La Salle Universidad Bolivia

AUDITORIA DE SISTEMAS

Freddy Cuarite

LA PAZ - BOLIVIA - 2012

Auditoria de Sistemas

Contenido

ANEXOS

1 Introducción

1.1 Las empresas y las Tecnologías de Información y Comunicación (TIC)

Todas las organizaciones empresariales, se encuentran inmersas en un entorno donde cada día se sufre cambios, fundamentalmente por el uso de Tecnologías de Información y de Comunicación, por lo que se encuentran expuestas a diferentes amenazas que acompañan al uso de estas nuevas tecnologías.

Este aspecto se debe a que las organizaciones empresariales, cualquiera sea su naturaleza, cuentan con un flujo de información tanto interno (dentro de la organización) como externo (puede ser a nivel local, nacional o internacional), el cual puede realizarse de forma verbal, escrita o cualquier otra, y a través de diferentes canales (aire, papel, medios electrónicos, u otros), de tal manera que esta información atraviesa diferentes fases:

- La preparación por parte del emisor (acorde a diferentes necesidades o requerimientos realiza una codificación),
- El envío a través de un canal (el cual puede contener diferentes tipos de ruido - amenazas),
- La recepción de la información (el cual deberá decodificar la misma para poder interpretarla).

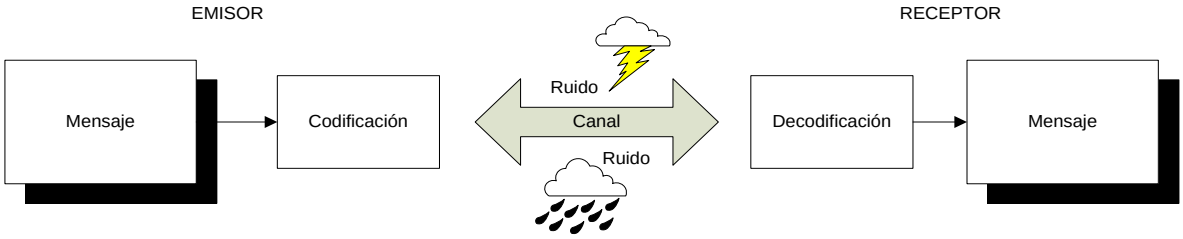

Figura 1.1
Flujo de información básica

A la organización, ante esta necesidad de manejo de información y el uso de tecnologías para que el mismo pueda fluir, se le presenta una serie de interrogantes que resolver: ¿Conozco la información que fluye interna y externamente?, ¿Cuál es el nivel de categoría de esta información?, ¿Puedo confiar en la información que se utiliza de mi organización?, ¿Los medios por los cuales fluye toda la información son confiables?, etc.

Al intentar responder estas interrogantes, posiblemente se tengan que considerar requerimientos externos como ser: el cumplimiento de leyes, relaciones con otras organizaciones, compromisos legales adquiridos, etc., asimismo, la necesidad de crear y aplicar reglas internas para el manejo de esta la información tanto a nivel interno como externo.

Debido a estas necesidades, la información tiende a crecer de manera desorganizada, lo cual es el principio para generar eventos no deseados, como ser: la pérdida de información, sanciones por entregas tardías, búsquedas de información lentas, etc., generando un caos en la información de la organización. En este sentido, al intentar solucionar estos problemas, se incorpora reglas internas, se capacita al personal con conocimientos para la gestión de los mismos y se usa Tecnología adecuada para la gestión de información y comunicación para el envío y recepción tanto a nivel interno como externo.

1.2 Las Tecnologías de Información y Comunicación (TIC)

La Tecnología de Información y Comunicación (TIC) es una de las ramas con mayor crecimiento y por tanto con mayor oferta de productos. Debido a esto, es difícil creer que existan aspectos cotidianos que no estén vinculados con las TIC. Las TIC han jugado un papel muy importante en los últimos años a nivel de las organizaciones, su correcto uso genera grandes mejoras ya que automatizan y evolucionan los procesos operativos y administran la información como un activo primordial de la empresa, buscando consolidarse como una ventaja competitiva que impulse el crecimiento empresarial.

Al observar la totalidad de los activos de una organización, nos damos cuenta que con el pasar del tiempo, existe un incremento cada vez más exponencial en la dependencia que tienen las organizaciones en dos activos en particular: las Tecnologías de Información y Comunicación (TIC) y la información propiamente dicha. Como consecuencia de este incremento, se ha disparado la utilización de las tecnologías en las organizaciones, ya que estas TIC generan un valor que en la gran mayoría de casos es ignorado por los empleados, por el desconocimiento de su funcionalidad, es decir, que su uso se ha delegado de tal manera que solo los ingenieros son los únicos en establecer cuanto, cuando y donde utilizar los recursos TIC, olvidando la relación de valor que estas brindan o podrían brindar a la organización.

Este fenómeno del desconocimiento del valor que aportan las TIC dentro de las organizaciones, se refleja específicamente en el descuido por parte de las autoridades administrativas frente a la desmesurada inversión en TIC y en la adopción de una actitud mecanicista y limitada frente al uso de las mismas por parte de sus usuarios directos.

Es así como, las organizaciones ven en el área de TIC un apoyo estratégico para cumplir las metas propuestas, en algunas ocasiones este apoyo puede no se ser el esperado por la organización, debido a deficiencias que puedan existir entre los objetivos corporativos con los objetivos y procedimientos que realiza el área de TIC y justificar las grandes inversiones que se hace hoy en día en recursos de tecnologías de información.

De acuerdo a lo anterior, es importante resaltar que en la actualidad el área de TIC debe procurar optimizar, controlar y asegurar la disponibilidad de la información para soportar y cumplir los objetivos del negocio, y de otro lado, deben evidenciar que haya un buen retorno de la inversión, pero ¿Cómo nos aseguramos que las inversiones hechas en TIC aportan a esas metas que los ejecutivos esperan alcanzar?, ¿Cómo se está encaminando el área de TIC hacia la misma línea que sigue la organización?.

Como parte de la solución a este fenómeno, se debería realizar un alineamiento de los objetivos y estrategias del área de TIC a los objetivos y estrategias corporativas, el cual debe arrojar resultados medibles e interpretables para las autoridades administrativas y permitan observar de esta manera el valor que las TIC generan al negocio, los riesgos que se asumen al realizar inversiones en TIC y determinar cuál es el impacto que estas tienen dentro de los procesos de negocio que apoyan, de este planteamiento surge el concepto de gobierno TIC, el cual hace parte integral del gobierno corporativo, y ayuda a dirigir y controlar este alineamiento del departamento de TIC con la organización; es definido como: el liderazgo, los procesos y las estructuras que aseguran que las tecnologías de información de la organización apoyan los objetivos y estrategias de la misma, logrando con esto ilustrar por medio de modelos racionales de gestión, ese aporte de valor.

Es así como en este nuevo contexto, aparecen diferentes marcos de trabajo como COBIT, ITIL e ISO, que plantean llevar a cabo actividades de gestión de procesos, control de objetivos de procesos y buenas prácticas para la gestión de servicios TIC.

En síntesis, las TICs, tienen un rol muy importante dentro de la gestión empresarial, ya que son herramientas que se integran a los procesos organizacionales y ayudan a las empresas a operar con mayor calidad y eficiencia, lo cual les permite obtener ventajas competitivas en los segmentos de mercados donde la empresa participa.

2 La Información y los Sistemas de Información

Como se vio anteriormente, uno de los aspectos más importantes de cualquier organización es la gestión de la información, para este propósito debemos comprender a que específicamente nos referimos con dato, información y conocimiento; en este sentido, se presenta los conceptos básicos aplicados.

2.1 Conceptos aplicados sobre información

Los términos: datos, información y conocimiento suelen utilizarse indistintamente y esto puede llevar a una interpretación errónea de cada uno de ellos. Es importante diferenciar que los **datos** están localizados en nuestro alrededor y el **conocimiento** está se ubica en agentes de cualquier tipo (personas, empresas, máquinas), mientras que la **información** adopta un papel mediador entre ambos.

Figura 2.1
Pirámide al conocimiento

2.1.1 Dato

Dato es cualquier cosa real o abstracta que tiene una representación simbólica (numérica, alfabética, sonido, imagen, etc.). Un dato no tiene valor semántico (sentido) en sí mismo, y se corresponden con elementos primarios de información que por sí solos son irrelevantes como apoyo a la toma de decisiones.

Un número telefónico o un nombre de una persona, por ejemplo, son datos que, sin un propósito, una utilidad o un contexto no sirven como base para apoyar la toma de una decisión. Los datos pueden ser una colección de hechos almacenados en algún lugar físico como un papel, un dispositivo electrónico (CD, DVD, disco duro), o la mente de una persona. En este sentido las tecnologías de la información han aportado mucho a recopilación de datos.

Entonces, los datos pueden provenir de fuentes externas o internas a la organización, pudiendo ser de carácter objetivo o subjetivo, o de tipo cualitativo o cuantitativo, etc.

Las organizaciones actuales normalmente almacenan datos mediante el uso de tecnologías. Todas las organizaciones necesitan datos y algunos sectores son totalmente dependientes de ellos. Bancos y otras Instituciones Financieras, compañías de seguros, instituciones gubernamentales y de Seguridad Social son ejemplos obvios. En este tipo de organizaciones la buena gestión de los datos es esencial para su funcionamiento, ya que operan con millones de transacciones diarias. Pero en general, para la mayoría de las empresas tener muchos datos no siempre es bueno. Las organizaciones almacenan datos sin sentido. Realmente esta actitud no tiene sentido por dos razones: la primera es que demasiados datos hacen más complicado identificar aquellos que son relevantes; segundo, y todavía más importante, es que los datos no tienen significado en sí mismos.

Los datos describen únicamente una parte de lo que pasa en la realidad y no proporcionan juicios de valor o interpretaciones, y por lo tanto no son orientativos para la acción. La toma de decisiones se basará en datos, pero estos no nos dirán que hacer. Los datos no dicen nada acerca de lo que es importante o no. A pesar de todo, los datos son importantes para las organizaciones, ya que son la base para la creación de información.

2.1.2 Información

La información es un conjunto organizado de datos, y que tienen un significado (relevancia, propósito y contexto), y que por lo tanto son de utilidad para quién debe tomar decisiones, al disminuir su incertidumbre. Los datos se pueden transforman en información añadiéndoles valor:

- **Contexto:** se sabe en qué contexto y para qué propósito se generaron.
- **Categoría:** se conocen las unidades de medida que ayudan a interpretarlos.
- **Calculo:** los datos pueden haber sido procesados matemática o estadísticamente.
- **Corrigiendo:** se han eliminado errores e inconsistencias de los datos.
- **Condensando:** los datos se han podido resumir de forma más concisa (agregación).

Por tanto, la información es la comunicación de conocimientos o inteligencia, y es capaz de cambiar la forma en que el receptor percibe algo, impactando sobre sus juicios de valor y sus comportamientos.

Información = Datos + Contexto (añadir valor) + Utilidad (disminuir la incertidumbre)

Recordamos que un mensaje, normalmente bajo la forma de un documento o algún tipo de comunicación audible o visible tiene un emisor y un receptor. La información es capaz de cambiar la forma en que el receptor percibe algo, es capaz de impactar sobre

sus juicios de valor y comportamientos. Tiene que informar; marcan la diferencia. La palabra “informar” significa originalmente “dar forma a“, y la información es capaz de formar a la persona que la consigue, proporcionando ciertas diferencias en su interior o exterior. Por lo tanto, estrictamente hablando, es el receptor, y no el emisor, el que decide si el mensaje que ha recibido es realmente información, es decir, si realmente le informa. Un informe lleno de tablas inconexas, puede ser considerado información por el que lo escribe, pero a su vez puede ser juzgado como “ruido” por el que lo recibe.

La información se mueve en torno a las organizaciones a través de redes formales e informales. Las redes formales tienen una infraestructura visible y definida: cables, buzones de correo electrónico, direcciones. Los mensajes que estas redes proporcionan incluyen correo electrónico, servicio de entrega de paquetes, y transmisiones a través de Internet. Las redes informales son invisibles. Se hacen a medida.

A diferencia de los datos, la información tiene significado (relevancia y propósito). No sólo puede formar potencialmente al que la recibe, sino que está organizada para algún propósito. Los datos se convierten en información cuando su creador les añade significado.

Las computadoras nos pueden ayudar a añadir valor y transformar datos en información, pero es muy difícil que nos puedan ayudar a analizar el contexto de dicha información. Un problema muy común es confundir la información (o el conocimiento) con la tecnología que la soporta. Desde la televisión a Internet, es importante tener en cuenta que el medio no es el mensaje. Lo que se intercambia es más importante que el medio que se usa para hacerlo. Muchas veces se comenta que tener un teléfono no garantiza mantener conversaciones brillantes. En definitiva, que actualmente tengamos acceso a más tecnologías de la información no implica que hayamos mejorado nuestro nivel de información.

2.1.3 Conocimiento

El conocimiento es una mezcla de experiencia, valores, información y *know-how* que sirve como marco para la incorporación de nuevas experiencias e información, y es útil para la acción. Se origina y aplica en la mente de los conocedores. En las organizaciones con frecuencia no sólo se encuentra dentro de documentos o almacenes de datos, sino que también está en rutinas organizativas, procesos, prácticas, y normas.

El conocimiento se deriva de la información, así como la información se deriva de los datos. Para que la información se convierta en conocimiento es necesario realizar acciones como:

- Comparación con otros elementos.
- Predicción de consecuencias.
- Búsqueda de conexiones.
- Conversación con otros portadores de conocimiento.

Así, es habitual describir los significados de las palabras "dato", "información" y "conocimiento" para evidenciar que es necesario un proceso de transformación de uno a otro, y que mediante estas transformaciones la información numérica va ganando valor (dinero). Y el uso de nuevas tecnologías para automatizar la transformación del dato en conocimiento es útil para la gestión empresarial.

