIC	Decisiones Erróneas			
	Operaciones no controladas			
Gestión de la Seguridad TIC	Pérdida de Información			
	Hurto y/o daño activos TIC			

1.1.5.- Análisis de Índices e Indicadores de Gestión

De acuerdo a las perspectivas de gestión Institucional (Ej. Cuadro de Mando Integral) se identificaran los índices e indicadores de gestión establecidos, ejemplo:

Indicadores Estratégicos TIC	Porcentaje planificado de beneficios obtenidos vs. beneficios proyectados de TI
	Porcentaje de recursos consolidados/compartidos en las unidades
	Porcentaje de ahorros en el presupuesto total de TI
	Porcentaje planificado de beneficios proyectados vs. obtenidos de TI en toda la organización

Indicadores Clientes **TIC**	Porcentaje de los clientes satisfechos con la entrega de productos TI
	Porcentaje de clientes satisfechos con el mantenimiento y soporte técnico en TI
	Porcentaje de nuevos usuarios capaces de utilizar las aplicaciones de software sin ayuda después de un entrenamiento inicial
	Porcentaje de clientes satisfechos con las soluciones a sus problemas
Indicadores internos de la Entidad en TIC	Porcentaje de disminución de problemas en software
	Porcentaje de proyectos que cumplen los requerimientos de funcionalidad
	Porcentaje de proyectos presupuestados ejecutados oportunamente
	Porcentaje de aplicaciones disponibles
Indicadores de Talento Humano **(innovación y aprendizaje)**	Porcentaje del personal profesionalmente certificado
	Porcentaje de empleados que manejan aplicaciones tecnológicas avanzadas
	Porcentaje del presupuesto de TI asignado a la capacitación y desarrollo del personal
	Porcentaje del personal de gerencia de TI capacitado en habilidades/destrezas gerenciales

1.1.6.- Resultados del Análisis General

En conclusión el análisis general requiere de una concentración de esfuerzo en el conocimiento y comprensión a través del estudio y análisis de la información y documentación solicitada a la entidad y que ha sido detallada anteriormente, lo que permitirá determinar el modelo de gestión a las TIC's aplicado por la Entidad, considerando como base, los estándares: ITIL, ISO 27002, COBIT, COSO, Proceso Administrativo Tradicional (planificación, organización, dirección y control), o un hibrido entre ellos.

Como producto de la etapa del análisis general se identifica las unidades organizativas y/o procesos claves de la Entidad, los cuales serán objeto de una evaluación preliminar, se aplicara juicio sobre la criticidad de los

procesos y definir las áreas, las cuales se denominará Áreas Críticas de Evaluación Preliminar (ACEP's).

Las Áreas Críticas de Evaluación Preliminar (ACEP's), son áreas de mayor importancia para el cumplimiento de los objetivos de la Entidad y los servicios TIC. Debe de considerarse las áreas de impacto con mayor criticidad de riesgos, obtenidas en el análisis general de la aplicación del modelamiento y análisis de riesgos que resultan del mayor escore obtenido de las áreas de impacto.

Las Áreas Críticas de Evaluación Preliminar deben de elegirse de los distintos tipos de procesos: institucionales y servicios TIC, como ejemplo los siguientes:

- Gestión Automatizada de Procesos Operativos
- Gestión Automatizada de Procesos de Apoyo
- Gestión Automatizada de Procesos de Asesoría
- Gestión de los Servicios TIC
    - Gestión de Base de Datos
    - Gestión de Sistemas Operativos
    - Gestión de Redes y Comunicaciones
    - Gestión de Comercio y Gobierno Electrónico
    - Gestión del Ciclo de Desarrollo de Sistema
    - Gestión de Aplicaciones
    - Gestión de Adquisiciones de Bienes y Servicios Informáticos
    - Gestión de Outsourcing
    - Gestión de las Operaciones de Servicios
    - Gestión de la Seguridad
    - Proceso Administrativo (planificación, organización, dirección y control)

La selección de las Áreas Críticas de Evaluación Preliminar (ACEP's) dependerá de criterios definido por la Entidad Fiscalizadora Superior de cada País.

Se finaliza la etapa de análisis general con la preparación de un plan de auditoría para el Examen Preliminar. A menudo se usa una descripción que incluye tablas y la programación que sea apropiada. Las secciones típicas que éste puede incluir son:

- Descripción General de la Entidad Auditada.
- Descripción General de las TIC utilizada por la Entidad
- Descripción de las Áreas Críticas de Evaluación Preliminar (ACEP's).
- Equipo de auditoría.
- Objetivos y Alcance de la auditoría.
- Programación del trabajo.

La estructura y el contenido del Plan de Trabajo para la Evaluación Preliminar, dependerá de criterios definido por la Entidad Fiscalizadora Superior de cada País.

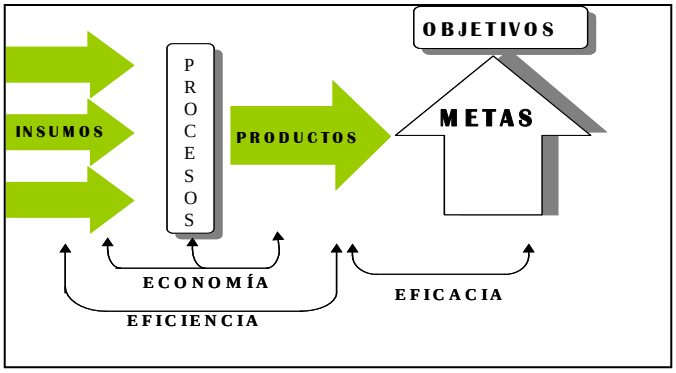
1.2.- Etapa de Evaluación Preliminar

La Evaluación Preliminar, tiene como objetivo explorar en una forma eficiente las Áreas Críticas de Evaluación Preliminar (ACEP's), identificadas durante la etapa de análisis general y profundizar el conocimiento y la comprensión inicial.

En esta etapa es necesario enumerar y agrupar en proyectos de auditoría las Áreas Críticas de Evaluación Preliminar afines. Por cada proyecto y/o ACEP, se deben identificar todos los factores y elementos relativos el flujo de trabajo del proceso. Asimismo, se deben identificar los criterios de auditoría y evaluar el sistema de control interno.

1.2.1.- Exploración y Esquema de Áreas Críticas para Examen Preliminar

Se deberá efectuar conocimiento y análisis específicos sobre las Áreas Críticas (procesos) seleccionados para el Examen preliminar, emprendiendo de diagrama y/o Matrices, "INSUMO – PROCESO – OBJETIVO –IMPACTO", Ejemplo:



ACEP's Institucionales (operativos, apoyo, asesores, decisorio)

Insumos TIC	Proceso y/o ACEP´s	Producto	Objetivo	Impacto
Aplicación	Proceso Operativo A	Producto X	Objetivo A.1	
Infraestructura TIC				
Red y Comunicaciones				
Seguridad				
Internet	Proceso de Apoyo A	Producto Y	Objetivo B.1	
Seguridad				
Aplicativo Web				

ACEP´s de la Gestión de los Productos y/o Servicios TIC

Insumos	Proceso TIC	Producto	Objetivo	Impacto
Recursos Humano	Desarrollo de Sistemas	Software Aplicaciones	Objetivo A.1	
Marco Normativo				
Herramienta de Desarrollo				
Infraestructura Desarrollo				

Recurso Humano Software Normativa	Administración de Base de Datos	Modelamiento Y disponibilidad de Datos	Objetivo B.1	
Marco normativo	Seguridad y Gestión de Riesgos	Controles	Objetivo C.1	

El equipo de auditores debe explorar de manera profunda cada ACEP, de forma que puedan conocer y entender su operatividad. Para obtener un adecuado discernimiento de cada ACEP, es importante considerar la información siguiente

- Normativa (externa y/o interna) aplicada al proceso
- Los insumos necesarios para generar los productos y servicios,
- El flujo de actividades y tareas del proceso,
- Los Puestos de trabajo involucrados en el Proceso
- Los productos y/o servicios generados,
- La trasformación de los productos y/o servicios
- Los objetivos y metas del procesos y actividades
- Los Riesgos del Proceso y actividades
- Los controles claves del proceso,
- Los Factores Críticos de Éxito,
- Los indicadores (logros y desempeño),
- Infraestructura de TIC utilizada
- Procesamiento de información (ingreso, procesamiento, almacenamiento, salida)
- Diagramas Conceptuales y Lógicos de los Sistemas de Información.
- Seguridad TIC

- Otros factores que a juicio profesional del auditor se estimen relevantes para determinar los asuntos y/o puntos críticos a auditar.

1.2.2.-Evaluación del Sistema de Control Interno a ACEP´s de la Gestión de producto y/o servicios TIC.

Los auditores deberán obtener una comprensión o entendimiento del Sistema de Control Interno, suficiente para planear la auditoría, desarrollando procedimientos para entender el diseño de los controles importantes, que han sido implantados y están en operación. Deberá obtenerse entendimiento de cada uno de los componentes orgánicos del sistema de control interno.