Como ejemplo podemos decir que "5000" es sólo un dato, y cuando lo contextualizamos y decimos que son "Bs 5000.- vendidos durante un mes" lo hemos transformado en información, y se convierte finalmente en conocimiento cuando lo comparamos con los meses anteriores, y con la evolución de otros productos y mercados, y nos sirve para mejorar nuestro negocio de alguna manera.

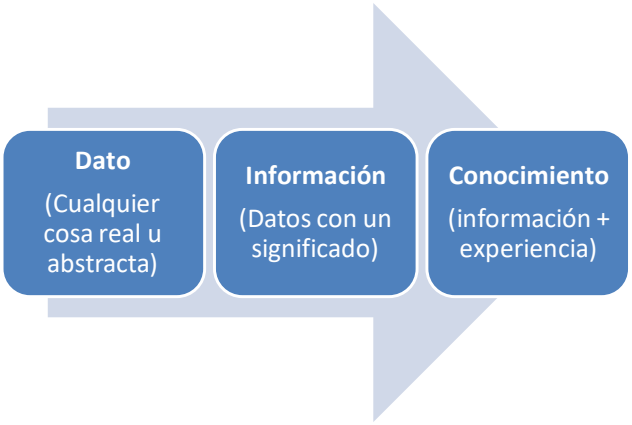

Figura 2.2
Del dato al conocimiento

La mayoría de la gente tiene la sensación intuitiva de que el conocimiento es algo más amplio, más profundo y más rico que los datos y la información.

Lo que inmediatamente deja claro la definición es que ese conocimiento no es simple. Es una mezcla de varios elementos; es un flujo al mismo tiempo que tiene una estructura formalizada; es intuitivo y difícil de captar en palabras o de entender plenamente de forma lógica. El conocimiento existe dentro de las personas, como parte de la complejidad humana y de nuestra impredecibilidad. Aunque solemos pensar en activos definibles y concretos, los activos de conocimiento son mucho más difíciles de manejar.

2.2 Los Sistemas de Información

Ahora que se aclaró lo que es información, podemos adicionar el concepto de sistema, para poder comprender que es un sistema de información.

2.2.1 Sistema

Un sistema es un conjunto estructurado de elementos interrelacionados entre sí organizados con el fin de lograr objetivos. Cualquier cambio o variación de cualquiera de los elementos puede determinar cambios en todo el sistema.

Entonces, un sistema es un todo, cuyas partes o componentes están relacionadas de tal modo que el objeto se comporta en ciertos aspectos como una unidad y no como un mero conjunto de elementos.

El ser humano, por ejemplo, es un sistema que consta de un número de órganos y miembros, y solamente cuando estos funcionan de modo coordinado el hombre es eficaz. Similarmente, se puede pensar que la organización es un sistema que consta de un número de partes que interrelacionan entre sí. Por ejemplo, una firma manufacturera tiene una sección dedicada a la producción, otra dedicada a las ventas, una tercera dedicada a las finanzas y otras varias. Ninguna de ellas es más que las otras, en sí. Pero cuando la firma tiene todas esas secciones y son adecuadamente coordinadas, se puede esperar que funcionen eficazmente y logren las utilidades.

2.2.2 Sistema de información

Un sistema de información es un conjunto de elementos interrelacionados entre sí orientados al tratamiento y administración de datos e información, organizados y listos para su posterior uso, generados para cubrir una necesidad (objetivo). Dichos elementos formarán parte de alguna de estas categorías:

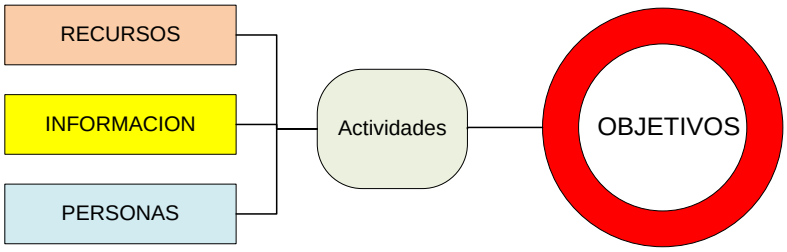

Figura 2.3
Sistemas de información

Todos estos elementos (personas, datos, actividades o técnicas de trabajo y recursos materiales en general) interactúan entre sí para procesar los datos (incluyendo procesos manuales y automáticos) dando lugar a información más elaborada y

distribuyéndola de la manera más adecuada posible en una determinada organización en función de sus objetivos.

Normalmente el término es usado de manera errónea como sinónimo de sistema de información informático, en parte porque en la mayoría de los casos los recursos materiales de un sistema de información están constituidos casi en su totalidad por sistemas informáticos, pero siendo estrictos, un sistema de información no tiene por qué disponer de dichos recursos (aunque en la práctica esto no suela ocurrir). Se podría decir entonces que los sistemas de información informáticos son una subclase o un subconjunto de los sistemas de información en general.

2.2.3 Sistema de información informático

El término **Sistemas de Información** hace referencia a un concepto genérico que tiene diferentes significados según el campo del conocimiento al que se aplique dicho concepto, en informática, un sistema de información es cualquier sistema o subsistema de comunicaciones o computacional interconectados y que se utilicen para obtener, almacenar, manipular, administrar, mover, controlar, desplegar, intercambiar, transmitir o recibir voz y/o datos, e incluye tanto los programas de computación ("software" y "firmware") como el equipo de cómputo.

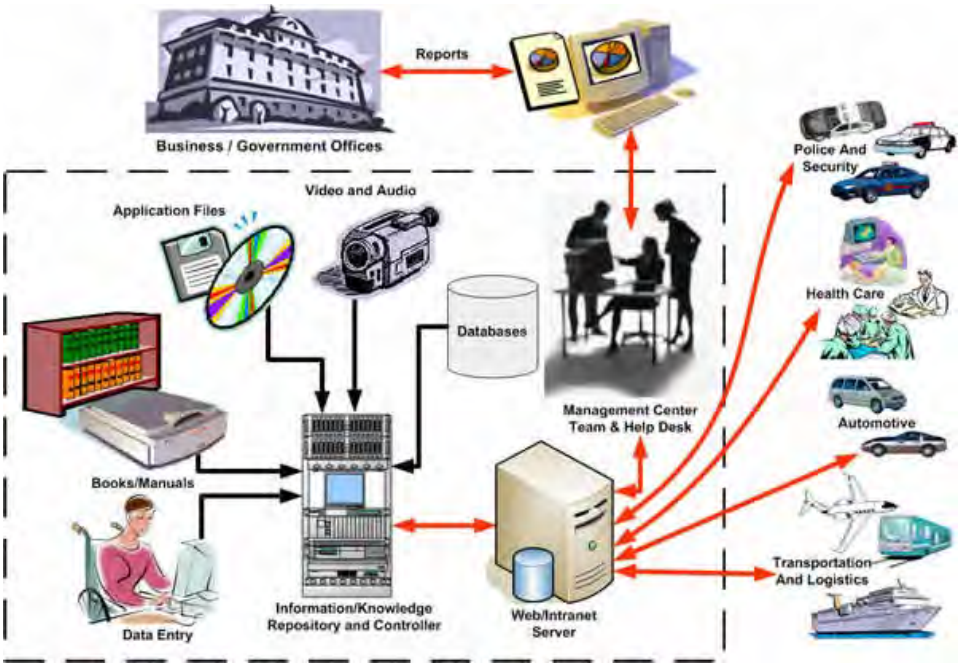

Figura 2.4
Sistema de Información Informático

2.2.4 Tipos de sistemas de información (SI)

Una clasificación bastante aplicable corresponde al punto de vista empresarial, el cual se basa en la jerarquía de una organización y se llama el modelo de la pirámide.

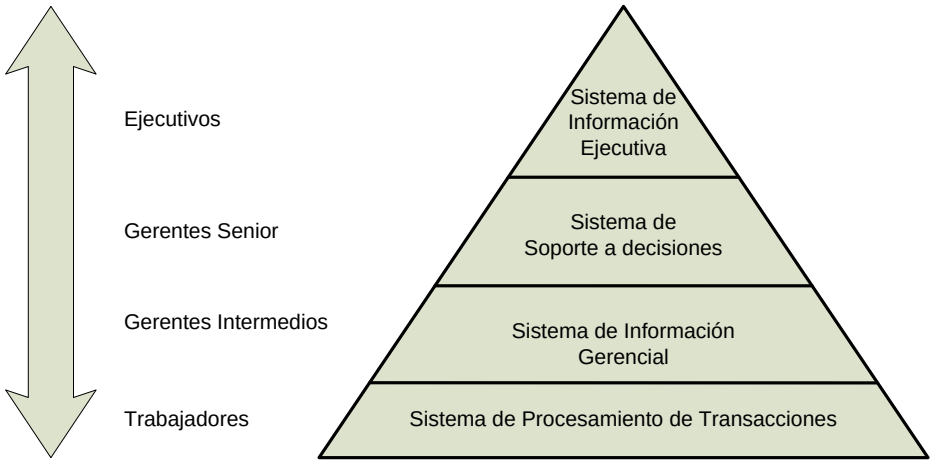

Figura 2.5
Modelo pirámide

Según la función a la que vayan destinados o el tipo de usuario final del mismo, los SI pueden clasificarse en:

- Sistema de procesamiento de transacciones (**TPS**).- Gestiona la información referente a las transacciones producidas en una empresa u organización.
- Sistemas de información gerencial (**MIS**).- Orientados a solucionar problemas empresariales en general.
- Sistemas de soporte a decisiones (**DSS**).- Herramienta para realizar el análisis de las diferentes variables de negocio con la finalidad de apoyar el proceso de toma de decisiones.
- Sistemas de información ejecutiva (**EIS**).- Herramienta orientada a usuarios de nivel gerencial, que permite monitorizar el estado de las variables de un área o unidad de la empresa a partir de información interna y externa a la misma.

Otra clasificación se ve de acuerdo al entorno de aplicación:

- Entorno transaccional: Una transacción es un suceso o evento que crea/modifica los datos. El procesamiento de transacciones consiste en captar, manipular y almacenar los datos, y también, en la preparación de documentos; en el entorno transaccional, por tanto, lo importante es qué datos se modifican y cómo, una vez que ha terminado la transacción. Los **TPS** son los SI típicos que se pueden encontrar en este entorno.

- Entorno decisional: Este es el entorno en el que tiene lugar la toma de decisiones; en una empresa, las decisiones se toman a todos los niveles y en todas las áreas (otra cosa es si esas decisiones son estructuradas o no), por lo que todos los SI de la organización deben estar preparados para asistir en esta tarea, aunque típicamente, son los **DSS** los que se encargan de esta función. Si el único SI de una compañía preparado para ayudar a la toma de decisiones es el **DSS**, éste debe estar adaptado a todos los niveles jerárquicos de la empresa.

2.3 Ciclo de vida de los Sistemas de Información

El desarrollo de sistemas se realiza a través de un ciclo de vida de desarrollo de sistemas, en el cual se aplican diferentes métodos de desarrollo que pueden ser entre otros: el análisis estructurado, la construcción de prototipos de sistemas, y el desarrollo orientado a objetos. Cada una de estas estrategias tiene un uso amplio en cada una de los diversos tipos de empresas que existen, y resultan efectivas si son aplicadas de manera adecuada.

El método de ciclo de vida para el desarrollo de sistemas es el conjunto de actividades que los analistas, diseñadores y usuarios realizan para desarrollar e implantar un sistema de información. El método del ciclo de vida para el desarrollo de sistemas consta de 6 fases:

1) Investigación Preliminar: La solicitud para recibir ayuda de un sistema de información puede originarse por varias razones: sin importar cuales sean estas, el proceso se inicia siempre con la petición de una persona.

2) Determinación de los requerimientos del sistema: El aspecto fundamental del análisis de sistemas es comprender todas las facetas importantes de la parte de la empresa que se encuentra bajo estudio. Los analistas, al trabajar con los empleados y administradores, deben estudiar los procesos de una empresa para dar respuesta a las siguientes preguntas clave:

- ¿Qué es lo que hace?
- ¿Cómo se hace?
- ¿Con que frecuencia se presenta?
- ¿Qué tan grande es el volumen de transacciones o decisiones?
- ¿Cuál es el grado de eficiencia con el que se efectúan las tareas?
- ¿Existe algún problema? ¿Qué tan serio es? ¿Cuál es la causa que lo origina?

3) Diseño del sistema: El diseño de un sistema de información produce los detalles que establecen la forma en la que el sistema cumplirá con los requerimientos identificados durante la fase de análisis. Los especialistas en sistemas se refieren, con

frecuencia, a esta etapa como diseño lógico en contraste con la del desarrollo del software, a la que denominan diseño físico.

4) Desarrollo del software: Los encargados de desarrollar software pueden instalar software comprobando a terceros o escribir programas diseñados a la medida del solicitante. La elección depende del costo de cada alternativa, del tiempo disponible para escribir el software y de la disponibilidad de los programadores.

Por lo general, los programadores que trabajan en las grandes organizaciones pertenecen a un grupo permanente de profesionales.

5) Prueba de sistemas: Durante la prueba de sistemas, el sistema se emplea de manera experimental para asegurarse de que el software no tenga fallas, es decir, que funciona de acuerdo con las especificaciones y en la forma en que los usuarios esperan que lo haga.

Se alimentan como entradas conjunto de datos de prueba para su procesamiento y después se examinan los resultados.

6) Implantación y evaluación: La implantación es el proceso de verificar e instalar nuevo equipo, entrenar a los usuarios, instalar la aplicación y construir todos los archivos de datos necesarios para utilizarla. Una vez instaladas, las aplicaciones se emplean durante muchos años. Sin embargo, las organizaciones y los usuarios cambian con el paso del tiempo, incluso el ambiente es diferente con el paso de las semanas y los meses.

Por consiguiente, es indudable que debe darse mantenimiento a las aplicaciones. La evaluación de un sistema se lleva a cabo para identificar puntos débiles y fuertes. La evaluación ocurre a lo largo de cualquiera de las siguientes dimensiones:

- **Evaluación operacional:** Valoración de la forma en que funciona el sistema, incluyendo su facilidad de uso, tiempo de respuesta, lo adecuado de los formatos de información, confiabilidad global y nivel de utilización.
- **Impacto organizacional:** Identificación y medición de los beneficios para la organización en áreas tales como finanzas, eficiencia operacional e impacto competitivo. También se incluye el impacto sobre el flujo de información externo e interno.
- **Opinión de los administradores:** evaluación de las actividades de directivos y administradores dentro de la organización así como de los usuarios finales.
- **Desempeño del desarrollo:** La evaluación de proceso de desarrollo de acuerdo con criterios tales como tiempo y esfuerzo de desarrollo, concuerdan con presupuestos y estándares, y otros criterios de administración de proyectos.

También se incluye la valoración de los métodos y herramientas utilizados en el desarrollo.

El desarrollo de los sistemas de información es bastante similar al desarrollo de proyectos en general, los cuales requieren que cada una de las fases deba ser documentada. Mucha de esta documentación puede ser particular de acuerdo a las políticas, procedimientos y estándares de desarrollo de cada organización, sin embargo, existe documentación básica que permite el desarrollo y el mantenimiento de los sistemas de información, así como también para una evaluación más efectiva por parte de auditoria; esta documentación es resultado de la aplicación de una metodología de desarrollo que abarque los siguientes elementos:

- **Marco conceptual**: tiene la misión de proporcionar las bases conceptuales mínimas que faciliten su entendimiento y que faciliten la comunicación entre los diferentes actores involucrados en el proceso de desarrollo, mantenimiento e interpretación.

  Ejemplos de documentación generada: Diseño conceptual, Diagrama de flujo de datos de Nivel 1.

- **Marco instrumental**: es responsable de proveer los instrumentos de análisis y de diseño, es decir, es aquella parte de la metodología que, precisamente, a veces se ha confundido con un algoritmo.

  Ejemplos de documentación generada: Modelo entidad relación de la base de datos, Diccionario de datos, Diagrama de estados, Diseño lógico y físico de la base de datos.

- **Marco procedimental**: establece las fases y los procedimientos básicos, señalando sus objetivos, así mismo identifica y describe los productos que deben obtenerse de cada fase, incluido el producto final.

  Ejemplos de documentación generada: Como resultado de aplicar la fase de desarrollo del software se puede generar una Guía o manual de usuario, una Guía o manual de administración del sistema, etc.

2.4 Bases de Datos

Las bases de datos son el método preferido para el almacenamiento estructurado de datos. Desde las grandes aplicaciones multiusuario, hasta los teléfonos móviles y las agendas electrónicas utilizan tecnología de bases de datos para asegurar la integridad de los datos y facilitar la labor tanto de usuarios como de los programadores que las desarrollaron.

Una base de datos es un “almacén” que nos permite guardar grandes cantidades de información de forma organizada para que luego podamos encontrar y utilizar fácilmente.

Desde el punto de vista informático, la base de datos es un sistema formado por un conjunto de datos almacenados en discos que permiten el acceso directo a ellos y un conjunto de programas que manipulen ese conjunto de datos.

Cada base de datos se compone de una o más tablas que guarda un conjunto de datos. Cada tabla tiene una o más **columnas** y **filas**. Las columnas guardan una parte de la información sobre cada elemento que queramos guardar en la tabla, cada fila de la tabla conforma un registro.

Entonces, se define una base de datos como una serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de una empresa o negocio en particular.

Características

Entre las principales características de los sistemas de base de datos podemos mencionar:

- Independencia lógica y física de los datos.
- Redundancia mínima.
- Acceso concurrente por parte de múltiples usuarios.
- Integridad de los datos.
- Consultas complejas optimizadas.
- Seguridad de acceso y auditoría.
- Respaldo y recuperación.
- Acceso a través de lenguajes de programación estándar.

3 Auditoría y Auditoría de TIC

3.1 Auditoria

La evolución de la función de auditoría ha sido continua a lo largo de estos últimos años, caracterizada por el progresivo aumento de atribuciones y responsabilidades, con el objetivo fundamental de servir cada vez mejor a la dirección de las empresas, como instrumento que asegure la eficiencia de su gestión.

Ha sido preciso recorrer un largo camino desde el inicio de la auditoría, como una rama de la contabilidad, a la que se creía vinculada, hasta el momento actual, en que constituye toda una especialidad de la administración y gestión de la empresa. Al principio la finalidad de la función auditoría era simplemente revisar la situación económica – financiera de la empresa, buscando posibles fraudes o errores y asegurando la aplicación correcta de las normas contables, sin embargo, en los años previos a la segunda guerra mundial, los hombres de empresa tomaron conciencia de que se hacía necesario, implantar en ellas un sistema de control independiente de la estructura jerárquica y operativa, aduciendo para ello razones como:

- La creciente complejidad de los fenómenos económicos y la dinámica cambiante de los métodos y sistemas de administración y gestión de empresas.
- La dimensión de las empresas, que obligaba a los directores a dedicar su atención a los problemas más importantes, por carecer de tiempo y posibilidades físicas para gestionar y examinar de cerca todas las actividades de la compañía.
- La multiplicación de la delegación de funciones, poderes y alejamiento de las empresas filiales de sus empresas matrices.
- La evolución de las comunicaciones a escala mundial.

De esta manera la auditoria fue evolucionando, estableciendo diferentes definiciones de Auditoría:

1. Un proceso sistemático independiente que consiste en obtener y evaluar objetivamente evidencia sobre las afirmaciones relativas a los actos y eventos de carácter económico expuestos en información cuantificable, con el fin de determinar el grado de correspondencia entre esas afirmaciones y los criterios establecidos, para luego comunicar los resultados a las personas interesadas.
   La auditoria es la recopilación y evaluación de datos sobre información cuantificable de una entidad económica para determinar e informar sobre el grado de correspondencia entre la información y los criterios establecidos. La auditoria debe ser realizada por una persona competente e independiente. (Alvin A. Arens)

2. Una sistemática evaluación de las diversas operaciones y controles de una organización, para determinar si se siguen políticas y procedimientos aceptados, si

se siguen las normas establecidas, si se utilizan los recursos eficientemente y si se han alcanzado los objetivos de la organización.

3. Un proceso sistemático para obtener y evaluar de manera objetiva, las evidencias relacionadas con informes sobre actividades económicas y otras situaciones que tienen una relación directa con las actividades que se desarrollan en una entidad pública o privada. El fin del proceso consiste en determinar el grado de precisión del contenido informativo con las evidencias que le dieron origen, así como determinar si dichos informes se han elaborado observando principios establecidos para el caso.

De esta última definición analizamos algunas particularidades importantes para saber que la auditoría es un proceso que reúne varias características, que son indispensables para una ejecución completa y correcta.

- Es un ***proceso sistemático***, esto quiere decir que en toda auditoría debe existir un conjunto de procedimientos lógicos y organizados que el auditor debe cumplir para la recopilación de la información que necesita para emitir su opinión final. Sin embargo cabe destacar que estos procedimientos varían de acuerdo a las características que reúna cada empresa, pero esto no significa, que el auditor no deba dar cumplimiento a los estándares generales establecidos por la profesión.
- También en esta definición se indica que la evidencia se obtiene y evalúa de ***manera objetiva***, esto quiere decir que el auditor debe realizar su trabajo con una actitud de independencia neutral frente a su trabajo.
- La ***evidencia*** que debe obtener el auditor consiste en una amplia gama de información y datos que lo puedan ayudar a elaborar su informe final. Esta definición no es estricta en cuanto a la naturaleza de la evidencia que se ha revisado, más bien nos indica que el auditor debe usar su criterio profesional para saber cual de toda la evidencia que posee es la apropiada para el trabajo que está ejecutando, él debe considerar cualquier elemento o dato que le permita realizar una evaluación objetiva y expresar un dictamen profesional.
- Los informes a los cuales hace mención la definición, no solo se refiere a las actividades económicas, es decir, informes financieros de la empresa, sino que también al ser una definición general se puede aplicar criterio profesional para poder relacionarlo con otras actividades de interés personal.
- El auditor tiene un papel que desarrollar en este proceso, el cual es, determinar el ***grado de precisión*** que existe entre los hechos que ocurren en realidad y los informes que se han elaborado después de haber sucedido tales hechos.
- El auditor debe realizar una evaluación y un informe de los acontecimientos revisados, para ello debe acogerse a ***principios establecidos***. El auditor debe conocer claramente los principios aplicados en cada informe que emita, también

debe tener la capacidad suficiente para determinar que dichos principios han sido aplicados de manera correcta en cada situación. Lo más común es que el auditor realice su trabajo de acuerdo a los principios de contabilidad generalmente aceptados (*PCGA*), en la actualidad se aplica las Normas Internacionales de Información Financiera (NIIF), sin embargo, en algunas ocasiones los principios apropiados son algunas leyes, reglamentos, convenios contractuales, manuales de procedimientos y otras disposiciones establecidas por la autoridad competente en el tema.

Figura 3.1
Ciclo inicial de la auditoria

Si visualizamos la figura podríamos decir que la auditoría es un proceso a través del cual un sujeto (auditor) lleva a cabo la revisión de un objeto (situación auditada), con el fin de emitir una opinión acerca de su razonabilidad (o fidelidad), sobre la base de un patrón o estándar establecido.

Sujeto; es el auditor que realiza la revisión del objeto bajo examen, que puede ser una cuenta contable determinada, un departamento en forma completa, un procedimiento, etcétera.

Objeto; es la situación auditada, esta puede ser muy diversa, ya que en algunos casos se da que sea una empresa en forma completa y en otros, solo se realiza esta revisión a una situación precisa.

Estándar; es el punto de comparación que tiene el auditor, para poder evaluar si la situación bajo examen cumple o no, con un determinado patrón establecido con anterioridad a la ocurrencia de la situación. Este estándar puede ser por ejemplo, principios de contabilidad generalmente aceptados, normas de auditorías, ley de impuestos, manuales de procedimiento, en otras palabras cualquier documento que nos permita apoyar el dictamen final del auditor.

Es así, que debido al vertiginoso desarrollo tecnológico y globalización de los negocios, ha llevado a que el proceso de la auditoria deba reorientarse dentro de la perspectiva del ámbito tecnológico. No basta la evaluación de la auditoría financiera, es decir los riesgos relacionados a las tecnologías de información y comunicación se han incrementado tanto que requiere una particular atención para que se logre la confiabilidad deseada. Hoy, sin lugar a dudas, es cada vez más significativo la necesidad de que el contexto tecnológico de la empresa sea auditada por especialistas, en pro de los objetivos institucionales.

3.2 Auditoria de Tecnologías de Información y Comunicación (TIC)

Una vez establecidos los conceptos de información, sistemas de información y auditoria, se puede establecer el marco de trabajo para realizar una auditoría de Tecnologías de Información y a su vez como el Auditor Financiero puedo explotar los conceptos y herramientas tecnológicas vigentes.

Para este fin, partamos de lo que diferentes autores entienden por Auditoria de Tecnologías de información o Auditoria de Sistemas o Auditoria Informática:

- Un conjunto de procedimientos y técnicas para evaluar y controlar total o parcialmente un sistema informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existente en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente.
- Proceso formal llevado adelante por especialistas en auditoría y en informática a efectos de verificar y asegurar que los recursos y procesos involucrados en la construcción y explotación de los sistemas de información cumplen con los procedimientos establecidos y se ajustan a criterios de integridad, eficiencia, seguridad, efectividad y legalidad.
- La auditoría en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.
- La auditoria de informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo los fines de la organización y utiliza eficientemente los recursos

Por otra parte, instituciones relevantes plantean las siguientes definiciones:

- La auditoria de sistemas es aquel "*examen profesional, objetivo, fundamentado e imparcial de las políticas, normas, prácticas y procedimientos que una entidad establece para la administración de sus recursos tecnológicos, en pro de disponer de información confiable, oportuna, de calidad y segura con la finalidad de lograr una gestión eficaz, eficiente y económica*". (Contraloría General de la República de Chile).
- La Contraloría General del Estado Plurinacional de Bolivia define que "*La Auditoría de Tecnologías de la Información y la Comunicación es el examen objetivo, crítico, metodológico y selectivo de evidencia relacionada con políticas, prácticas, procesos y procedimientos en materia de Tecnologías de la Información y la Comunicación, para expresar una opinión independiente respecto:*
  - *A la confidencialidad, integridad, disponibilidad y confiabilidad de la información.*
  - *Al uso eficaz de los recursos tecnológicos.*
  - *A la efectividad del sistema de control interno asociado a las Tecnologías de la Información y la Comunicación.*"

De estas definiciones extractamos aspectos particulares para comprender de forma general lo siguiente:

- La función es realizada por un profesional.
- La función consiste en la revisión de la seguridad y control de los sistemas de información en una organización, mediante una metodología de trabajo.
- Es un proceso de evaluación independiente y objetiva que asegura que la información ha sido procesada en una manera segura e integra.
- Que las operaciones son eficientes, efectivas y adecuadas; y si se salvaguarda la información.
- Es un examen y validación de los controles y procedimientos utilizados por el área de informática, a fin de verificar que los objetivos de continuidad de servicio, seguridad de la información y coherencia de la información se estén cumpliendo satisfactoriamente y de acuerdo a la normativa vigente (interna y externa).
- Evalúa y comprueba los controles y procedimientos informáticos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoría, incluyendo el uso de software.
- Determina el grado de cumplimiento y eficacia de:
  - La planificación, el desarrollo y la implantación de los sistemas utilizados.
  - La información producida por los sistemas y su pertinencia y confiabilidad.
  - La documentación básica de cada sistema, su implantación y la divulgación de la misma entre los usuarios.
  - Los mecanismos de control incorporados en los sistemas.
  - Los recursos idóneos identificados y disponibles para garantizar la continuidad de las operaciones en caso de desastres.