Se entenderá como sistema de control interno, el conjunto de procesos continuos e interrelacionados realizados por la máxima autoridad, funcionarios y empleados, diseñados para proporcionar seguridad razonable en la consecución de los objetivos Institucionales.

Al evaluar el Sistema de control interno, es muy importante contar con referentes que constituyan el modelo contra el cual contrastar la realidad institucional. Es así que los profesionales, al hacer un juicio frente al contexto en que se encuentran, seleccionan los controles aplicables, y de ese subconjunto, surge el marco sobre el cual se ha de comparar el estado del control interno.

Siempre ha de utilizarse los mejores y modernos referentes o modelos de control, los cuales, día a día están evolucionando o surgiendo. Por la vía del ejemplo, se pueden mencionar entre otros:

- COSO (Control interno. USA).
- CoCo (Control Interno. Canadá)
- Informe Cadbury (Gobernabilidad Corporativa Financiera. UK).
- Informe Turball (Gobernabilidad Corporativa. UK)
- COBIT (TI. USA)

- eSAC (TI. USA)
- Informe Olivencia (Transparencia y Seguridad Mercds. Bursátiles. España),
- ISO / IEC 27002 (TI. Internacional)
- ITIL (Administración TI. UK).
- GASSP (Generally Accepted System Security Principles) (TI. USA)
- Etc.

Estos modelos de control, además de otras variables, pueden diferenciarse entre estándares o normas, y regulaciones. Por otra parte, ningún estándar es autosuficiente por sí mismo, por lo que con frecuencia, unos son complementarios de otros en determinados aspectos, y por cierto, también se solapan unos a otros.

El modelo, la estructura y el contenido del Sistema de Control Interno, dependerá de criterios definido por la Entidad Fiscalizadora Superior de cada País. Por lo que la evaluación del sistema del control interno dependerá de cada EFS. Para efectos de ejemplo presentamos un esquema aplicando cuestionarios por cada componente y áreas TIC, con el enfoque COBIT, así:

Componente y áreas a Evaluar el Control Interno		Número de Preguntas	Puntos	Ponderación
1.- Planificación y Organización				
	Gerencia TIC			
	Comité Técnico TIC			
2.- Adquisiciones e implementación de TIC				
	Desarrollo de Sistemas			
	Gestión de Base de Datos			
3.- Entrega de Servicios y soporte de TIC				
	Soporte Técnico			
	Seguridad			

4.- Monitoreo				
	Investigación y Desarrollo TIC			
	Auditoría Interna			

1.2.3.- Evaluación del Sistema de Control Interno a ACEP's Institucionales

Además de evaluar el sistema de control interno al área de los servicios TIC, será necesario hacer evaluaciones a cada una de las ACEP´s de los niveles operativo y/o administrativo de la Entidad. El modelo, la estructura y el contenido del Sistema de Control Interno, dependerá de criterios definido por la Entidad Fiscalizadora Superior de cada País. Por lo que la evaluación del sistema del control interno dependerá de cada EFS. Para efectos de ejemplo en nuestra propuesta sugerimos aplicar COSO II-ERM (Enterprise Risk Managemnet – Gestión Integral de Riesgos). Siendo los componentes del control interno los siguientes: ambiente de control, establecimiento de objetivos, Identificación de Eventos, evaluación del riesgo, Respuestas al Riesgos, actividades de control, información y comunicación y monitoreo de la entidad. Se utilizara cuestionario para cada una de las ACEP´s, Así:

Proceso y/o ACEP´s	Número de Preguntas	Puntos	Ponderación
Proceso Operativo A			
Proceso de Apoyo B			

Además, se evalúan los controles internos dentro del ambiente de Sistemas de Información para asegurarse de la validez, confiabilidad y seguridad de la información.

1.2.4.- Evaluación de Riesgo Versus Efectividad de Controles.

El Objetivo de esta actividad es identificar la exposición al riesgo a través de la medición de los controles implementados para las actividades que están sujetas a riesgo. El equipo de auditores deberá realizar los aspectos siguientes:

- Identificar las matrices que están relacionadas con el modelamiento de riesgos.
- Identificar los controles aplicados a las actividades que están sujetas a riegos operacionales.
- Elaborar una matriz comparativa que contenga el modelamiento de riesgos versus los controles aplicados a cada actividad sujeta al riesgo.
- El auditor deberá conocer el método de análisis de riesgos utilizado por la entidad, y adaptar las ponderaciones a las definidas.
- Tomar los Riesgos con mayor criticidad identificados en el análisis general
- Analizar los controles aplicados para administrar el riesgo
- Analizar la efectividad de los controles aplicados
- Evaluar los riesgos contra los controles aplicados

Se desarrolla matrices que evidencien la evaluación de Riesgos Vrs controles, así:

Área de Impacto	Análisis de Riesgos			Score de Riesgo	Controles Críticos Imperantes				Exposición al Riesgo
	Riesgo	Probabilidad	Impacto		Actividad	Tipo	Clasificación	Efectividad	

1.2.5.- Resultados del Examen Preliminar

Con base en los resultados del conocimiento y análisis específicos de las ÁCEP´s, el cumplimiento al marco normativo del control interno y a la Exposición al riesgo, se hará una conclusión sobre lo adecuado del Sistema de Control Interno a las Áreas Críticas de Evaluación Preliminar. Así mismo, se determinara el riesgo y materialidad de auditoría. También se debe de identificar las Actividades Críticas de Pruebas de Auditoría (ACPA). Que son los puntos y/o hechos importantes en donde el auditor considera que existen presuntas deficiencias, las cuales deben de ser evidenciadas en la siguiente fase del proceso auditoría.

1.2.5.1 Riesgo de Auditoría

El Riesgo de Auditoría (RA) es la probabilidad de que el auditor inadvertidamente pueda llegar a una conclusión incorrecta basado en los hallazgos de auditoría. Esto puede deberse a errores o irregularidades existentes y que aquél no logró detectar con la aplicación de sus procedimientos de auditoría.

Para cada auditoría se determinarán los riesgos relacionados con las operaciones de la entidad, programa, área o actividad sujeta al examen. Existen los riesgos inherentes o propios de las actividades operacionales de la entidad, los riesgos de control generados por la ausencia de procedimientos en el diseño de los controles internos y el riesgo de detección o riesgo de auditoría, el cual consiste en posibilidad de emitir un informe sin que los errores o irregularidades importantes incluidos en las operaciones, programa, área o actividad de la tecnología de información y comunicaciones, hayan sido detectados por los procedimientos de auditoría programados y aplicados.

Se determinará el Riesgo de Auditoría de acuerdo a los resultados obtenidos de la evaluación del sistema de control interno y la evaluación de riesgos versus controles. También se comprende que el Riesgo de Auditoria (RA) es el máximo riesgo posible que el auditor está dispuesto a asumir que, en su conjunto, los errores no sean detectados durante la Auditoría.

Se deberá considerar la experiencia y capacidad del recurso humano asignado al equipo de auditoría a fin de determinar el máximo riesgo posible dispuesto a aceptar para que los errores en la gestión de la tecnología de información y comunicaciones de la entidad auditada no sean detectados durante la auditoría.

El Riesgo de Auditoría se determinara aplicando la ecuación típica, aplicada en cualquier tipo de auditoría, así:

RA = RI * RC * RD

Riesgo de Control (RC), Se ha evaluado el control interno a las aéreas responsables de las TIC, a procesos operativos y administrativos institucionales y a la unidad de Auditoría Interna (siempre que dicha unidad efectúe auditoria a las TIC).

Riesgo Inherente (RI).- Se ha ponderado en un 50% el riesgo inherente que es la posibilidad de que los procesos automatizados (apoyados con TIC) de la Entidad, contengan errores que puedan ser importantes al sumarse a los errores de los sistemas informáticos, a pesar de los controles internos establecidos en cada uno de ellos y por el grado de susceptibilidad de los diferentes productos y servicios TIC utilizados en la Entidad.

Riesgo de Detección (RD).- Representa el riesgo de que los procedimientos que aplique el auditor no le permita detectar errores en la gestión a las TIC.

1.2.5.2.- Materialidad o Importancia Relativa

Este concepto tiene una importancia gravitante en las decisiones de auditoría, a la hora de definir las Actividades Críticas de Pruebas de Auditoría (ACPA) y los puntos y/o hechos importantes en donde a criterio profesional del auditor, considera que existen presuntas deficiencias a ser examinadas con mayor profundidad. También es importante respecto a la asignación de recursos de tiempo, expertos, requerimientos tecnológicos para pruebas, etc.

La materialidad se relaciona con el mayor puntaje obtenido a la exposición al riesgo el cual resulta de la diferencia entre el score de riesgos menos la efectividad del o los controles aplicados al riesgo encontrado.

La Materialidad de la auditoría será establecida considerando el proceso para identificar los asuntos de potencial importancia, como resultados de los aspectos siguientes:

- Modelamiento y análisis de riesgos, determinando las Áreas Críticas de Evaluación Preliminar (ACEP's)
- Evaluando los riesgos Versus los controles, determinando Áreas Criticas con mayor exposición al Riesgo (actividades relevantes)

La materialidad determinada en la fase de planeación, surge aplicando para la auditoría el enfoque metodológico del modelamiento y gestión de riesgos.