- El programa de adiestramiento al personal de sistemas de información, sus usuarios y los auditores.

Entonces, se entiende por Auditoría de TIC como “un examen profesional, objetivo, metodológico, sistemático y selectivo de evidencia relacionada con políticas, prácticas, procesos y procedimientos en materia de Tecnologías de la Información y la Comunicación (TIC), para expresar una opinión respecto a la confidencialidad, integridad y disponibilidad de la información, al uso eficaz de los recursos tecnológicos, y a la efectividad del sistema de control interno asociado a las TIC”.

Por lo tanto la auditoría de TIC debe analizar la función informática, que engloba el análisis de la organización, seguridad, segregación de funciones y gestión de las actividades de proceso de datos.

3.2.1 Objetivos de la auditoria TIC

Verificar el control de la gestión informática, asegurando a la alta dirección y al resto de las áreas de la empresa que la información que les llega es la necesaria en el momento oportuno, y es confiable, ya que les sirve de base para tomar decisiones importantes.

Eliminar o reducir al máximo la posibilidad de pérdida de la información por fallos en los equipos, en los procesos o por una gestión inadecuada de los archivos de datos.

Detectar y prevenir fraudes por manipulación de la información o por acceso de personas no autorizadas a transacciones que exigen traspasos de fondos.

3.2.2 El Auditor Informático

El Auditor informático es la persona que pone a disposición de la función auditora, sea externa o interna, sus conocimientos técnicos de informática. Evalúa y comprueba los controles y procedimientos informáticos más complejos, desarrollando y aplicando técnicas sofisticadas en algunos casos, incluyendo el uso de software, es decir, debe actuar como auditor y consultor de la empresa en materia de seguridad, control interno operativo, eficiencia y eficacia, tecnología informática, gestión de riesgos, etc.

Las funciones de análisis y revisión del auditor informático, pueden chocar con la psicología del auditado, ya que es un informático y tiene la necesidad de realizar sus tareas acorde a las tecnologías vigentes. La reticencia del auditado es comprensible y, en ocasiones, fundada. El nivel técnico del auditor es a veces insuficiente, dada la gran complejidad de los Sistemas, unidos a los plazos demasiado breves de los que suelen disponer para realizar la auditoria.

Es por ello que se dice que, es más fácil que un informático adquiera los principios del control, de la auditoría y de la seguridad, que un auditor financiero llegue a adquirir el nivel técnico informático necesario.

Que hacen y no deben hacer los auditores informáticos, entre otras acciones;

Deben hacer	No deben hacer
+ Recomendar + Ser independientes y objetivos + Ser competentes + Basar su opinión en evidencias + Conocer perfiles de usuarios + Conocer criterios y prácticas de TIC + Velar que los sistemas contengan e incorporen normas y requerimientos de información de la organización. + Revisar codificación de aplicaciones + Revisar documentación + Evaluar riesgos e informar + Aplicar pruebas o procedimientos de auditoría.	• Obligar, forzar o amenazar • Actuar en beneficio propio • Asumir responsabilidades para los cuales no está preparado. • Basar su opinión en suposiciones • Realizar gestión de perfiles de usuarios • Realizar labores de desarrollo o gestión de tecnología • Gestión y asignación de contraseñas • Hacer funciones de documentación y análisis • Codificar, programar o documentar • Garantizar inexistencia de riesgos

Tabla 3.1
Acciones de los auditores

3.2.3 Principales dificultades en la gestión las TIC

a) Percepción de la función de los sistemas de información

Es muy común que se perciba a esta función como un servicio de soporte de las funciones de línea, por lo que los recursos que se asignan y la atención de la dirección se dirigen a las líneas en teoría más importante, aun en una gran mayoría se mantiene.

Muchos usuarios ven a la función de los sistemas de información como “un restaurante de cocina rápida”. Las necesidades de los clientes son siempre inmediatas y tiene prioridad número uno, sobre cualquier tema de gestión interna de la función.

Así es frecuente encontrar; documentación escasa de operación y soporte de explotación, gestión eficiente del almacenamiento, planificación de la capacidad, seguimiento y gestión del rendimiento de los equipos, instalación desactualizada de versiones y correcciones de errores ene l software proporcionado por los vendedores, procedimientos de control de cambios en aplicaciones, planes de recuperación en caso de desastres y prueba de los mismos, revisiones periódicas de las librerías críticas para asegurar que rutinas no autorizadas no se han insertado en programas por

programaciones de sistemas u otros profesionales y seguimiento de los informes de intentos de violación de seguridad.

b) Excesivo poder de los informáticos

Los sistemas de información son, por su naturaleza, un tema esotérico y los técnicos lo saben y han ejercido un tremendo poder debido a su experiencia.

La naturaleza técnica, complejidad y rápida evolución de los sistemas de información, crean una barrera formidable para los que son ajenos a la función.

La alta dirección carece de tiempo y de inclinación a educarse en tales áreas técnicas.

Los directivos informáticos raramente son promocionados a posiciones de alta dirección debido a su falta de experiencia en el negocio.

c) Abdicación de la alta dirección

La alta dirección generalmente abdica de sus responsabilidades sobre los sistemas de información. Los directivos de las empresas se pueden clasificar en tres categorías:

- Aquellos que desearían que la tecnología desapareciera.
- Los que piensan que este trabajo debería ser elevado en su categoría y delegado en una persona importante dentro de la organización, alguien que se ocupe de ello y le mantenga informado y alejado de los problemas.
- Los que perciben la tecnología como una parte integral del día a día y reconocen que el director de sistemas de información debe formar parte del equipo de la alta dirección.

d) Los usuarios tienen dificultad para definir sus necesidades

Los usuarios tienen serias dificultades en la definición de sus necesidades.

La dificultad humana básica, es especificar requisitos para sistemas abstractos, tales como especificar por adelantado los criterios positivos para evaluar los sistemas actuales.

Así mismo, se demuestra que los usuarios están más capacitados para identificar fallas, esto es, capacidad que posee un usuario para señalar, cuándo el sistema no es capaz de resolver su problema como él esperaba.

e) Resistencia de los usuarios al cambio

La tecnología de la información es, a menudo, aplicada inapropiadamente y desperdiciada muchas de sus potencialidades debido a los procedimientos obsoletos de trabajo utilizada por los usuarios y su resistencia al cambio.

Una nueva aplicación se desarrolla, de acuerdo con las especificaciones de los usuarios, ya que estos están muy interesados en mantener las relaciones actuales de dependencia, se evitan cambios fundamentales en el trabajo.

f) Informática de usuario final

Hoy los usuarios explotan directamente máquinas con una mínima intermediación en infinidad de áreas, cada vez son más independientes en los trabajos que realizan.

Hay tres razones importantes para ello:

- La acelerada evolución de la tecnología de información representada por los microprocesadores.
- El gran incremento de la formación de los usuarios.
- El gran crecimiento de las carteras de aplicación.

Dada esta situación nos lleva a preguntarnos ¿cómo mejorar la gestión y el control de las tecnologías de información?; como hemos visto cada vez se hace más evidente para legisladores, usuarios y proveedores de servicios la necesidad de un marco de referencia para la seguridad y el control de la tecnología de la información.

3.2.4 Síntomas de necesidad de una Auditoría Informática:

Las empresas acuden a las auditorías externas cuando existen síntomas bien perceptibles de debilidad. Estos síntomas pueden agruparse en clases:

- Síntomas de descoordinación y desorganización:
  - No coinciden los objetivos de la Informática de la Compañía y de la propia Compañía.
  - Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente.

- Puede ocurrir debido a algún cambio masivo de personal, o en una reestructuración fallida de alguna área o en la modificación de alguna Norma importante.

- Síntomas de mala imagen e insatisfacción de los usuarios:
  - No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios de Software en los terminales de usuario, refrescamiento de paneles, variación de los ficheros que deben ponerse diariamente a su disposición, etc.
  - No se reparan las averías de Hardware ni se resuelven incidencias en plazos razonables. El usuario percibe que está abandonado y desatendido permanentemente.
  - No se cumplen en todos los casos los plazos de entrega de resultados periódicos. Pequeñas desviaciones pueden causar importantes desajustes en la

actividad del usuario, en especial en los resultados de Aplicaciones críticas y sensibles.

- Síntomas de debilidades económico-financiero:
  - Incremento desmesurado de costes.
  - Necesidad de justificación de Inversiones Informáticas (la empresa no está absolutamente convencida de tal necesidad y decide contrastar opiniones).
  - Desviaciones Presupuestarias significativas.
  - Costes y plazos de nuevos proyectos (deben auditarse simultáneamente a Desarrollo de Proyectos y al órgano que realizó la petición).

- Síntomas de Inseguridad: Evaluación de nivel de riesgos
  - Seguridad Lógica
  - Seguridad Física
  - Confidencialidad
  - Continuidad del Servicio. Es un concepto aún más importante que la Seguridad. Establece las estrategias de continuidad entre fallos mediante Planes de Contingencia Totales y Locales.

    Planes de Contingencia:

    Por ejemplo, la empresa sufre un corte total de energía o explota, ¿Cómo sigo operando en otro lugar? Lo que generalmente se pide es que se hagan Backus de la información diariamente y que aparte, sea doble, para tener un Backup en la empresa y otro afuera de ésta. Una empresa puede tener unas oficinas paralelas que posean servicios básicos (luz, teléfono, agua) distintos de los de la empresa principal, es decir, si a la empresa principal le proveía teléfono Cotel, a las oficinas paralelas seria otra como Entel. En este caso, si se produce la inoperancia de Sistemas en la empresa principal, se utilizaría el Backup para seguir operando en las oficinas paralelas. Los Backups se pueden acumular durante dos meses, o el tiempo que estipule la empresa, y después se van reciclando.

  - Centro de Proceso de Datos fuera de control. Si tal situación llegara a percibirse, sería prácticamente inútil la auditoría. Esa es la razón por la cual, en este caso, el síntoma debe ser sustituido por el mínimo indicio.

3.2.5 Estándares internacionales para Auditoría de TIC (COBIT, ISO 2700x)

Existen dos estándares ampliamente usados para la realización de auditorías de TIC, estos son COBIT y la familia ISO 2700x, a continuación se da una breve descripción de ellos.

3.2.5.1 COBIT

COBIT es un acrónimo para Control Objectives for Information and related Technology (Objetivos de Control para tecnología de la información y relacionada); desarrollada por la Information Systems Audit and Control Association (ISACA) y el IT Governance Institute (ITGI).

COBIT es un estándar aceptada mundialmente para el adecuado control de proyectos de tecnología, los flujos de información y los riesgos que éstas implican. La metodología COBIT se utiliza para planear, implementar, controlar y evaluar el gobierno sobre TIC; incorporando objetivos de control, directivas de auditoría, medidas de rendimiento y resultados, factores críticos de éxito y modelos de madurez.

El término "generalmente aplicable y aceptado" es utilizado en el mismo sentido que los Principios de Contabilidad Generalmente Aceptados (PCGA o GAAP por sus siglas en inglés), proveyendo un marco de referencia para la Administración (gerencia), Usuarios y Auditores.

COBIT contribuye a reducir las brechas existentes entre los objetivos de negocio, y los beneficios, riesgos, necesidades de control y aspectos técnicos propios de un proyecto TIC; proporcionando un Marco Referencial Lógico para su dirección efectiva.

¿Qué ofrece COBIT?

El marco referencial conceptual de la metodología COBIT proporciona una visión integral, capaz de responder a las necesidades de directivos, usuarios (de diverso nivel) y auditores (internos y externos).

Se busca enlazar los objetivos empresariales con los objetivos TIC y los procesos TIC. En la práctica esto se logra identificando los:

- Requerimientos del negocio para la información, y los
- Recursos de TIC que son impactados en forma primaria por cada objetivo de control, asociado a cada proceso TIC.

1. Requerimientos de negocio para la información:

- Efectividad: Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.

- Eficiencia: Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.

- Confidencialidad: Se refiere a la protección de información sensible contra divulgación no autorizada.
- Integridad: Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.
- Disponibilidad: Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.
- Cumplimiento: Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocio está sujeto, por ejemplo, criterios de negocio impuestos externamente.
- Confiabilidad: Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

2. Recursos TIC:

- Datos: Los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.
- Aplicaciones: Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.
- Tecnología: La tecnología cubre hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.
- Instalaciones: Recursos para alojar y dar soporte a los sistemas de Información.
- Personal: Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorizar servicios y sistemas de información.

3. Procesos de TIC:

4 dominios en línea con el ciclo administrativo o ciclo de vida aplicable a los procesos de TI:

- Planeación y organización
- Adquisición e implementación
- Entrega y soporte
- Monitoreo

Asociados a los 4 dominios existen 34 procesos de alto nivel, desagregados en 302 procesos y/o actividades menor jerarquía.

Para cada proceso de alto nivel existen objetivos, medidas de control de diversa naturaleza, indicadores asociados (de objetivo clave –key goal indicator, KGI- y de rendimiento clave - key performance indicator, KPI-), además de modelos de madurez.

Para cada medida de control se lleva a cabo una clasificación dentro del marco referencial CobIT:

- **Primario**: es el grado al cual el objetivo de control definido impacta directamente el requerimiento de información de interés.
- **Secundario**: es el grado al cual el objetivo de control definido satisface únicamente de forma indirecta o en menor medida el requerimiento de información de interés.
- **Blanco (vacío)**: podría aplicarse; sin embargo, los requerimientos son satisfechos más apropiadamente por otro criterio en este proceso y/o por otro proceso.

A su vez cada proceso y/o actividad de menor jerarquía involucra una sumatoria de buenas prácticas necesarias de considerar para el cumplimiento de los requisitos de control exigidos para cada caso, estableciendo los resultados deseados o propósitos a ser alcanzados mediante su implementación.

En resumen, la 1) información que los procesos de negocio necesitan es proporcionada a través del empleo de 2) recursos TIC. Con el fin de asegurar que los requerimientos de negocio para la información sean satisfechos, se deben definir, implementar, monitorear y evaluar las medidas de control adecuadas para estos recursos.

3.2.5.2 ISO/IEC 27001

ISO (Organización Internacional de Estándares) e **IEC** (Comisión Internacional de Electrotécnia) conforman un especializado sistema especializado para los estándares mundiales.

La familia completa ISO 27000 está formada por los siguientes documentos:

ISO/IEC	Descripción
27000	Vocabulario y definiciones (*InformationTechnology – Information Security Management – Fundamentals and Vocabulary*).

27001	Especificación de la estructura metodológica (basada en el BS7799-2:2002) (*InformationTechnology –Security Techniques– Information Security Management Systems – Requirements*).
27002	Código de prácticas (*Code of Practice for Information Security Management*). Actualmente ISO/IEC 17799:2005, publicado el 15 de junio de 2005.
27003	Guía de implementación (ISMS *Implementation Guidance*, en desarrollo).
27004	Métricas y medidas (*Information Security Management Measurement,* en desarrollo).
27005	La Administración del Riesgo (basado BS 7799-3) (*Information Security Risk Managemen*t, basado e incorporado a ISO/IEC 13335 MICTS part 2, en desarrollo).
27006	Requerimientos para organismos de acreditación de Sistemas de Gestión de Seguridad de la Información (*Information Technology – Security Techniques – Requirements for Bodies Providing Audit and Certification of Information Security Management Systems*).

Tabla 3.2
Familia ISO 2700x

Este estándar Internacional ha sido preparado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

- La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos y sus sistemas de apoyo cambien a lo largo del tiempo.
- Se espera que la implementación de un SGSI se extienda en concordancia con las necesidades de la organización; por ejemplo, una situación simple requiere una solución SGSI simple.
- Este Estándar Internacional promueve la adopción de un enfoque del proceso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización.

- La aplicación de un sistema de procesos dentro de una organización, junto con la identificación y las interacciones de estos procesos, y su gestión, puede considerarse un ‘enfoque del proceso’.

Un enfoque del proceso para la gestión de la seguridad e la información presentado en este Estándar Internacional fomenta que sus usuarios enfaticen la importancia de:

a) entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información;
b) implementar y operar controles para manejar los riesgos de la seguridad de la información;
c) monitorear y revisar el desempeño y la efectividad del SGSI; y
d) mejoramiento continúo en base a la medición del objetivo.

Este Estándar Internacional adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI (Sistema de Gestión de Seguridad de la Información).

- **Planear (establecer el SGSI)**

Establecer política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.

- **Hacer (implementar y operar el SGSI)**

Implementar y operar la política, controles, procesos y procedimientos SGSI.

- **Chequear (monitorear y revisar el SGSI)**

Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión.

- **Actuar (mantener y mejorar el SGSI)**

Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continúo del SGSI.

Alcance

- Este Estándar Internacional abarca todos los tipos de organizaciones (por ejemplo; empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro).
- Este Estándar Internacional especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos comerciales generales de la organización. Especifica los requerimientos para la implementación de controles de seguridad personalizados para las necesidades de las organizaciones individuales o partes de ella.
- El SGSI está diseñado para asegurar la selección adecuada y proporcionar controles de seguridad que protejan los activos de información y den confianza a las partes interesadas.

Aplicación

Los requerimientos establecidos en este Estándar Internacional son genéricos y están diseñados para ser aplicables a todas las organizaciones, sin importar el tipo, tamaño y naturaleza.

Requerimientos generales

La organización debe establecer, implementar, operar, monitorear, mantener y mejorar continuamente un SGSI documentado dentro del contexto de las actividades comerciales generales de la organización y los riesgos que enfrentan. Para propósitos de este Estándar Internacional, los procesos utilizados se basan en el modelo PDCA.

3.3 Técnicas de Auditoria Asistidas por Computador (TAAC)

Actualmente en toda organización moderna se procesan las transacciones a través del computador. El procesamiento electrónico transforma miles de datos en información con valor económico constituyéndose uno de los activos más valiosos de la organización, por lo cual es importante la gestión sobre la información a efecto de que no se vuelva de difícil acceso se destruya o sea manipulada con fines dolosos.

Por tanto la administración como los auditores deben conocer como se produce esa información y como debe protegerse.

Esto significa que los auditores tienen que realizar sus exámenes y emitir su opinión profesional sobre datos e información que surgen de sistemas computadorizados. Por tal motivo es importante que se conozca el tipo de implicancias y efectos que sobre la tarea profesional causa este tipo de procesamiento en comparación con los sistemas convencionales, enfocado hacia la evidencia de auditoría que proporcionan. Estas características son:

- La pista de auditoría en los sistemas computadorizados no se evidencia de forma expresa o no es de fácil acceso. En muchos casos la realización del control forma parte de la lógica del programa utilizado, incluido en pasos específicos del mismo que no utiliza mayor documentación por lo que la forma de revisión tiene que cambiar en la forma de buscar y evaluar evidencias de auditoría.
- Si desde los sistemas computarizados, se desliza un error éste tiene un gran efecto multiplicador, porque afecta a un mayor volumen de transacciones.
- Muchos errores que se producen en los sistemas computadorizados son difícilmente detectables por que se encuentran en un gran volumen de transacciones que se procesan a grandes velocidades por lo que son muy difíciles de evaluar manualmente.
- El procesamiento de información mediante computadora somete uniformemente todas las transacciones de un tipo de transacción al mismo algoritmo, por lo tanto usa las mismas instrucciones de procesamiento para transacciones similares, con poca participación del elemento humano, por esta causa, tienen mayor materialidad por su efecto multiplicador, en este punto son la calidad de las consistencias, la actualización, su monitoreo la forma de contrarrestar sus efectos negativos y esto manualmente puede hacerse con limitado alcance por lo cual frente a ello surge la importancia de las Técnicas de Auditoría Asistidas por Computador - TAACs.
- El acceso sin autorización de ciertos individuos, incluyendo aquellos que realizan procedimientos para alterar datos sin dejar evidencias visibles, puede ser mayor en los sistemas computarizados que en los sistemas manuales. Ello se debe a que la información es almacenada en forma electrónica, con una menor participación del hombre en el procesamiento, reduciéndose por consiguiente la oportunidad de detectar manualmente los accesos no autorizados, toda vez que la segregación de funciones como factor de control interno es afectada sustancialmente.
- Es siempre muy importante, tener en cuenta que aún cuando existen diferencias sustanciales entre la forma de procesar información en forma manual y mediante sistemas computarizados, toda la normatividad señala que esto no afecta a los objetivos del control interno, la responsabilidad de la dirección y la revisión del auditor en todo los casos sin limitaciones inherentes al sistema de control interno; pero si afecta el enfoque para la evaluación del mismo y el tipo de evidencia de auditoría que se obtiene.

Por lo tanto, se establece que las condiciones cambiantes son el factor que determina el nuevo enfoque que debe tener el auditor frente a los procesos automatizados que tiene que examinar.

Practicar auditorías en un ambiente computarizado, donde la informatización de los sistemas contables y de gestión han alcanzado un desarrollo notable, conlleva la introducción de una concepción diferente a la existente durante décadas; donde la

informática participa activamente como una valiosísima herramienta, que permite a esta disciplina evolucionar al mismo ritmo de las transformaciones incorporadas a la estructura del registro y del Control Interno.

Consecuentemente, se hace indispensable el empleo de las técnicas de auditoría asistidas por computadora (TAAC) que permiten al auditor, evaluar las múltiples aplicaciones específicas del sistema que emplea la unidad auditada, examinar un diverso número de operaciones específicas del sistema en explotación, facilitar la búsqueda de evidencias, reducir al mínimo el riesgo de la auditoría para que los resultados expresen la realidad objetiva de las deficiencias, así como de las violaciones detectadas y elevar notablemente la eficiencia en el trabajo. En tal sentido, el auditor tendrá que enfrentar un importante reto al tener que adentrarse en el conocimiento de una nueva forma de practicar esta disciplina.

Atendiendo a la importancia que reviste para la auditoría un ambiente informático, al ser un elemento estratégico para la organización y por constituir una de las áreas que mayores posibilidades aportan en la obtención de evidencias de forma rápida y precisa, la incursión en este ámbito es decisiva ya que posibilita, obtener evidencias y pistas viables que permitan establecer una valoración fiable con relación a las deficiencias, violaciones, adulteraciones e incluso detectar prácticas presuntamente delictivas.

Ventajas del uso de las TAAC

La utilización de las TAAC ofrece las ventajas siguientes:

- Incrementan o amplían el alcance de la investigación y permiten realizar pruebas que no pueden efectuarse manualmente;
- Incrementan el alcance y calidad de los muestreos, verificando un gran número de elementos;
- Elevan la calidad y fiabilidad de las verificaciones a realizar;
- Reducen el período de las pruebas y procedimientos de muestreos a un menor costo;
- Garantizan el menor número de interrupciones posibles a la entidad auditada;
- Brindan al auditor autonomía e independencia de trabajo, al no depender sólo de las verificaciones que se detallan en las guías de auditoría;
- Permiten efectuar simulaciones sobre los procesos sujetos a examen y monitorear el trabajo de las unidades;
- Realizar un planeamiento a priori sobre los puntos con potencial violación del Control Interno;

- Disminución considerable del riesgo de no-detección de los problemas;
- Posibilidad de que los auditores actuantes puedan centrar su atención en aquellos indicadores que muestren saldos inusuales o variaciones significativas, que precisan de ser revisados como parte de la auditoría;
- Elevación de la productividad y de la profundidad de los análisis realizados en la auditoría;
- Posibilidad de rescatar valor[1] en el resultado de cada auditoría;
- Elevación de la autoestima profesional del auditor, al dominar técnicas de punta que lo igualan al desarrollo de la disciplina en el ámbito internacional.

Es importante recalcar que las TAAC solamente son una herramienta que puede ser utilizado para una auditoría financiera o una auditoria de la información, no es equivalente a realizar una Auditoria de Tecnologías de Información y Comunicación.

3.4 Principales enfoques de la Auditoría de TIC

Para determinar los posibles enfoques que se le puede dar a una auditoria de TIC, es necesario determinar determinados criterios que podrían aplicarse. Para este propósito, recordemos que una auditoría financiera aplica fundamentalmente las NIIF y NIA como criterios fundamentales. De manera similar una auditoria TIC requiere criterios para su evaluación. En este sentido, conozcamos en primera instancia como está compuesta de forma general un área de Tecnología de Información:

[1] El valor rescatado en la auditoria es el gasto o la pérdida que no se incurrirá por la unidad si esta sigue las recomendaciones que se señalan en la auditoría, puede relacionarse con un pronóstico de aumento de ventas o de disminución de pérdidas al no vencerse los productos.

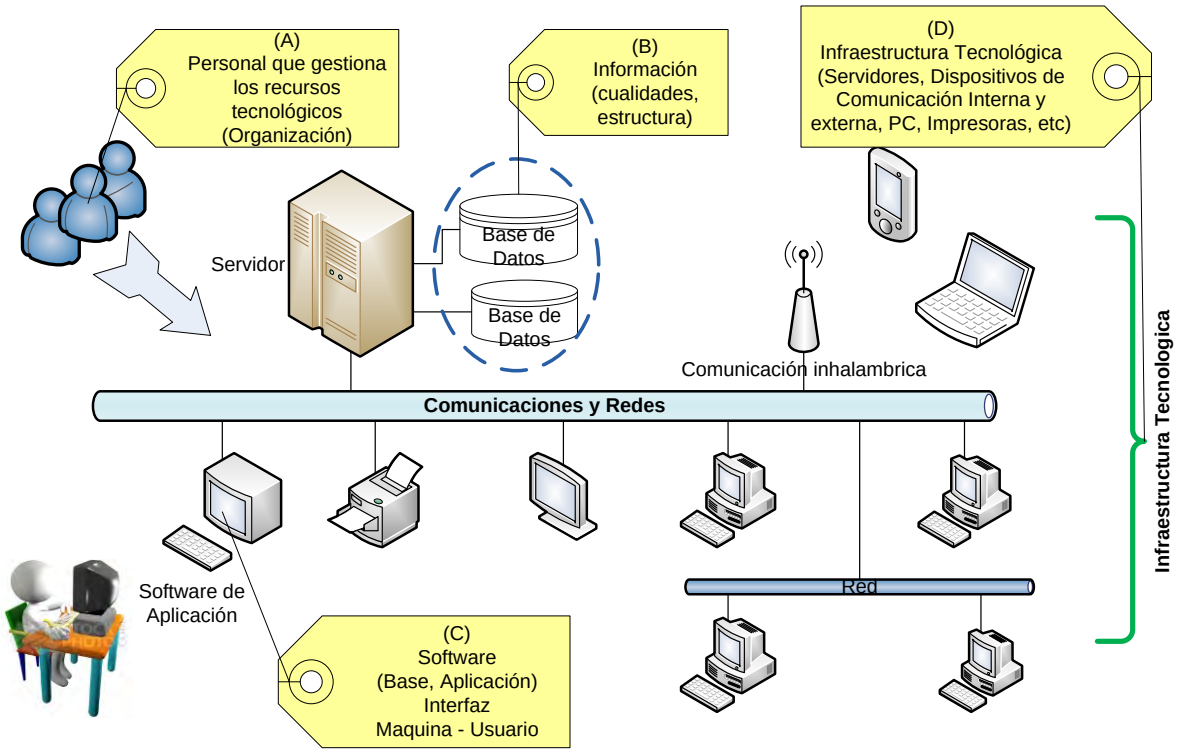

Figura 3.2
Consideraciones al enfocar una auditoría de TIC

El funcionamiento de un Área de Tecnología de Información de acuerdo al grafico es el siguiente: “Los usuarios finales interactúan con los sistemas de información a través de software (software base y de aplicación), los cuales utilizan infraestructura tecnológica (servidores, PC, impresoras, dispositivos de comunicación, etc.) para registrar, almacenar (Base de Datos) y generar reportes. Cada aspecto tecnológico es gestionado por Personal de la Gerencia de Sistemas”.