1.2.5.3.- Plan de Ejecución del Examen

Se finaliza la etapa de Examen Preliminar con la preparación de un plan de auditoría para la Ejecución del Examen. La estructura y el contenido del Plan de Examen, dependerá de criterios definido por la Entidad Fiscalizadora Superior de cada País. Como ejemplo presentamos lo siguiente:

- Introducción
- Objetivos y Alcance de Auditoría
- Diagramas y/o matrices de las Áreas Críticas de Examen Preliminar.
- Resultados de la Evaluación de Control Interno.
- Determinación de riesgo y materialidad de la auditoría
- Identificación de Fuentes de Criterio de auditoría
- Bosquejo del Plan del Examen de Auditoría
    - Nombre del Proyecto
    - Objetivos del Proyecto
    - Áreas de Impacto con mayor exposición de riesgo
    - Actividades Críticas para Pruebas de Auditoría (ACPA).
    - Identificación de Criterios de Auditoría a ser aplicados.
    - Recursos (Tiempo, especialista, materiales, HW/SW medición)
- Cronograma de Actividades

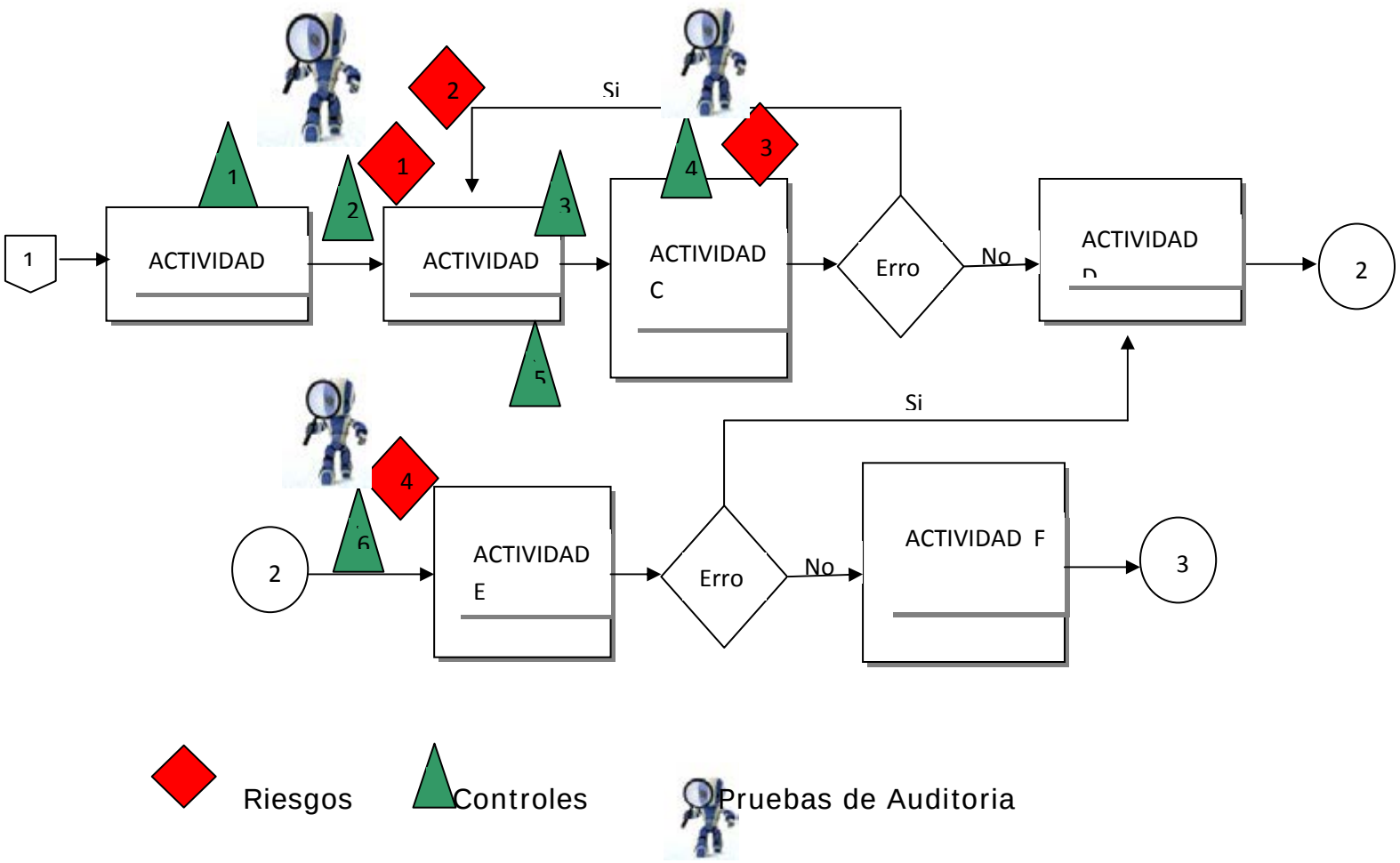
2.- Fase de Ejecución del Examen

La Aplicación de Pruebas de Auditoría de Gestión en la fase de ejecución le permitirá cumplir con el plan y programa de auditoría, lo cual debe derivar en hallazgos bien sustentados con evidencias suficientes, competentes y pertinentes. Se utilizaran 3 tipos de pruebas:

- Pruebas de Control o de Cumplimiento
- Pruebas Sustantivas
- Pruebas Analíticas
    - Análisis Comparativo usando Índices e Indicadores
    - Análisis Estadístico
    - Análisis de Regresión
    - Análisis de Costo Beneficio
    - Simulaciones y Modelos
    - Mapeo de Flujos de trabajo y de Comunicaciones
    - Pruebas de Proceso Insumo–->Proceso-->Producto (Evaluar 3 E's)
    - Benchmarking (análisis comparativo mejores prácticas)

Las pruebas de auditoría serán dirigidas a las actividades críticas y para un adecuado direccionamiento de la ejecución de examen, es recomendable diseñar una matriz y/o diagramas, en donde se refleje hacia donde están siendo enfiladas las pruebas de auditoría, así:

Área de Impacto con Mayor Exposición a Riesgos	Área Critica de Examen Preliminar	Actividad Critica Para Pruebas	Criterios de Auditoría	Pruebas de Auditoría



2.1.- Pruebas de Control o de Cumplimiento.

En el plan y programa de trabajo, se identifican las actividades de control que se consideran efectivas para prevenir, detectar o corregir, los errores e irregularidades importantes en las áreas, procesos, procedimientos, actividades y sistemas que se auditan. Tales actividades constituyen la base para la evaluación preliminar del riesgo de control, desde bajo o moderado hasta alto riesgo, constituyen a su vez la base para modificar la naturaleza, oportunidad y alcance de los procedimientos sustantivos de auditoría que se planearon. Además, mediante la aplicación de las pruebas de control obtenemos evidencia sobre la efectividad del diseño y operación de las actividades de control.

Generalmente, las pruebas de control aplican combinando técnicas de obtención de evidencia, pero aplicadas para obtener la evidencia relacionada con los todos los modelos y componentes del control interno (TIC y Procesos Institucionales). Estas técnicas combinadas o por separado pueden ser las entrevistas, encuestas, cuestionarios, indagación, observación rastreo e inspección documental, pero también puede involucrar otras técnicas de auditoría como las Técnicas de Auditoría Asistidas por Computadoras (TAAC).

Para complementar las pruebas de control, cuando sea aplicable, es necesario elaborar pruebas al software que se utiliza en la ejecución o control de los procesos misionales de la entidad auditada y verificar el funcionamiento y control de sus sistemas, esto permite inferir resultados a partir de una muestra de observaciones a la población total.

La obtención de evidencia suficiente sobre la efectividad del control interno depende de la naturaleza, oportunidad y alcance de las Pruebas de control aplicadas.

El auditor debe considerar aquellos controles que tienen mayor impacto para el cumplimiento de los objetivos de auditoría (Controles Claves). Para la Planificación de las Prueba de control o Cumplimiento, se debe de considerar los aspectos siguientes:

- ¿Qué Área Critica para Examen Preliminar voy a verificar?
- ¿Qué Actividad Critica Para Pruebas de Auditoría (ACPA) voy a verificar?
- ¿Qué riesgos están involucrados en la ACPA?
- ¿Qué datos y informaciones necesito para la realización de la prueba?
- ¿Dónde están los datos (sistemas)?
- ¿Qué técnica de auditoría aplicaremos para la prueba?
- ¿Qué herramienta (TAAC) voy a utilizar?

Cuando es necesario utilizar apoyo del computador, y el procedimiento se define como una TAAC's, deben cumplirse todas las normas referentes a la planificación, diseño, testing, ejecución, documentación y revisión de la misma. Las TAAC's aplicadas a las pruebas de cumplimiento, por lo general, se refieren a la verificación de controles generales de las TIC.

2.2.- Pruebas Sustantivas

Una vez determinado el riesgo en el control interno, se aplican las pruebas sustantivas programadas en el plan y programas de trabajo, en la densidad y según la muestra que la confiabilidad de los sistemas de control permita, de manera tal que a mayor confiabilidad menor será la muestra.

Las pruebas sustantivas nos permiten precisar y comprobar la información referida a los procesos misionales o de apoyo de la organización, a fin de obtener la información y evidencia que analizaremos mediante una o varias de las técnicas o procedimientos analíticos, que sean pertinentes utilizar.

Estas se encuentran directamente orientadas a probar la calidad o veracidad de los productos finales de los sistemas, a diferencia del caso anterior, cuyo objetivo era verificar que los controles que soportan los procesos sean adecuados para garantizar la producción de buenos output o productos.

Las principales técnicas que, entre otras se aplican como pruebas sustantivas: Comparación, Cálculo, Confirmación, Inspección, Examen físico, Rastreo. Pero también puede involucrar otras técnicas de auditoría como las Técnicas de Auditoría Asistidas por Computadoras (TAAC). Para la Planificación de las Pruebas sustantivas, se debe de

considerar los mismos aspectos tomados para las pruebas de control o cumplimiento.

2.3.- Pruebas Analíticas.

La documentación e información recopilada a través de la aplicación de la pruebas de control y sustantivas, deberá ser analizada y evaluada por el equipo de auditoría, hasta el grado en que les permita determinar problemas e inferir desviaciones en los procesos y actividades sujetos a Examen, y definir los hallazgos de auditoría, son muchas las pruebas que se pueden aplicar como procedimientos analíticos en la fase de ejecución, entre ellos podemos mencionar:

2.3.1.- Análisis Comparativo usando Índices e Indicadores.

También utilizable en la fase de planeación, en la fase de ejecución sirve para comparar valores reales encontrados (condición) con los esperados (metas), para calificar o cuantificar un hallazgo de auditoría en el contexto, de manera tal de observar sus causas y efectos, para observar o detectar un cambio extraordinario, producto del análisis comparativo del desempeño histórico al interior de la misma organización o comparándola con indicadores de organizaciones similares, para establecer el grado con el cual se satisfacen los criterios.

2.3.2.- Análisis Estadístico.

Ayuda a decidir si una variable o resultado de ejecución o gestión satisface un criterio de auditoría o para interpretar distribuciones de probabilidad para evaluar riesgos o determinar tendencias; además, para evaluar si una muestra de datos es representativa de la población.

2.3.3.- Análisis de Regresión.

Implica revisar el comportamiento histórico de una situación, mediante la desagregación en el tiempo del comportamiento de las variables que lo componen, sirve para probar una relación que se supone existente, para identificar y evaluar valores inusuales o extremos (desviaciones) que no se ajustan a la relación regular entre dos variables, para hacer predicciones o proyecciones (inferencias) a partir de una relación observada que se ha dado en el pasado, y para construir modelos de las operaciones de la entidad auditada.

2.3.4.- Análisis de Costo Beneficio.

Sirve para tener certeza de que un análisis realizado por el equipo auditor satisface las normas profesionales. Se basa en la comparación de costos y beneficios, cuando ambos son conocidos o pueden ser razonablemente estimados; y la comparación de costos alternativos cuando los beneficios pueden ser asumidos como invariables.

2.3.5.- Simulaciones y Modelos.

Consiste en formular modelos o escenarios lógicos hipotéticos, definiendo un criterio basado en el deber de ser de procesos y productos sobre el aspecto evaluado, permite evaluar la idoneidad de los modelos encontrados al compararlos con el que el auditor usa para la toma de decisiones importantes; y responder la pregunta ¿Qué importancia tiene?, acerca del impacto de los problemas de auditoría, observaciones y recomendaciones.

2.3.6.- Mapeo de Flujos de Trabajo y de Comunicaciones.

Consiste en realizar un mapa de los procesos que se realizan, identificando los puntos críticos, cuellos de botella, las tomas de decisiones, las unidades de gasto, la oportunidad de las comunicaciones y cualquier otro aspecto que se considere importante para definir, en

base a un problema de auditoría, las causas y efectos probables, sirve para adquirir una comprensión de cómo una organización o sistema funciona, particularmente cuando el sujeto de la auditoría involucra muchos departamentos, unidades, o pasos complicados. Puntualiza los puntos clave de control y donde deben ampliarse la aplicación de pruebas de auditoría.

2.3.7.-Pruebas Proceso insumo-proceso-producto para evaluar las 3 E's.

Las mediciones de la Eficiencia, Eficacia y Economía en un proceso misional o de apoyo de una gestión, conocidas a menudo como las 3 E's, conforman la plataforma teórica de la auditoría de gestión. Para evaluar estos tres criterios se toma información o variables del proceso y se constituyen o evalúan con los indicadores de gestión. Para ello, el primer paso a realizar consiste en analizar los procesos determinando las entradas (insumos) y salidas (productos) de los procesos y revisando las actividades y tareas que se realizan. Una vez que conocemos estos aspectos podemos identificar variables de insumo, proceso y producto, para compararlas con las metas y objetivos de la organización, y con las variables del entorno, formular o interpretar indicadores de gestión.

La evaluación de la eficiencia se centra en la formulación o interpretación de los indicadores que consideran variables de insumo y variables de producto, es decir, medimos mediante las variables que intervienen en el indicador, el uso de los recursos en relación con el producto, bien o servicio que se deriva de los procesos.

La evaluación de eficacia se centra en la formulación o interpretación de indicadores que consideran variables de producto con los objetivos y metas, que la organización auditada se plantea, medimos entonces si el bien o servicio que se produce cumple total o parcialmente con los objetivos y metas que se formula el ente auditado, de acuerdo a su misión y a los requerimientos que la sociedad le exige.

La evaluación de economía relaciona variables de insumo y de producto, pero asociadas con los costos de los insumos o los procesos para generar el producto, bien o servicio que se requiere.

2.3.8.- Benchmarking (análisis comparativo mejores prácticas).

Esta técnica administrativa sirve para estimular una revisión objetiva de procesos, prácticas y sistemas importantes para la gestión de una entidad auditada mediante la comparación de su desempeño con una organización similar, considerada líder en su campo. Es útil para el auditor para el desarrollo de criterios y para identificar mejoras potenciales en las operaciones al presentar una meta común para el mejoramiento de la organización auditada. Además, sirve para obtener datos objetivos fuera de la organización y evidencia de auditoría competente para dar más credibilidad a las recomendaciones.

2.4.- Resultados de la Ejecución de Examen

Con base en los resultados obtenidos de las pruebas de auditoría, se hará una conclusión sobre lo adecuado de la Gestión TIC de las Áreas Críticas de Evaluación Preliminar y como efecto subsecuente de la Entidad. Así mismo, se determinara el los Hallazgos y deficiencias menores. Cuando existan oportunidades de mejoras, se debe de emitir recomendaciones dirigidas a incrementar la madures en la gestión TIC.

Una vez evidenciado los hallazgos de auditoría y las deficiencias menores, se elabora un informe de cada proyecto desarrollado, los cuales serán los insumos para la elaboración del borrador de informe de auditoría y la Carta de Gerencia.

Los hallazgo de auditoría se incluirán con todos sus atributos en el borrador de informe de auditoría y las deficiencias menores se incluirán en una nota que se denominará “Carta de Gerencia”

Los auditores prepararán recomendaciones siempre que existan acciones correctivas o preventivas, que mejoren la gestión de la entidad auditada, caso contrario no se emitirán. Las recomendaciones se presentarán en un capitulo aparte de los resultados de la auditoría.

Se finaliza la fase de Ejecución de Examen con la preparación del Borrador de Informe de Auditoría. La estructura y el contenido del Borrador de Informe, dependerá de criterios definido por la Entidad Fiscalizadora Superior de cada País. Como ejemplo presentamos lo siguiente:

- Introducción
- Objetivos y alcance de la auditoría
- Limitaciones en el alcance de la auditoría
- Descripción General de la Entidad y Gestión TIC
- Resultados de la auditoría:
- Proyecto Examinados
- Descripción de Áreas Criticas
- Hallazgos
- Conclusión por proyectos
- Recomendaciones

3.- Fase de Comunicación de Resultados (Informe)

El equipo de auditoría elaborará y comunicará por escrito, a los funcionarios de la entidad u organismo auditado, un informe que describa el alcance y los objetivos de la auditoría, así como los comentarios, conclusiones y recomendaciones sobre los hallazgos relacionados con los objetivos de la auditoría, a fin de que adopten las recomendaciones y las medidas correctivas de manera oportuna.

El Equipo de Auditoría, deberá preparar, editar y entregar el Informe final de Auditoría, el cual debe ser oportuno, completo, exacto, objetivo y convincente. Asimismo el informe debe ser claro y conciso para que

sea comprensible para los interesados, principalmente para aquellos que deben tomar decisiones respecto de las recomendaciones emitidas.