En el grafico se presenta las siguientes etiquetas importantes:

(A) Existe personal o recursos humanos que se encarga de gestionar todos los recursos tecnológicos (generalmente una Gerencia de Sistemas), estos normalmente se encuentran bajo una estructura organizativa formalmente aprobada, como parte de toda la institución y con funciones definidas en manuales, por lo que se espera que la gestión de los mismos sea eficaz eficiente y económico.

(B) La información debe contar con ciertas cualidades deseadas como ser: Integridad, confidencialidad, disponibilidad, etc., cada uno de los cuales de acuerdo al estado en que se encuentre mostrará un determinado nivel de la información en cuanto a su seguridad.

(C) El software utilizado permite la interacción entre usuarios y las maquina, de acuerdo a su nivel de relación se utilizan desde el software base que incluye los Sistemas Operativos (Windows, Linux, Android, etc.), y otros que permiten interactuar entre dispositivos y personas, hasta los de aplicación que son los que usan los usuarios finales (Office, OpenOffice, etc). Se espera que este cuente con niveles de seguridad aceptables en su configuración para proteger la información almacenada y transmitida.

(D) La infraestructura utilizada desde equipos PC, impresoras a nivel mono usuario se integran a través de dispositivos de red con grandes equipos como Servidores de Base de Datos, de Aplicación, de Correos, etc., incluyendo desde y hacia dispositivos móviles (Celulares, Palm, IPad, Laptop, etc.). Se espera que esta infraestructura sea aprovechada de la manera más eficaz, eficiente y económica.

En este sentido, existen diferentes enfoques para enfrentar una auditoria de TIC. Entre estos tenemos los siguientes:

La auditoria de TIC de acuerdo a las Normas de Auditoria Gubernamental puede ser orientada hacia uno o varios de los siguientes enfoques:

- **Enfoque a las Seguridades**: Consiste en evaluar las seguridades implementadas en los sistemas de información con la finalidad de mantener la confidencialidad, integridad y disponibilidad de la información.
- **Enfoque a la Información**: Consiste en evaluar la estructura, integridad y confiabilidad de la información gestionada por el sistema de información.
- **Enfoque a la Infraestructura tecnológica**: Consiste en evaluar la correspondencia de los recursos tecnológicos en relación a los objetivos previstos.
- **Enfoque al Software de Aplicación**: Consiste en evaluar la eficacia de los procesos y controles inmersos en el software de aplicación, que el diseño conceptual de éste cumpla con el ordenamiento jurídico administrativo vigente.
- **Enfoque a las Comunicaciones y Redes**: Consiste en evaluar la confiabilidad y desempeño del sistema de comunicación para mantener la disponibilidad de la información.

Otro enfoque aceptable es la que distribuye en:

- Auditoria alrededor del computador
- Auditoria a través del computador

3.4.1 Auditoria alrededor del computador

En el enfoque alrededor del computador, los programas y los archivos de datos no se auditan.

La auditoría alrededor del computador concentra sus esfuerzos en la entrada de datos y en la salida de información. Es el más cómodo para los auditores de sistemas, por cuanto únicamente se verifica la efectividad del sistema de control interno en el ambiente externo de la máquina. Naturalmente que se examinan los controles desde el origen de los datos para protegerlos de cualquier tipo de riesgo que atente contra la integridad, completitud, exactitud y legalidad.

La auditoría alrededor del computador no es tan simple como aparentemente puede presentarse, pues tiene objetivos muy importantes como:

- Verificar la existencia de una adecuada segregación funcional.
- Comprobar la eficiencia de los controles sobre seguridades físicas y lógicas de los datos.
- Asegurarse de la existencia de controles dirigidos a que todos los datos enviados a proceso estén autorizados.
- Comprobar la existencia de controles para asegurar que todos los datos enviados sean procesados.
- Cerciorarse que los procesos se hacen con exactitud.
- Comprobar que los datos sean sometidos a validación antes de ordenar su proceso.
- Verificar la validez del procedimiento utilizado para corregir inconsistencias y la posterior realimentación de los datos corregidos al proceso.
- Examinar los controles de salida de la información para asegurar que se eviten los riesgos entre sistemas y el usuario.
- Verificar la satisfacción del usuario. En materia de los informes recibidos.
- Comprobar la existencia y efectividad de un plan de contingencias, para asegurar la continuidad de los procesos y la recuperación de los datos en caso de desastres.

Se puede apreciar la ambición de los objetivos planteados, pues solamente faltarían objetivos relacionados con el examen de los archivos y los programas, lo cual es parte de otro enfoque.

Informe de esta Auditoría: deberá redactarse en forma sencilla y ordenada, haciendo énfasis en los riesgos más significativos e indicando el camino a seguir mediante recomendaciones económicas y operativamente posibles.

Pasos que se deben seguir en la auditoría:

- Metodología de la auditoría.
- Objetivos de la auditoría.
- Evaluación del sistema de control interno.
- Procedimientos de auditoría.
- Papeles de trabajo.

- Deficiencias de control interno.
- Informe de auditoría.

3.4.2 Auditoria a través del computador

Este enfoque está orientado a examinar y evaluar los recursos del software, y surge como complemento del enfoque de auditoría alrededor del computador, en el sentido de que su acción va dirigida a evaluar el sistema de controles diseñados para minimizar los fraudes y los errores que normalmente tienen origen en los programas.

Este enfoque es más exigente que el anterior, por cuanto es necesario saber con cierto rigor, lenguajes de programación o desarrollo de sistemas en general, con el objeto de facilitar el proceso de auditoría.

Objetivos de esta auditoría

- Asegurar que los programas procesan los datos, de acuerdo con las necesidades del usuario o dentro de los parámetros de precisión previstos.
- Cerciorarse de la no-existencia de rutinas fraudulentas al interior de los programas.
- Verificar que los programadores modifiquen los programas solamente en los aspectos autorizados.
- Comprobar que los programas utilizados en producción son los debidamente autorizados por el administrador.
- Verificar la existencia de controles eficientes para evitar que los programas sean modificados con fines ilícitos o que se utilicen programas no autorizados para los procesos corrientes.
- Cerciorarse que todos los datos son sometidos a validación antes de ordenar su proceso correspondiente.

Informe de Auditoría: deberá orientarse a opinar sobre la validez de los controles, en este caso de software, para proteger los datos en su proceso de conversión en información.

De acuerdo a estos enfoques se puede observar que los enfoques en general son a la Gestión del Tecnologías de Información (alrededor del computador) y el enfoque a la Seguridad de la Información (a través del computador). Estos enfoques pueden ser cubiertos por metodologías propias y adaptadas de estándares como el COBIT y la ISO 127001 particularmente.

4 Metodología de la Auditoría de TIC

Al parecer, muchos tienen la impresión de que conociendo lo que es informática, puedan ser aptos para realizar una auditoría de TIC. Por otra parte, existen los que consideran que siendo auditores pueden desempeñar esta labor de forma complementaria. Ambos se encuentran bastante lejos de la realidad, debido a que en ambas profesiones existen vacíos para poder desempeñar la función de Auditor de TIC; a los Auditores les hace falta conocer aspectos tecnológicos que por el grado de avance de la tecnología le será más difícil adquirir y mantener el nivel adecuado; por otra parte el Informático requiere conocer técnicas de auditoría que normalmente no son tan variantes como la tecnología, por lo tanto, el informático es más probable que pueda alcanzar lograr contar con los conocimientos necesarios para desempeñar la función de Auditor de TIC. Sin embargo, cada uno puede cruzar la frontera y aprender para lograr desempeñar esta función tan delicada.

Debido a esto existen autores que consideran que las únicas metodologías que se pueden encontrar en la auditoría informática son dos familias: las auditorias de controles generales como producto estándar de auditorías profesionales, y las metodologías de auditores internos.

El objetivo de las auditorias de controles generales es “dar una opinión sobre la fiabilidad de los datos del computador para la auditoría financiera”. Sin embargo, el resultado externo es bastante escueto en cuanto al informe generado, ya que es parte del informe de auditoría, donde se destacan la vulnerabilidad encontrada. Están basados en pequeños cuestionarios estándares que dan como resultado informes muy generales. Tienen apartados para definir pruebas y anotar sus resultados. La auditoría debe demostrar con pruebas todas las afirmaciones, y por ello siempre debe contener dicho apartado.

Estas metodologías están muy cuestionadas, pero no porque sean malas en sí mismas, sino porque dependen mucho de la experiencia de los profesionales que las usan y existe una práctica de utilizarlas por profesionales sin ninguna experiencia.

Todas estas anomalías nacen de la dificultad que tiene un profesional sin experiencia que asume la función auditora y busca una fórmula fácil que le permita empezar su trabajo rápidamente. Definitivamente esto es una utopía, el auditor informático necesita una larga experiencia y gran formación tanto auditora como informática y esta formación debe ser adquirida mediante el estudio y la práctica.

Dado lo anterior, es necesario decir que la metodología del auditor interno debe ser diseñada y desarrollada por el propio auditor, y ésta será la repercusión de su grado de experiencia y habilidad.

El auditor de TI debe evaluar los riesgos globales y luego desarrollar un programa de auditoría que consta de objetivos de control y procedimientos de auditoría que deben satisfacer esos objetivos. El proceso de auditoría exige que el auditor de TI reúna evidencia, evalúe fortalezas y debilidades de los controles existentes basado en la evidencia recopilada, y que prepare un informe de auditoría que presente esos temas en forma objetiva a la gerencia. Asimismo, la gerencia de auditoría debe garantizar una disponibilidad y asignación adecuada de recursos para realizar el trabajo de auditoría.

4.1 Perspectivas de la auditoria y de la informática

4.1.1 Auditoría de la función informática

Su finalidad es verificar la existencia de control interno en el centro de proceso de datos. Para ello, se deben analizar los riesgos inherentes a las funciones básicas de gestión, administración, planificación, organización y normativa general, y a las más especializadas, como son las de desarrollo y explotación y técnica de sistemas, así como la seguridad física de las instalaciones y los datos.

La primera parte de este análisis respondería al mismo esquema utilizado en cualquier otra área de la empresa, ya que se trataría de examinar la organización existente con la finalidad de determinar si responde a los criterios fijados por la dirección y a las necesidades actuales y si asegura la salvaguarda física de la información de la empresa.

Una segunda parte se refiere a los procedimientos de trabajo relativos tanto a la operativa informática normal (explotación), como al mantenimiento e implementación de nuevos sistemas informáticos (desarrollo).

La tercera parte debería verificar todos los controles globales del sistema informático y las medidas de seguridad del equipo, los programas y los datos.

En síntesis, el programa de trabajo consistiría en analizar; la organización y gestión de las actividades del centro de proceso de datos o departamento informático, los sistemas informáticos en fase de desarrollo, el mantenimiento de los sistemas informáticos, la explotación de los recursos informáticos, la seguridad, los sistemas de comunicaciones, la administración de la base de datos.

Un sistema informático es el conjunto de programas desarrollados para dar una solución informática a un problema concreto, dentro de un área de actividad empresarial. Por ejemplo; contabilidad, nóminas, gestión de proveedores, reservas de plazas, facturación, etc.

El auditor puede analizar;

- La totalidad de la aplicación o una serie de programas relacionados con uno de estos tratamientos, según donde se haya detectado el problema, también pueden evaluarse las relaciones de una aplicación mecanizada con otras aplicaciones.
- Los controles que afectan a todas las aplicaciones y verificar si existe un nivel suficiente de control en todas y cada una de las áreas y sí éstas son una garantía de que el entorno en el que van a desenvolverse las aplicaciones, es seguro y adecuado.
- El grado de eficiencia y utilidad de los sistemas, así como la fiabilidad y seguridad de la información que suministran.

Por lo tanto, la finalidad de la auditoría de un sistema informático es evaluar en qué medida se está garantizando el control interno con la utilización de esa aplicación, la seguridad de los datos y programas, así como el rendimiento de la misma en relación a la finalidad con la que fue diseñada, en términos de costo – eficiencia.

Para ello es necesario, en primer lugar, llegar a conocer el proceso, detectar los controles existentes y probar su funcionamiento. El desarrollo del trabajo sería el siguiente:

- Definición de los objetivos.
- Análisis de la eficacia del sistema, su eficiencia y utilidad.
- Identificación del proceso, procedimientos administrativos, flujo de información, etc.
- Analizar la organización existente alrededor del sistema, segregación de funciones, etc.
- Análisis de la aplicación de; controles de entrada, controles de procesamiento, controles de salida, controles generales.
- Identificar los controles operativos y hacer pruebas de cumplimiento.
- Identificar fallas de control.
- detectar los riesgos.
- Proponer sugerencias.

4.1.2 La informática en la auditoría

Nos da la posibilidad de:

- Profundizar en las áreas más complejas de la empresa.
- Reducir las horas dedicadas a trabajos respectivos.
- Mejorar la propia gestión de la auditoría.

En realidad, prácticamente todos los trabajos de auditoría son susceptibles a mecanización, el que conceda prioridad a unos u otros depende de la organización

interna, del interés que se tenga en potenciar cada una de esas actividades de auditoría y de los medios disponibles. Teniendo esto en cuenta, se debe proceder a diseñar el plan informático de auditoría, que ha de ser fiel reflejo de los recursos y necesidades de cada empresa.