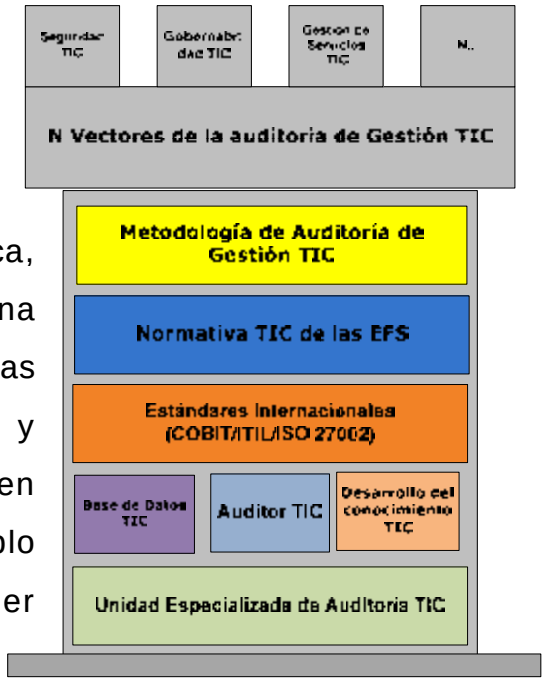
Se elaborará el Informe Definitivo, siempre que el Comité Técnico de Auditoría y los funcionarios de la entidad auditada hayan hecho las observaciones correspondientes. La estructura y el contenido del Informe de Auditoría, dependerá de criterios definido por la Entidad Fiscalizadora Superior de cada País. Como ejemplo se presente lo siguiente:

- Resumen Ejecutivo.
- Informe de Auditoría de Gestión a los Sistemas de Información
- Objetivos y Alcance de la Auditoría
- Limitaciones
- Información de la Entidad y la Gestión TIC
- Principales realizaciones y/o logros
- Resultados de la auditoría (Desarrollo de proyectos de auditoría)
- Proyecto Examinados
- Descripción de Áreas Criticas
- Hallazgos
- Conclusión por proyectos
- Recomendaciones
- Conclusión general
- Identificación, Firma y Fecha

4. Seguimiento

El informe de auditoría contiene regularmente hallazgos y recomendaciones orientadas a superar dichas deficiencias, las que se convierten a su vez en un compromiso para la entidad auditada. En consecuencia, el auditor efectúa revisiones posteriores para evaluar el grado de cumplimiento de las recomendaciones, determinando si éstas han dado los resultados esperados, todo lo cual debe ser reportado en la forma acordada con la administración.

3.8 LOS N VECTORES DE LA AUDITORIA DE GESTIÓN TIC.



¿Hacia dónde nos dirigimos? Nuestros vectores, representan la dirección y sentido de la Auditoria de la gestión TIC en el tiempo. Nos referimos al factor tiempo ya que la tecnología es dinámica, y lo que hoy es de vanguardia, mañana ya no lo es. Así que para que las auditorias TIC sean siempre efectivas y oportunas hay que dirigir nuestro examen con objetivos actualizados, como ejemplo podemos mencionar que mantener actualizados los enfoques

1. **Seguridad**
2. **Gobierno de TI**
3. **Servicios**
4. **N…**

3.8.1 SEGURIDAD

¿Qué es la seguridad?, El término seguridad proviene de la palabra *securitas* del latín. Cotidianamente se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia, que para nuestro ámbito de investigación, será la seguridad en las TIC.

Hace aproximadamente 35 años los riesgos de un ataque, o acceso no autorizado a los datos almacenados en un computador eran mínimos, debido a que la tecnología era utilizada por solo por los expertos en informática, y no era accesible a todas las personas comunes, así

mismo, dichos ordenadores eran resguardados en edificios sin contar con muchos servicios online, se trabajaba en ellos directamente y no desde alguna terminal remota, por lo que la seguridad prácticamente se basaba en una buena cerradura y alguno que otro guardia de seguridad que impidiera el acceso físico a los servidores. Hoy en día este escenario ha cambiado, ahora hasta una persona sin conocimientos bastos en informática y, desde la tranquilidad de su casa podría causar algún daño a un sistema informático y robar información de alguna base de datos, sin dejar de mencionar un ataque planificado por un Hacker.

Lo cierto es que el mundo de hoy, donde las tecnologías de la información y comunicaciones avanzan a grandes velocidades, es cada vez más vulnerable al ataque de estos individuos.

ANTECEDENTES INTERNACIONALES DE SEGURIDAD

Existe un sin número de ataques informáticos famosos en la historia, pero para nuestra investigación detallaremos uno reciente para analizar el impacto que este podría tener en los diferentes ámbitos sociales y las pérdidas multimillonarias que podrían generar dichas acciones delictivas “Cyber terrorismo”.

El caso se narra desde el problema de seguridad, aparentemente insignificante desde la perspectiva de un usuario de TICs, hasta llegar al impacto negativo que se generó en la empresa.

El Caso SONY

Una mañana durante la vacación de Semana Santa (2011) me dispuse a disfrutar tiempo, jugando videojuegos en línea “haciendo uso del internet” con una consola de SONY “PlayStation 3”, así que, para iniciar la partida ingrese con mi usuario y contraseña a los servidores de

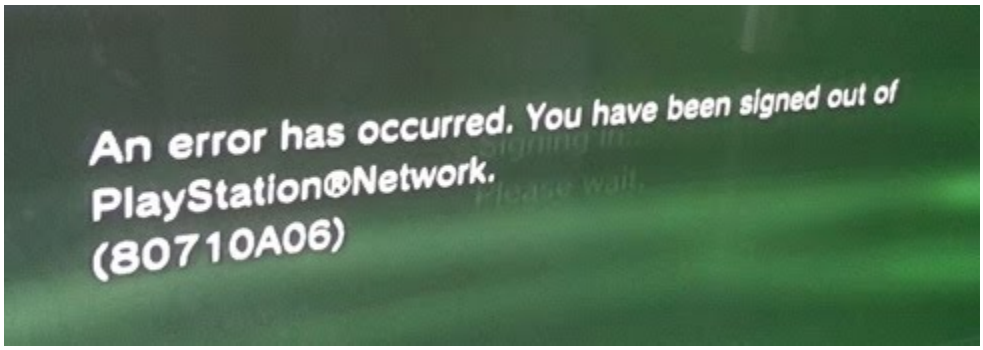
PlayStation Network de SONY, pero como cosa no usual, el sistema me advirtió un mensaje de error; inicialmente pensé que solo era algún problema en mis dispositivos de comunicaciones, el servicio de internet o la consola de juegos misma, pero después de varios pruebas, mi desesperación me llevo a consultar por internet si pasaba algo más que estuviera fuera de mi alcance. Y en efecto, empecé a encontrar en sitios web, noticias y comentarios como los siguientes.

Día 21 de abril del 2011

"**PlayStation Network cerrada a nivel mundial, código de error 80710A06**

Los usuarios no pueden acceder a PlayStation Network, se baraja la posibilidad de un ciberataque de Anonymous"

A través del Blog Oficial de PlayStation nos llega una mala noticia para todos los aficionados al juego online en PlayStation 3.



El servicio PSN se encuentra cerrado por tareas de mantenimiento, aunque debido a problemas inesperados podríamos tardar hasta 48 horas en tener restablecida la conexión con los servidores de Sony. "

Al parecer hasta ese entonces solo era cuestión de esperar unas 48 horas para restablecer todos los servicios, pero las sorpresas continuaron con los días y SONY declaro en sus sitios oficiales que sus

servicios tomarían más de 48 horas en restablecerse, siendo la fecha límite para el inicio de operaciones "indefinida".

Página Web consultada:
http://www.zonared.com/ps3/noticias/playstation-network-cerrada-nivel-mundial-codigo-error-80710a06/

Día 3 de mayo 2011

"Sony Online Entertainment anuncia el robo de datos de sus sistemas

El ataque por parte del Hackeo criminal hacía SOE se considera detenido

Tokio, 3 de mayo de 2011 - Sony Corporation y Sony Computer Entertainment han anunciado hoy que la investigación en curso acerca de las intrusiones ilegales en Sony Online Entertainment LLC (SOE) revelaron ayer por la mañana (2 de mayo, hora de Tokio) que los hackers pueden haber robado información de los clientes de SOE durante su intrusión los días 16 y 17 de abril de 2011 (PDT). SOE tiene su sede en San Diego, California, EE.UU.

Esta información, que fue descubierta por los ingenieros y consultores de seguridad revisando los sistemas de SOE, mostró que la información personal de aproximadamente 24.6 millones de cuentas de SOE pueden haber sido robados, así como cierta información de una base de datos desactualizada de 2007. La información de la base de datos obsoleta que puede haber sido robada incluye aproximadamente 12.700 números de tarjetas de crédito y débito de fuera de Estados Unidos así como sus fechas de caducidad (los códigos de seguridad de las tarjetas están a salvo), y cerca de 10.700 registros de las cuentas de determinados clientes en Austria, Alemania, Países Bajos y España"

Página Web consultada:

http://community.eu.playstation.com/t5/Ayuda-PlayStation-Network/Comunicado-de-Prensa-de-Sony-Online-Entertainment-sobre/m-p/12802642?WT.mc_id=TSO_ES_0098

Día 10 de mayo 2011

"**Sony desconoce el impacto económico del ataque a PSN**

La compañía cree que se tardarán meses en calcular las pérdidas

En su opinión, las pérdidas podrían superar los 864 millones de euros."

Página Web Consultada:

http://www.meristation.com/v3/des_noticia.php?id=cw4dc958084b470&pic=GEN

Día 18 de mayo 2011

"Sony Computer Entertainment incrementa las medidas de seguridad antes de restablecer los servicios de PSN.

Incremento de las medidas de seguridad

Como resultado del ataque cibernético sufrido por el centro de datos de la empresa ubicado en San Diego, California (Estados Unidos), SNEI cerró el acceso a los servicios de PlayStation Network y Qriocity el 20 de abril de 2011 para llevar a cabo una investigación y realizar mejoras globales en la seguridad de la infraestructura de red.

Tras colaborar estrechamente con varias compañías de seguridad externas, la empresa ha implementado medidas de seguridad adicionales para incrementar la protección contra actividades no autorizadas, así como ofrecer a sus clientes una mayor protección de su información personal.

La empresa ha puesto en práctica numerosas mejoras en la seguridad de los datos, como la incorporación y actualización de tecnologías de seguridad avanzadas, software adicional para la supervisión, pruebas para evitar la vulnerabilidad y el acceso no autorizado, mayores niveles de codificación de datos y cortafuegos adicionales.

Además, la empresa ha incorporado otra serie de medidas a la infraestructura de red, como un sistema de advertencia para la detección de patrones de actividad poco habituales, que podrían indicar un intento de acceso no autorizado a la red."

Pagina Web consultada:

http://es.playstation.com/home/news/articles/detail/item369677/%C3%9Altimas-noticias-sobre-las-interrupciones-en-el-servicio-de-PSN/

"a nivel mundial ya se están analizando acciones legales contra Sony por el incidente de seguridad". Y señaló que algunos analistas indican que "podría costarle unos 1.500 millones de dólares" a la empresa. Así, cada uno de los 77 millones de clientes en el primer ataque y cuyos datos podrían estar comprometidos, recibiría un promedio de 20 dólares

El punto es que, no hay manera, hasta el momento, de impedir que los hackers o crackers cometan delitos informáticos, pero si se pueden minimizar los riesgos de un incidente de este tipo a través de la prevención. Es por esto que se vuelve importante en la auditoria a las TIC fortalecer el enfoque a la seguridad.

Hacer más eficientes y efectivos los servicios que presta una entidad a través de las TIC no me asegura el éxito de mi gestión, Hay que implementar las medidas de seguridad necesarias en las TICs.

En una auditoria de gestión TIC se conseguirá encontrar todas aquellas vulnerabilidades que podrían impactar de forma negativa los servicios a los ciudadanos, proporcionados por las entidades gubernamentales. Una vulnerabilidad no atendida a tiempo, podría representar el no cumplimiento de los objetivos institucionales.

"Lo ideal sería, ¿que los auditores TIC de las EFS sean Hackers?", lo que en realidad se pretende dar a entender con esta interrogante es que, hay que contar con Auditores capacitados para detectar vulnerabilidades, no solo para señalar la materialización de las mismas; si no advertirlas antes de que se materialicen, y esto se puede lograr siempre y cuando las EFS estén dispuestas a invertir en el desarrollo de dichas habilidades en su personal de auditoria a través de capacitación especializada en las TIC.

Es tanta la importancia sobre el tema de seguridad que países están tomando acciones a nivel gubernamental para minimizar estos riesgos, tal es el caso de Israel:

"Israel ha creado un cibercomando gubernamental para proteger al país de ataques informáticos a sus redes clave e impulsar la competitividad de las industrias locales especializadas en seguridad tecnológica." Noticia del 18/05/2011

Pagina Web consultada: http://www.eleconomista.es/tecnologia-internet/noticias/3079685/05/11/Israel-lanza-un-cibercomando-contra-ataques-informaticos.html

3.8.2 GOBERNABILIDAD DE LAS TICS

El término " gobernabilidad " define la capacidad de una organización para controlar y regular su propio funcionamiento con el fin de evitar los conflictos de intereses relacionados con la división entre los beneficiarios y los actores.

El término " gobernabilidad " cobró popularidad debido a los incidentes en que se vieron implicados grandes grupos industriales (Enron, Swissair) donde la falta de supervisión o la confusión de los roles produjo la bancarrota de estas empresas.

La Gobernabilidad de las TIC se refiere a la administración y regulación de los sistemas de información que establece una compañía para el logro de sus objetivos. Por lo tanto, la gobernabilidad de TIC forma parte integral del control corporativo.

De esta manera en la auditoria a las TIC, se buscara examinar de qué manera los recursos informáticos adquiridos por la entidad están apoyando a sus procesos sustantivos. Así mismo determinar que tanto depende la entidad de la tecnología para operar, ya que una vez que todos los servicios y procesos se encuentran automatizados a través de las TIC, el uso de dichas tecnologías se vuelve crítico en la entidad pera el cumplimiento de sus objetivos institucionales.

Así mismo en la auditoria se deberán identificar a aquellas entidades cuyos servicios necesitan ser automatizados, para que de alguna manera los resultados de la auditoria vayan encaminados a determinar cuáles mejoras deberá implementar la entidad fiscalizada para mejorar sus procesos haciendo uso de las TIC.

3.8.3 GESTION DE SERVICIOS TIC

Las organizaciones actuales hacen inversiones importantes en recursos de tecnología de información para apoyar los procesos de negocio. El valor significativo y relevante que el uso de la información tiene para las organizaciones, determina que todos los procesos relativos a la producción, administración y uso de servicios de Tecnologías de Información (TI) deben ser óptimamente gestionados y controlados para asegurar la calidad de la información, soporte del cumplimiento de los objetivos del negocio.

Los procesos de datos e información producto de las operaciones y procesos del negocio, requieren la aplicación de técnicas y medidas de control en el marco de un sistema de gestión que garantice la prestación de los servicios y la reducción de vulnerabilidad a amenazas generadoras de riesgo que pongan en peligro la estabilidad del sistema operacional, organizacional y del sistema macro del negocio. Todo lo anterior, justifica la necesidad de optimizar los recursos de TI en apoyo y alineación con los objetivos de negocio a través de procesos efectivos de "Gestión de servicio TIC".

En las organizaciones existe una organización de TI que genera y provee los servicios de TI y un grupo de clientes internos (usuarios) y externos que demandan esos servicios y esperan su prestación oportuna y con calidad. Las relaciones y comunicaciones entre el proveedor de TI y los clientes de TI deben ser canalizadas a través de un sistema que garantice la optimación de los procesos de entrega y soporte de servicios a través de la consolidación de Gestión de Servicio TI.

Este nuevo paradigma basado en el servicio debe tener un acercamiento a las organizaciones de cualquier tamaño, las empresas deben adoptar y

adaptar estas mejores prácticas bajo un enfoque de "Calidad de Servicio" y oportunidad para el cambio del negocio con la aplicación de estándares actualizados. Este paradigma se fundamenta en el mejoramiento continuo de la Cultura de Servicio TI.

Los productos y servicios de estos marcos de referencia están orientados a la implantación de sistemas consolidados de mejoramiento continuo en la gestión de servicio de tecnología de información en alineación con los objetivos del negocio, de punta a punta desde las fases diagnostica y de planificación hasta la implantación, monitoreo, supervisión y optimación. La tendencia de Gestión de Servicio TI se basa en la promoción y soporte de aplicación de las mejores prácticas, marcos referenciales y estándares de aceptación internacional, tales como ISO/IEC 20000, ITIL, ITSCMM, COBIT, ISO/IEC -17799 – 2700X y otras.

3.8.4 VECTOR N

El vector N, serán los enfoques sobre la Gestión TIC necesarios de auditar, una nueva tendencia, riesgos en la gestión TIC, nueva tecnología desarrollada y de gran aceptación por las entidades públicas.

Así como mantener la seguridad de la información de una plataforma tecnológica hoy es prioritaria debido a las vulnerabilidades que las mismas TICs han propiciado, en un futuro no muy lejano, las TICs nos seguirán sorprendiendo con nuevas tecnologías que continuaran abonando a la evolución de la forma de vida de la sociedad, por lo tanto las EFS deben estar preparadas para auditar la tecnología del futuro.