Para desarrollar este plan se determina; su ámbito o alcance, los recursos necesarios y la formación informática de los auditores. Se trata de examinar las distintas actividades de auditoría con posibilidades de mecanización; es decir, los tipos de auditoría susceptibles de utilizar en ellos herramientas informáticas a fin de facilitar el trabajo de los auditores y ahorrar tiempo.

4.1.3 Los controles internos en la TI

Tradicionalmente se han definido los controles internos como cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos.

Los controles internos que se utilizan en el entorno informático evolucionan continuamente a medida que los sistemas informáticos se vuelven más complejos.

Históricamente, los objetivos de los controles informáticos se han clasificado en las siguientes categorías;

Controles preventivos; para tratar de evitar un evento, como el uso de un software de seguridad que impida los accesos no autorizados al sistema.

Controles detectores; cuando fallan los preventivos para tratar de conocer cuanto antes o porque ha ocurrido el evento, por ejemplo, el registro de intentos de acceso no autorizados, el registro de la actividad diaria para detectar errores u omisiones, etc.

Controles correctivos; facilitan la vuelta a la normalidad cuando se han producido incidencias.

Por ejemplo, la recuperación de un fichero dañado a partir de las copias de seguridad. Es muy importante conocer la relación que existe entre los métodos de control, los objetivos de control y los objetivos de auditoría. Se trata de un tema difícil por el hecho de que, históricamente, cada método de control ha estado asociado unívocamente con un objetivo de control. Por ejemplo, la seguridad de ficheros se conseguía manteniendo la sala de computadoras cerrada con llave. Hoy los controles informáticos han evolucionados hasta convertirse en procesos integrados en los que se atenúan las diferencias entre las categorías tradicionales de controles informáticos. La relación que existe entre los métodos de control y los objetivos de control puede demostrarse mediante el siguiente ejemplo, en el que un mismo conjunto de métodos de control se

utiliza para satisfacer objetivos de control tanto de mantenimiento como de seguridad de los programas:

- Objetivo de control de mantenimiento; asegurar que las modificaciones de los procedimientos programados están adecuadamente diseñadas, probadas, aprobadas e implementadas.
- Objetivos de control de seguridad de programas; garantizar que no se pueden efectuar cambios no autorizados en los procedimientos programados.

La especial atención prestada a la obtención de ventajas competitivas así como a la economía de la TI implica una dependencia creciente de la informática por parte de las organizaciones, como el componente más importante de la estrategia de éstas, lo cual requiere la incorporación de mecanismos de control más poderosos en los computadores y en las redes, tanto en el hardware como en el software. Además, las características estructurales fundamentales de estos controles están evolucionando al mismo paso que las tecnologías de computación y redes.

4.2 Metodología general

En general el proceso seguido en una auditoría es similar al siguiente;

4.2.1 Planificación

En esta etapa se deben realizar algunas actividades como las que a continuación se indica;

Elaboración del plan de auditoría; se deben fijar las fechas y lugares en donde se realizara la auditoría, objetivos y alcance de la misma, normativa de referencia y vigente, los miembros del equipo auditor, medios y recursos necesarios para la ejecución, horario de la auditoría y identificar las personas responsables de cada área.

Conocimiento del negocio del cliente y del sector industrial en que opera*;* para poder planear adecuadamente su trabajo, el auditor deberá obtener suficiente información del negocio del cliente, que le permita comprender los eventos, controles y otras situaciones que pudieren tener un efecto significativo sobre el plan estratégico que la empresa ha proyectado llevar a cabo.

También deberá tener conocimiento sobre el negocio: tipo de negocio, tipos de productos y servicios, sucursales de la compañía y características operativas de la entidad, así como de sus métodos de producción y marketing; tipo de industria, vulnerabilidad de la industria a las condiciones económicas cambiantes, y políticas y prácticas importantes de la industria; estructura de control interno. Asimismo, debe buscar contar con conocimiento sobre la tecnología utilizada, sistemas existentes,

plataformas utilizadas en software base, de aplicación y comunicaciones. Relaciones con empresas externas para su mantenimiento.

Estudiar los documentos de trabajos anteriores; en una auditoría recurrente el auditor podrá examinar sus propios documentos de trabajo para refrescar sus conocimientos acerca del cliente.

Además, los papeles de trabajo podrán revelar áreas de problemas que ocurrieron en auditorías anteriores y que pudieran continuar en el futuro. Respecto a un cliente nuevo podrá obtener información acerca de la industria en que él opera leyendo información de la industria, recabada por la firma de auditores o por publicaciones de la industria.

Para obtener conocimiento acerca del negocio del cliente, el auditor podrá; examinar las informes internos, boletines e información generada por los auditores financieros quienes revisaran escrituras constitutivas así como los estatutos, actas de las asambleas de accionistas y juntas de directores, contratos vigentes importantes, publicaciones del ramo y de la industria respecto a acontecimientos actuales de los negocios y la industria, así el auditor obtendrá conocimiento y copia del plan estratégico que se ha propuesto la empresa con sus respectivos avances y controles que se han aplicado a los diferentes objetivos.

Visita a las instalaciones del cliente; una visita a las instalaciones y oficinas es de gran ayuda para el auditor con el fin de obtener conocimiento acerca de las características de la tecnología de información aplicada, así como las operaciones, conocer los tipos de controles aplicados, instalaciones y los hábitos del personal.

El auditor deberá documentar la información obtenida de las visitas a la planta y a la oficina.

Plantear interrogantes de la administración tecnológica; tanto para el caso de los clientes nuevos como para clientes actuales, establecer conversaciones con sus administradores podrá revelar acontecimientos que afectan a la empresa y que pudieren tener significado en la auditoría. Además, la administración deberá conocer disposiciones gubernamentales y de la industria que pudieran afectar a la empresa. Se podrá también interrogar a la administración respecto al alcance y oportunidad de involucrar al personal del cliente en la elaboración de análisis para el auditor.

Para seleccionar el área tecnológica que se desea auditar se puede considerar;

Los problemas y debilidades conocidas; es decir, identificación de los problemas específicos de las áreas que son puntos de partidas para algunos procesos, la ocurrencia de eventos irregulares en la administración tecnológica, en apariencia nocivos, la sospecha de que existen áreas cerradas ineficientes que pueden generar la necesidad de examinarlas.

Identificar algunos aspectos tecnológicos que no han sido auditadas anteriormente; es decir, otra forma de seleccionar que auditar esta dado por el interés de saber cómo está desempeñando su labor aquellos aspectos que no han sido auditados anteriormente.

Definición del alcance y objetivos; es decir una declaración precisa acerca de lo que la auditoría se propone conseguir y/o a la pregunta que responderá.

Notificación al auditado; se debe comunicar el plan, resolver necesidades especiales y confirmar a los asistentes que acudirán a reuniones de apertura y cierre.

Evaluación de los riesgos; el auditor determina su opinión o conclusión final, con base primordialmente en la evidencia obtenida durante la verificación de que se estén cumpliendo los objetivos propuestos. El objetivo del auditor es restringir el riesgo de auditoría, de manera tal que al concluir su examen, el riesgo de auditoría se encuentre suficientemente bajo.

Los objetivos y metas; es decir, revisar los resultados o efectos que la empresa esperaba alcanzar al momento de poner en marcha un proyecto tecnológico.

Recursos autorizados; revisar la asignación de fondo que autorizo la empresa, para una actividad u proyecto tecnológico, para así poder medir la variación que existe entre las variables costo, tiempo y calidad.

Sistemas y controles existentes; revisar los sistemas que existen en la empresa, ya que son estos los que permitirán que se logren los objetivos planteados, así se podrá medir que las actividades que se realizaron aseguraron el logro de los objetivos.

Auditorias anteriores; revisar que se han aplicado las medidas correctivas que se indicaron en el informe de auditoría antes realizada, es decir, un seguimiento a las actividades implementadas por la empresa.

Conocimiento de la estructura del control interno; revisar el ambiente de control interno de la empresa para verificar que este entrega la confianza y la estructura necesaria para asegurar que las actividades que se desarrollan cumplen el objetivo para que fueran creadas.

Desarrollar listas de verificación; esta etapa permite obtener los últimos datos importantes para la ejecución de la auditoría, como por ejemplo, ¿qué quiero mirar?, ¿qué estoy buscando?, ¿con quién debo hablar?, ¿qué deseo preguntarle?.

Preguntas	Información Requerida	Resultado
¿Qué?	Normas, políticas y procedimientos aplicados a sistemas y controles claves	Conocimiento de la empresa
¿Por qué?	Objetivos, metas y planificación estratégica	Líneas de responsabilidad funcional
¿Cómo?	Entrevistas con funcionarios	Sistemas en general
¿Quién?	División de funciones y responsabilidad	Empresa
¿Dónde?	Observaciones del medio ambiente	Factores internos y externos
¿Cuándo?	Fechas y eventos importantes, variación de tiempo y vida útil	Situaciones importantes

Tabla 3.2
Información requerida en una auditoria TIC

Si bien las actividades relacionadas con la planificación tienen mayor incidencia al inicio del examen, ellas continúan durante la ejecución y aún en la formulación del informe, por cuanto mientras el documento final no sea aprobado y distribuido, su contenido puede estar sujeto a ajustes y reconsideraciones, producto de nuevas decisiones que obligarán a afinar la planificación aún en la fase del informe. Durante esta etapa, el equipo de auditoría se dedica básicamente a obtener una adecuada comprensión y conocimiento de las actividades y operaciones ejecutadas por la empresa a examinar, llevando a cabo ciertas acciones que ayuden a la revisión final, con el objetivo de determinar, entre otros aspectos, los objetivos y alcance del examen, así como las condiciones para realizarlas. En esta etapa el auditor dedica sus mayores esfuerzos a planear la estrategia que utilizará en la auditoría que ejecutará. La cantidad de planeación requerida en un trabajo variará con el tamaño y complejidad del cliente y respecto al conocimiento y experiencia del auditor en referencia al cliente.

4.2.2 Programa

Como última fase de la etapa de la planificación, se deberá confeccionar el programa de auditoría, el que tiene como objetivo reunir evidencias suficientes, pertinentes y válidas para sustentar las conclusiones a emitir respecto del objeto sometido a examen. Este programa servirá de guía de evaluación de los problemas seleccionados en la fase anterior y en la determinación de sus posibles causas y efectos.

La realización del programa de auditoría es de fundamental importancia para el Supervisor y/o Coordinador de la auditoría, porque constituye una evidencia de la

planificación que se realizo y de los procedimientos previstos. Representa además un elemento de control del cumplimiento del mismo.

Se deberá realizar un programa detallado describiendo minuciosamente la forma práctica de aplicar los procedimientos y técnicas de auditoría a los efectos de la ejecución por parte de los auditores integrantes del equipo. El programa deberá incluir como mínimo, los problemas específicos que se están analizando, periodo a que corresponde y área o unidad correspondiente.

A medida que avance el programa de trabajo, el alcance del programa puede variar, de acuerdo a la cantidad y tipo de evidencias que el auditor necesita obtener para llegar a emitir conclusiones debidamente fundadas.

Deberá efectuarse una descripción detallada de todos los procedimientos a efectuar en cada actividad, indicando específicamente si se trata de entrevistas, repaso de antecedentes, exámenes, cálculos, análisis, comparaciones, etc.

Para cada procedimiento se indicará;

- Cuál es el límite de tiempo para realizar cada paso, que período se analizará, cuál es la secuencia de cada procedimiento y su relación con otros.
- Lugar, sucursal, unidad, etc., en cual se realizará el trabajo.
- Deberá indicarse documentación a utilizar y se hará referencia al papel de trabajo a utilizar.
- Deberá indicarse el tiempo asignado (hora hombre) y las personas que la ejecutaran.

La etapa final es ejecutar los procedimientos del programa de auditoría tendiendo a lograr evidencias, que permitan medir el éxito o no de una gestión. Para ello el Coordinador deberá establecer un sistema de medición del rendimiento, siempre que pudiera contar con la información consistente y oportuna.

4.2.3 Ejecución

Empieza con la reunión de apertura, en las instalaciones donde se realizara la auditoría e incluye la recolección y análisis de la información existente. En una reunión de apertura se deben revisar las siguientes situaciones; presentar al equipo auditor y sus responsabilidades, identificar contraparte de la empresa, definir los aspectos tecnológicos y de gestión a auditar, solicitar copias de los documentos de referencia necesarios, establecer reglas para la auditoría, revisión del programa de auditoría y arreglos administrativos.

En otras palabras esta fase involucra básicamente la recopilación de evidencias suficientes, competentes y pertinentes sobre los asuntos más importantes para la

realización de pruebas y análisis de las evidencias, para asegurar el éxito de la auditoría, de modo de acumular bases suficientes para la formulación de observaciones, conclusiones y/o recomendaciones efectivas y debidamente respaldadas, así como para acreditar haber llevado a cabo el examen de acuerdo con los requisitos previamente establecidos.

También en esta etapa se aplican procedimientos y técnicas de auditoría que comprenden: pruebas y evaluación de controles, identificación de hallazgos (condición y criterio), desarrollo de observaciones (incluyendo condición, criterio, causa-efecto, y evaluación de comentarios de la entidad) y comunicación de los resultados a los funcionarios responsables de la empresa evaluada.

Las evidencias objetivas que necesita el auditor, las debe buscar de hechos reales con relación a hechos que estén fuera de lo normal, es fundamental que el auditor este bien informado acerca de los objetivos generales y específicos que el área tecnológica se ha propuesto en su planificación estratégica con el objetivo de estar seguro de que las evidencias que posee son las más correctas para la realización de su trabajo. Para obtener estas evidencias el auditor puede utilizar diferentes medios tales como: entrevistas con los ejecutivos y empleados que desarrollen su actividad en el área a auditar, visión ocular, revisión de documentos, registros de los logs o informes de gestión que posee la empresa, leyes, reglamentos internos, memorias, informes o cualquier otra fuente de información que nos ayude a obtener el conocimiento total del objetivo a ser revisado.