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

De la investigación realizada tanto bibliográfica como experimental, se emiten las conclusiones y recomendaciones siguientes:

5.1 CONCLUSIONES

a. Incorporar las TICs como apoyo a los procesos sustantivos de las instituciones gubernamentales les permiten administrar con mayor eficiencia, eficacia, y economía su operatividad, lo cual repercutirá en el incremento de los beneficios de los ciudadanos y por lo tanto, es su calidad de vida.
b. Una Base de Datos con información de las plataformas tecnológicas de cada entidad sujeta a fiscalización, propicia una planeación más precisa de la auditoria, así como el integrar en el equipo de auditoria TIC, los profesionales idóneos para la ejecución de la auditoria, se convierte en una herramienta para la toma de decisiones en materia TIC, de las EFS.
c. Las mejores prácticas y estándares más utilizados para perfeccionar el desempeño, transparencia y control sobre las actividades de las TICs son ITIL, COBIT e ISO/IEC 27002.
d. El uso de estándares y mejores prácticas tales como ITIL, COBIT e ISO/IEC 27002, proporciona a las entidades que las implementan mejoras de desempeño, transparencia y control sobre actividades TIC. Además, estos estándares se constituyen en un lenguaje común que permita un mejor entendimiento entre la entidad auditada y los auditores TIC.

e. No existe entre las EFS miembros de la OLACEFS un estándar oficial para la ejecución de la Auditoria de Gestión a las TICs.
f. La Auditoría de Gestión a las Tecnologías de Información y Comunicaciones, debe ser ejecutada bajo una estrategia que permita a las EFS mantener una superioridad tecnológica sobre las entidades sujetas a fiscalización, para vigilar, controlar, regular, monitorear y actuar ante los avances de las TIC.
g. Si bien existen buenas prácticas y estándares aplicados a la administración y control de las TICs, no existe una solución integral para el desarrollo de la Auditoria de Gestión de las Tecnologías de Información y Comunicaciones.
h. La falta de desarrollo continuo del talento humano en materia TIC, limita a los auditores de las EFS para realizar auditorías de forma eficiente y efectiva a estos a estas tecnologías.
i. La especialización en áreas TIC dentro del desarrollo continuo del talento humano de los auditores es de vital importancia para que los auditores estén actualizados y sean competentes en la ejecución de la auditoria a la gestión de las TICs.
j. Aún existen EFS que no cuentan con Normativa TIC de las EFS" que establezca los criterios básicos de control que deben observarse en la gestión TIC.
k. La forma tradicional de ejecutar las auditorias ha cambiado debido a que las TICs se han integrado a la operatividad de las entidades sujetas a fiscalización, por lo tanto, auditar una gestión institucional cuyos procesos sustantivos se encuentran soportados en tecnología, requiere de métodos especializados, luego, independientemente de los tipos de auditoria que se desarrollen, estas deberán aplicar a sus procedimientos técnicas relacionadas a las TICs.

l. La Auditoría de Gestión a las Tecnologías de Información Y Comunicaciones, va más allá de un examen a los controles de los elementos de hardware y software de una plataforma tecnológica, también examina como estos elementos tecnológicos apoyan a los procesos sustantivos de las entidades gubernamentales en la consecución de sus objetivos institucionales.

5.2 RECOMENDACIONES

a. A todas las Entidades Fiscalizadoras Superior miembros de OLACEFS, se les recomienda: Tomar de modelo la propuesta de solución planteada en el capítulo tres de este documento, para realizar la Auditoría de Gestión a las Tecnologías de Información y Comunicaciones.

b. A las Entidades Fiscalizadoras Superiores y así como a las coordinadoras de las capacitaciones del Recursos Humanos de las mismas, que implementen una estructura de capacitación continua a los auditores en general, orientado a la ejecución de la Auditoría de Gestión a las Tecnologías de Información y Comunicaciones.

c. A los Altos funcionarios de las Entidades Fiscalizadoras Superiores y Unidades o Áreas que administran las Tecnologías de información en las mismas, que se rompa el paradigma de que el auditor TIC, no debe obtener capacitación especializada en áreas afines, ya que esto no abona a la consecución de los beneficios expuestos en el capítulo tres “Desarrollo del Conocimiento TIC”, en este sentido cabe mencionar un dicho popular “Para poder juzgar…hay que saber jugar”. Así cuando se examina la gestión

TIC de una entidad los auditores deben poseer el mismo nivel de conocimiento o superior al de los administradores de las TICs auditadas.

d. Que todas las Entidades Fiscalizadoras Superiores miembros de La OLACEFS elaboren la "**Normativa TIC de las EFS**" que establezca los criterios básicos de control que deben observarse en la gestión TIC.

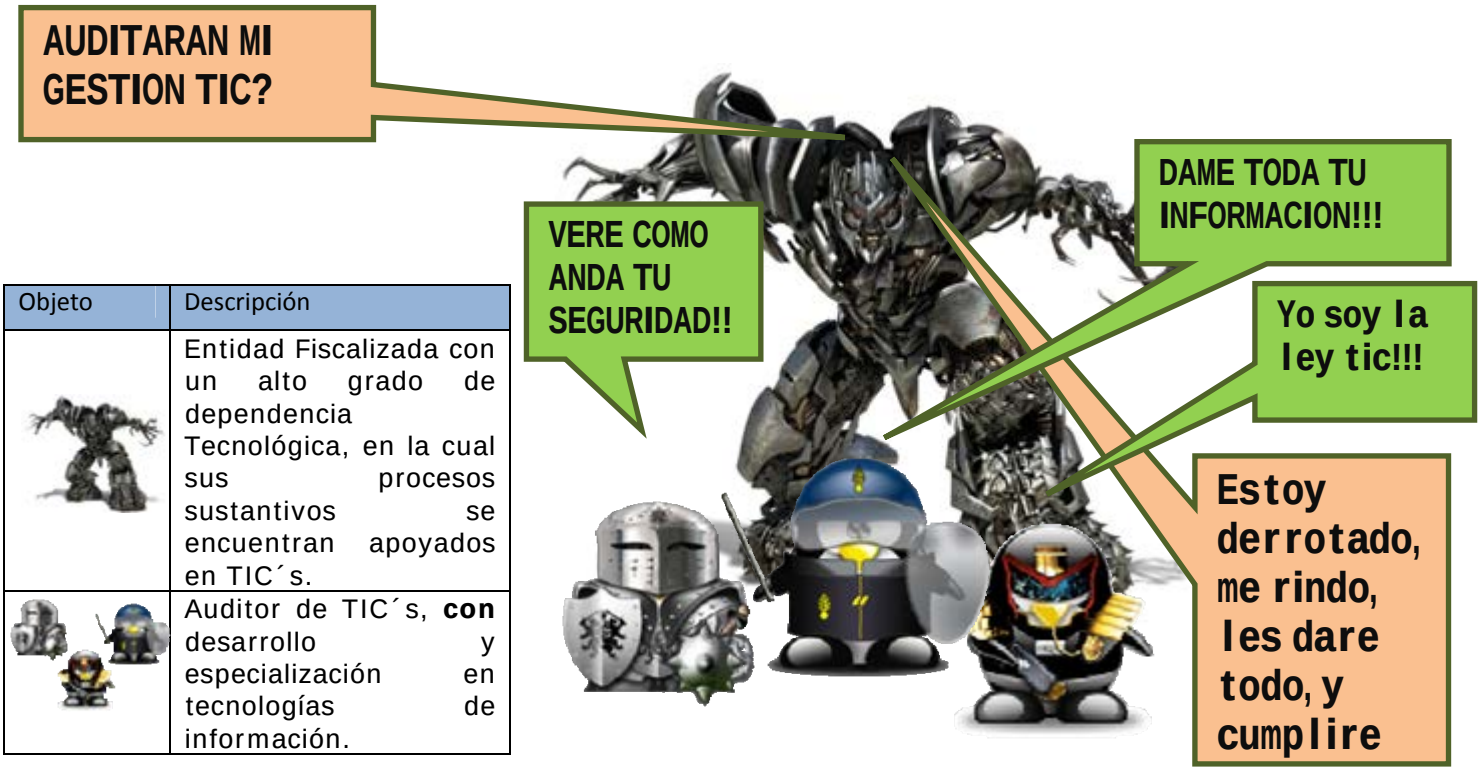
e. Se recomienda que las EFS procuren que los auditores TIC obtengan certificaciones internacionales como Auditor de Sistemas de Información (Certified Information Systems Auditor - CISA™) la cual está reconocida a nivel mundial como uno de los estándares más prestigiosos en las áreas de auditoria, control, seguridad y gobernabilidad de Sistemas de Información.

f. Se recomienda a la OLACEFS que utilice la los componentes de la Torre TIC como un instrumento de medición que le permita verificar las áreas críticas o los problemas de las EFS para efectuar Auditoria de Gestión TIC de forma más precisa.

ANTES DE LA IMPLEMENTACION DE LA TORRE TIC…

Objeto	Descripción
	Entidad Fiscalizada con un alto grado de dependencia Tecnológica, en la cual sus procesos sustantivos se encuentran apoyados en TIC´s.
	Auditor de TIC´s, **sin** desarrollo/especialización en tecnologías de información.

DESPUES DE LA IMPLEMENTACION DE LA TORRE TIC…



Objeto	Descripción
	Entidad Fiscalizada con un alto grado de dependencia Tecnológica, en la cual sus procesos sustantivos se encuentran apoyados en TIC´s.
	Auditor de TIC´s, **con** desarrollo y especialización en tecnologías de información.

BIBLIOGRAFIA

Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa.

Informe del Undécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, 18 a 25 de abril de 2005, Bangkok (Tailandia)

Avances en Tecnologías de La Información y De Las Comunicaciones Para la Seguridad y la Defensa. Centro Superior de Estudios de la Defensa Nacional, Monografías del CESEDEN No. 88.

Programación En Auditoría En Base A Riesgos, Documento Técnico n° 24 – Versión 0.3, Marzo 2006.

TICs y Buen Gobierno: La contribución de las Tecnologías de la Información y la Comunicación al Gobierno Local en América Latina, Carlos Batista**,** NP3 – Núcleo de Investigación en Políticas Públicas Universidad de Brasilia, Brasil, Enero, 2003

FUENTES DE INTERNET CONSULTADAS

http://www.microsiervos.com/archivo/ordenadores/el-primer-ordenador-del-mundo.html

http://es.wikipedia.org/wiki/Tecnologías_de_la_información_y_la_comunicación

http://reconceptualizandolaexperiencia.wordpress.com/2010/04/06/historia-de-las-tic-y-sus-impactos/

http://www.monografias.com/trabajos37/tic-en-educacion/tic-en-educacion.shtml

https://www.isaca.org/Pages/default.aspx

http://www.slideshare.net/roumi2010/importancia-de-las-tics-en-la-auditoria

http://es.playstation.com/home/news/articles/detail/item369677/%C3%9Altimas-noticias-sobre-las-interrupciones-en-el-servicio-de-PSN/

http://www.slideshare.net/dcordova923/auditoria-de-la-gestion-de-las-tic

http://tecnologia.iprofesional.com/notas/115496-Cmo-fue-el-robo-de-datos-a-Sony-y-cul-es-el-impacto-en-usuarios-argentinos

GLOSARIO

Auditor TIC: Auditor que realiza auditorías a las Tecnologías de Información y Comunicaciones.

Auditoria TIC: Auditoria realizada a las Tecnologías de Información y Comunicaciones.

Outsourcing: El outsoucing consiste en que una empresa contrata, a una agencia o firma externa especializada, para hacer algo en lo que no se especializa

Bases de datos: Una base de datos o banco de datos (en ocasiones abreviada con la sigla *BD* o con la abreviatura *b. d.*) es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

Balanced Scorecard: Es una perspectiva de la administración estratégica que traduce una visión en un grupo claro de objetivos y factores críticos del éxito, provee una estructura para gerencia de organizaciones de manera que ejecuten sus estrategias de manera rápida y confiable

Checklist: Lista de verificación o chequeo

COBIT: Control Objectives for Information and related Technology

Crackers: El término cracker (del inglés *crack*, romper) se utiliza para referirse a las personas que *rompen* algún sistema de seguridad

Ciberterrorismo: El ciberterrorismo o terrorismo electrónico es el uso de medios de tecnologías de información, comunicación, informática,

electrónica o similar con el propósito de generar terror o miedo generalizado en una población, clase dirigente o gobierno, causando con ello una violencia a la libre voluntad de las personas. Los fines pueden ser económicos, políticos o religiosos principalmente.

Hackers: El término hacker trasciende a los expertos relacionados con la informática, para también referirse a cualquier profesional que está en la cúspide de la excelencia en su profesión, ya que en la descripción más pura, un hacker es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas.

Hacking ético: es realizado por una empresa o consultor especializado en seguridad informática, con autorización de la organización a ser evaluada y con la condición que las debilidades de seguridad o vulnerabilidades encontradas serán reportadas al cliente, junto con recomendaciones para solucionarlas.

ISACA: se ha convertido en una organización global que establece las pautas para los profesionales de gobernación, control, seguridad y auditoría de información.

ITIL: La Biblioteca de Infraestructura de Tecnologías de Información.

Leguajes de desarrollo: o Un lenguaje de programación es un idioma artificial diseñado para expresar computaciones que pueden ser llevadas a cabo por máquinas como las computadoras.

Memoria ram: La **memoria de acceso aleatorio** (en inglés: *random-access memory*, cuyo acrónimo es **RAM**) es la memoria desde donde el procesador recibe las instrucciones y guarda los resultados.

Memoria USB: O también conocido como Pendrive, dispositivo de almacenamiento externo portátil que se conecta a puertos usb.

Ordenador: computadora personal, PC**.**

Paradigma: Paradigma es un modelo o patrón en cualquier disciplina científica, religiosa u otro contexto epistemológico

Plataforma tecnológica: Son los elementos de Hardware y software como servidores, estaciones de trabajo PC´s, redes con que cuenta una entidad.

PSN: PlayStation Network.

Redes: Una red de computadoras, también llamada red de ordenadores o red informática, es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos para compartir información y recursos.[1] Este término también engloba aquellos medios técnicos que permiten compartir la información**.**

Seguridad perimetral: La seguridad perimetral es un conjunto de sistemas de detección electrónica diseñados para proteger perímetros internos y externos

TAAC: técnicas de auditoría asistidas por computador

Technica Impendi Nationi: (Latín) - La tecnología impulsa a las naciones.

TIC: Las TIC se conciben como el universo de dos conjuntos, representados por las tradicionales Tecnologías de la Comunicación (TC) - constituidas principalmente por la radio, la televisión y la telefonía convencional - y por las Tecnologías de la información (TI) caracterizadas por la digitalización de las tecnologías de registros de contenidos (informática, de las comunicaciones, telemática y de las interfaces)". Pero en su sentido social y no netamente informático.

TASCOI.- Herramientas para identificar y diagnosticar sistemas y/o entes.

ANEXOS

ENCUESTA DE AUDITORÍA DE GESTIÓN A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Con el propósito de participar en el XIV Concurso Anual De Investigación 2011, sobre el Tema: "Auditoría de Gestión a las Tecnologías de Información y Comunicaciones." promovido por la Organización Latinoamericana Y Del Caribe De Entidades Fiscalizadoras Superiores (OLACEFS), solicitamos su valiosa colaboración en proporcionarnos respuesta a la siguiente encuesta.

DATOS GENERALES DEL ENCUESTADO

(Seleccione con un clic del mouse en la casilla para ingresar datos)

Entidad Fiscalizadora Superior (EFS):	
País:	
Área Organizativa:	
Cargo del funcionario que responde la encuesta:	

OBJETIVO: Recolectar información sobre la organización y dirección de las Entidades Fiscalizadoras Superiores (EFS) para la Auditoría a la Tecnologías de Información y Comunicaciones.

INDICACIONES: Marque con una "X" haciendo clic del mouse sobre la casilla y complemente según usted considere pertinente. Si es necesario marque más de una respuesta (solo para las preguntas 8 y 11). Al finalizar seleccione ***guardar*** en el menú de su procesador de texto (Microsoft Word de Office) para que sus respuestas queden almacenadas en el archivo.

1.- ¿Realiza su EFS auditorías a las Tecnologías de Información y Comunicaciones (TIC), en las entidades fiscalizadas?

☐ Si

☐ No

2.- ¿Dentro de la Estructura Organizativa de su EFS, existe un área especializada para realizar auditorías a las Tecnologías de Información y Comunicaciones (TIC) en las entidades fiscalizadas?

☐ Si
☐ No

3.- ¿Dentro del personal de la EFS, se cuenta con auditores que tengan los conocimientos y habilidades específicas en TIC?

☐ Si
☐ No

4.- Tiene definida su EFS un perfil de auditor TIC?

☐ Si
☐ No

5.- ¿Cuenta su EFS con un plan de desarrollo del talento humano sobre auditorías a las TIC?

☐ Si
☐ No

6.- ¿Tiene su EFS una base de datos con información general de las tecnologías de información y comunicaciones (TIC) que utilizan las entidades fiscalizadas de su país? (con el propósito de identificar la tendencia tecnológica: Hardware, software, aplicaciones, redes y comunicaciones, Sistemas operativos, bases de datos.)

☐ Si
☐ No

7.- ¿En su Entidad Fiscalizadora Superior (EFS), conocen sobre estándares de aceptación mundial para la administración de las Tecnologías de Información y comunicaciones?

☐ Mucho
☐ Poco
☐ Nada

8.- Si su respuesta a la pregunta anterior fue literal “mucho” o “poco” ¿Sobre qué estándares de aceptación mundial tiene conocimiento en su EFS?

☐ COSO
☐ COBIT
☐ ITIL
☐ ISO (17999/27001/27002)
☐ OTROS (mencione cuales):

9.- ¿Han recibido en su EFS algún tipo de instrucción o capacitación sobre estándares de aceptación mundial en la administración de las tecnologías de información y comunicaciones?

☐ Si
☐ No

10.- ¿Están enterados en su EFS sobre las entidades fiscalizadas, que han implementado estándares de aceptación mundial en la administración de las tecnologías de información y comunicaciones?

☐ Si
☐ No

11.- ¿Qué estándares de aceptación mundial en la administración TIC han implantado las entidades fiscalizadas del sector público en su país:

- ☐ COSO
- ☐ COBIT
- ☐ ITIL
- ☐ ISO (17999/27001/27002)
- ☐ OTROS (mencione cuales):

12.- ¿Su EFS ha emitido un marco Normativo Legal Técnico y de cumplimiento obligatorio, para la administración de las TICs en las entidades fiscalizadas?

- ☐ Si
- ☐ No

13.- ¿Cuenta la EFS con una metodología específica para el desarrollo de auditorías a las Tecnologías de información y Comunicaciones?

- ☐ Si
- ☐ No

14.- ¿En la auditoria a las tecnologías de Información y Comunicaciones, utilizan indicadores para medir la Gestión?

- ☐ Si
- ☐ No