Es posible que se hayan definido indicadores de rendimiento, ya sean cualitativos o cuantitativos los cuales pueden proporcionar al área tecnológica y sus ejecutivos o a al auditor un indicio sobre el grado de eficiencia, economía y efectividad de la ejecución de la gestión tecnológica.

Los indicadores cualitativos; estos no miden numéricamente una actividad, sino que se establecen a partir de los principios generales de una sana administración.

Indicadores cuantitativos; lo primero que deberá determinar el coordinador de la auditoría es si el ente auditado ha desarrollado un sistema de medición del rendimiento.

Si la administración del ente no ha desarrollado dicho sistema, deberá realizarlo el auditor. Para ello deberá desarrollar una batería de indicadores de gestión, debiendo decidir; ¿qué datos reunir?, ¿cómo reunirlos?, ¿cómo asegurar su confiabilidad?.

Indicadores de gestión; se busca asegurar la veracidad y confiabilidad de los antecedentes reunidos y confirmar que la información obtenida responda a la realidad de la empresa por área de estudio, debiendo el coordinador definir el nivel de

verificación que se estimará necesario, debiendo documentarse los datos incluidos, lo cálculos y las pruebas sustantivas, en papeles de trabajo respectivo.

Normas de rendimiento; se refieren a mediciones cuantitativas o cualitativas de cuál es el nivel que se considera como deseado o esperado, de una actividad. Se destaca la conveniencia de tratar de obtener la aprobación del ente auditado sobre las normas de rendimiento que se aplican. Si ello no ocurre, en el informe deberá indicarse tal situación, las opiniones del ente auditado y los fundamentos de la norma aplicada por parte del auditor.

Análisis y evaluación de evidencias*;* una vez determinadas las desviaciones cualitativas y cuantitativas respecto de los criterios o normas, deberá analizar y evaluar las evidencias para desarrollar los hallazgos.

Diagnóstico; la evidencia y hallazgos reunidos en la fase anterior, analizados y evaluados, permiten al auditor tener un panorama preciso de la realidad auditada y poder, en consecuencia, emitir un diagnóstico. Los hallazgos responden a la pregunta crítica de cuán bien o no está funcionando una actividad. Esto significa que el coordinador deberá comparar el rendimiento real con las normas para determinar el nivel de eficiencia, eficacia y economía de la gestión.

Todos los hallazgos negativos o positivos detectados deben tener cabida en el diagnóstico, determinándose las causas que los determinaron. Para facilitar la redacción posterior del informe, deberá confeccionarse en los papeles de trabajo una misma forma de anotación de los hallazgos;

Condición; es el nivel real del rendimiento obtenido.

Criterio; es el nivel deseado, esperado o planificado del rendimiento, veles decir la norma de rendimiento.

Causa; los factores determinantes de la variación del rendimiento (favorable o desfavorable).

Efecto; el impacto de la variación en el rendimiento, medido en unidades monetarias, cuando sea posible.

Recomendación; mediante éstas se intentará superar los problemas encontrados, evitar problemas futuros y consecuencias, con la finalidad de que la entidad auditada adopte las medidas recomendadas. Las recomendaciones deben enfocar aspectos significativos de la organización y de su gestión, además ser técnica y financieramente factibles de aplicar en los entes, de acuerdo a sus propias características.

Opinión del ente auditado; es un elemento útil para ratificar o rectificar las aprensiones del diagnóstico. Asimismo permite al ente auditado formular sus descargas.

Pronóstico; los auditores responsables de cada hallazgo consultarán a los afectados por las observaciones, salvo caso de fraudes detectados o malversaciones de fondos, solicitando su opinión sobre los hallazgos y recomendaciones formuladas, consignándose en los papeles de trabajo. El coordinador deberá discutir el borrador del informe con los máximos niveles de cara área, en reuniones, a las cuales deberá concurrir el personal a cargo de los sectores involucrados por las observaciones o recomendaciones. De esta manera se asegurarán de no haber omitido ningún antecedente o dejado sin considerar determinada evidencia. Además, tratarán de obtener información sobre la evolución del marco externo que más afecte a la organización a mediano o largo plazo, con el objetivo de proyectar las principales variables que ella maneja (pronóstico) a fin de confirmar, modificar o descartar determinadas recomendaciones. De los resultados de cada reunión se confeccionará una minuta que deberá estar firmada por cada uno de los participantes.

4.2.4 Informe

En esta etapa se informan las conclusiones a las cuales ha llegado el equipo de auditores, respecto de su objeto revisado, abarca la reunión de cierre con los máximos directivos de la empresa, y la emisión del informe final y formal de la auditoría.

Los informes de auditoría de gestión tienen características distintas del informe tradicional de auditoría de estados financieros. Las auditorías de gestión cubren una amplia gama de metas y objetivos, como resultados de lo cual es necesario normalizar, en lo posible, la estructura de los mismos.

Otra importante característica de los informes de auditoría de gestión es la ausencia en los mismos de cualquier opinión global respecto a los resultados de la auditoría o la actividad examinada. Excepto en muy raras circunstancias en las que se hayan aceptado normas de rendimiento tan generales que representen una base indiscutible para llegar a una opinión sobre operaciones globales, debería esperarse que el informe de auditoría de gestión se limite únicamente a las observaciones de hallazgos referentes a las situaciones encontradas durante la auditoría.

Informe de avance; es un informe de tipo administrativo que emite el coordinador con el objetivo de posibilitar una adecuada supervisión y efectuar oportunamente los ajustes que se estimen pertinentes. Los informes de avance, en general, se emitirán comparando un plan o presupuesto con las tareas realizadas en terreno. Inicialmente con el presupuesto de auditoría, a partir de la finalización de la etapa de estudio preliminar, con la planificación de recursos y desde la etapa de medición de rendimientos con el programa de auditoría. En términos generales el informe se emitirá

teniendo en cuenta el último plan en vigencia. Los informes de avance se emitirán con periodicidad, aunque de acuerdo a cada caso la supervisión podrá ampliar o disminuir ese lapso. El informe de avance debe contener;

Datos fijos; indicarán la organización, número de informe, período considerado, coordinador, etapa de auditoría y toda la información del género que surgirá de las anotaciones que se realizan en los papeles de trabajo.

Objetivo; se indicarán los objetivos detallados de la auditoría (última versión).

Periodo bajo examen; se consignará el periodo bajo examen.

Información de avance; contendrán a nivel de proyecto un detalle de las actividades programadas, el avance en el período estipulado y el avance total a la fecha a la cual está referido. Se puede utilizar en este punto diagramas de avance de tareas (barras horizontales o cartas Gantt). Como mínimo el informe deberá incluir como información específica;

- *Plan estratégico y presupuesto;* descripción del mecanismo de su formulación, elevación, aprobación, ejecución y seguimiento. Análisis de los principales rubros de ingresos, egresos a la fecha del informe y revisión comparativa con años anteriores.
- *Análisis del negocio;* se dará una idea global del negocio. Se explicarán las actividades tecnológicas significativas y aquéllas que requieren de atención, toda esta información estará disponible a la fecha del informe.
- *Áreas críticas;* se sugerirá un estudio más profundo sobre aquellas áreas de TIC, subáreas y actividades que se hayan detectado como críticas (con problemas actuales o potenciales).
- *Sistemas de aplicación;* se detallarán los sistemas de información que dispone la organización. En particular aquellos que apoya operaciones importantes de la organización y que puede interesar precisar, como ser un sistema de información en base de datos contables y extra contables que permita además apoyar la toma de decisiones de la alta gerencia y permita la auditoría interna y externa de la gestión empresarial contar con información en línea.
- *Otra información relevante;* se indicará a continuación cualquier otro dato o información considerada de interés por el coordinador para el desarrollo de la auditoría.

Informe final; como resultado de las tareas de auditoría de gestión se emitirá al finalizar la misma un informe, que detalle los resultados obtenidos en las tareas de auditoría planificadas.

Propósito; describir porqué se efectuó la auditoría y se obtiene de la última versión del programa de auditoría.

Alcance; se señalará con precisión el ámbito sometido a la evaluación (toda la organización, un área, una actividad, un contrato. etc.) y la muestra analizada. Se considerará, además las razones que hayan podido impedir una plena y libre realización de la auditoría. Se indicará asimismo el tipo de información utilizada (contable, extra contable, estadística, proyectada, etc.)

Metodología; se efectuará una descripción de la metodología utilizada para realizar el examen.

Antecedentes; se describe la organización, proyecto o actividad auditada. Deberá limitarse únicamente a la información necesaria para comprender loa hallazgos y recomendaciones presentadas en el informe.

Información específica; deben dejarse establecidos los hechos y circunstancias que caracterizan la situación en estudio (hallazgos) y sus aspectos positivos o negativos, latentes y evidentes.

Debe contener fundamentalmente información conceptual y conclusiones del análisis. Es conveniente que los detalles analíticos se muestren como anexos. Como mínimo el informe deberá incluir como información específica;

- *Plan estratégico y presupuesto;* análisis de los principales aspectos tecnológicos a la fecha del informe y compararlo con años anteriores. Cuantificación de metas y objetivos incluidos en la planificación estratégica de la empresa.
- *Análisis del negocio; por excepción,* si hay modificaciones relevantes respecto del último informe de avance.
- *Áreas críticas seleccionadas;* se deben extraer del informe de avance y se explicará su funcionamiento, problemas detectados, los problemas comprobables, la evidencia recolectada, pruebas desarrolladas, comentarios resultantes y conclusiones alcanzadas. En el análisis realizado se utilizarán los indicadores cuantitativos y cualitativos.
- *Sistemas de información;* se detallarán los sistemas de información gerencial de que se dispone en la organización.
- *Indicadores de rendimiento;* los sistema de información, deben contar con indicadores que permitan analizar la confiabilidad y oportunidad de los datos. En el informe se consignará el resultado de los indicadores áreas de TIC críticas. En caso contrario, el equipo incluirá un conjunto de indicadores de las áreas críticas. Se informará la opinión del ente auditado respecto a los indicadores utilizados, en el caso de no compartir la inclusión de determinados ratios.

Hallazgos, conclusiones y recomendaciones; se obtendrá la información de los papeles de trabajos en los que se detalla los hallazgos encontrados, se indicará para cada

hallazgo la condición, criterio, causa efecto o conclusión, y la recomendación que resulta del hallazgo.

La conclusión es el resultado obtenido como consecuencia del análisis de cada hallazgo específico. El informe deberá contener conclusiones cuando los objetivos de auditoría lo requieren. Las conclusiones deberán formularse explícitamente y no dejar que sean deducidas por los lectores.

Las recomendaciones son medidas que a juicio del grupo de auditoría permitirán a la organización lograr mayor eficacia, economía y eficiencia en sus objetivos propuestos, solucionando sus actuales problemas, vaticinando otros y aprovechando al máximo las posibilidades que el medio externo y sus propios recursos le ofrecen.

Organización auditada; la reunión de cierre tiene como objetivo presentar las observaciones de la auditoría a los representantes de la empresa auditada, de tal modo que se asegure que se han entendido claramente los resultados obtenidos, el auditor encargado presenta las observaciones teniendo en cuenta el grado de importancia de cada una de ellas, se le agradece al personal por su colaboración y apoyo para poder ejecutar de la mejor forma posible dicha auditoría.

4.2.5 Seguimiento

La auditoría no será efectiva si ha concluido con un buen informe y no se le efectúa un seguimiento para verificar, que la empresa auditada ha puesto en marcha las observaciones y recomendaciones que le ha propuesto el equipo auditor. El método para efectuar el seguimiento, dependerá del tipo de observación, y también de la importancia y materialidad de las observaciones y recomendaciones.

5 Bibliografía

- Arens Alvin A.; James K. Loebbecke. Auditoria un enfoque Integral, Editorial Prentice Hall Hispanoamericana, S.A., Sexta edición, México, 1996
- Mantilla Blanco, Samuel Alberto. Auditoria de Información Financiera, Editorial Kimpres Ltda., Primera edición, Bogotá, 2009
- Estupiñan Gaitan, Rodrigo. Administración o Gestión de Riesgos E.R.M. y la auditoría interna. Litoperla Impresores Ltda. Primera edición, Bogotá, 2006
- Bolivia, Contraloría General del Estado. (2006). Manual de Normas de Auditoría Gubernamental. Obtenida el 1 de Septiembre de 2011, de http://www.cge.gob.bo
- Normas de Auditoria. Obtenida el 17 de Septiembre de 2011, de http://www.auditorescontadoresbolivia.org/aprobadas.php
- Normas de Información Financiera. Obtenida el 17 de Septiembre de 2011, de http://www.auditorescontadoresbolivia.org/aprobadas.php
- Interpretaciones de Normas de Información Financiera. Obtenida el 17 de Septiembre de 2011, de http://www.auditorescontadoresbolivia.org/aprobadas.php
- Mantilla Blanco, Samuel Alberto (2009). Auditoria de Información Financiera (1 Ed). Colombia: ECOE
- Bell, Peecher, Solomon, Marrs, Thomas (2007). Auditoria basada en riesgos (1 Ed). Colombia: ECOE
- Estándar COBIT. ISACA. Obtenida el 17 de Septiembre de 2011, de http://www.isaca.org/
- Norma de auditoría. Contraloría General de la República de Chile. Obtenida el 1 de agosto de 2011, de http://www.contraloria.cl
- Dirección de la Auditoria de Tecnologías de Información. Instituto de Auditores Internos de España.
- Echenique, García José Antonio. Auditoría en Informática, Editorial McGrawHill, S.A., Segunda edición, México, 2001