UNIVERSIDAD DE MENDOZA
FACULTAD DE INGENIERIA
Asignatura: Auditoría de Sistemas.
Profesor Titular: Dr. Ing. Raúl Moralejo.
JTP: Ing. Julieta Suarez.

CONTENIDOS MÍNIMOS

UNIDAD 1: CONCEPTOS Y MODELOS/ESTÁNDARES DE AUDITORÍA

Antecedentes

Antes de profundizar en definiciones y en características de la auditoría, me gustaría compartir una historia que habla sobre sus orígenes. Cierta o falsa, como pueden ser muchas de las historias del mundo, ésta en particular presenta mucha coherencia con la evolución que ha experimentado la auditoría y con los vicios que la han perseguido y la persiguen desde hace muchos años.

En los tiempos de la colonia británica en Norte América y al igual que todas las colonias europeas en el resto del mundo, los ingleses veían al nuevo continente como una fuente casi inagotable de riqueza que utilizaban para alimentar sus arcas y financiar nuevas aventuras y conquistas alrededor del globo.
Muchos ingleses de la comunidad de "inversionistas" en América, tenían fuertes intereses económicos en Estados Unidos, pero en aquellos tiempos no existían medios de transporte ni de comunicación como con los que contamos hoy en día. Esto presentaba el problema de que las operaciones económicas fueran manipuladas en perjuicio de los dueños británicos.
Considerando esto, se pensó que sería conveniente contar con alguna persona o personas de confianza que mantuviesen al tanto de los acontecimientos a los dueños "legítimos" de la riqueza que se generaba en América y que debería ser reportada y enviada al Reino Británico.
Estas personas fueron los primeros auditores, de hecho la palabra auditor tiene su origen en la palabra inglesa *Auditory*, que es el nombre de un nervio del aparato auditivo, llamado también "octavo nervio". Este nervio, adicionalmente a su función auditiva, es el que permite mantener el sentido de equilibrio al ser humano.

Haciendo un paralelismo, podemos ver la relación que tiene este nervio con la función original del auditor y su primera encomienda, es decir informar sobre cualquier irregularidad en las operaciones y mantener un balance adecuado de las operaciones.

Este antecedente explica el por qué los auditores han sido "catalogados" a través del tiempo como personajes siniestros que se dedican a identificar todo lo que esté mal, para denunciarlo y alertar a quien deba ser alertado.

Hoy en día, debemos pensar en el auditor, como un elemento imprescindible para una sana operación de las empresas. Su rol ha pasado de ser un detector de problemas, aun identificador de oportunidades y emisor de propuestas de valor. Un auditor, hoy en día, no puede concebirse a sí mismo simplemente como el responsable de identificar riesgos en la operación de una empresa, aunque ciertamente la identificación de riesgos sigue siendo una parte importante de sus actividades, su compromiso profesional va más allá de fungir como un mecanismo detectivo.

Definición

Antes de proponer una definición de auditoría en tecnología de información, vale la pena conocer una definición de auditoría general, ya que la primera "hereda" muchos de los preceptos de la segunda, pues en realidad es sólo una especialidad de auditoría.

Podemos entender a la auditoría como ***la disciplina que mediante técnicas y procedimientos aplicados a una organización por personas independientes a la operación de la misma, evalúa el cumplimiento de los objetivos institucionales, emite una opinión al respecto y efectúa recomendaciones para mejorar el nivel de cumplimiento de dichos objetivos.***

Cabe mencionar que dependiendo del tipo de auditoría de que se trate, las definiciones reflejarán las particularidades correspondientes, fundamentalmente alineadas a los objetivos que cada auditoría persiga.

Como en toda definición, lo más importante es identificar las ideas fundamentales de la misma:

- **Es una disciplina**, lo cual implica que su desarrollo está regido por reglas, técnicas y principios formales que buscan su estandarización y aceptación general.
- **Es aplicada por personas independientes a la operación**, lo cual significa que quien desarrolle un trabajo de auditoría debe presentar una clara independencia de criterio y libertad para expresar su juicio sin existir ningún tipo de conflicto de intereses con respecto a los responsables de la operación de la empresa.
- **Busca evaluar el cumplimiento de los objetivos institucionales**, se considera necesario resaltar la importancia y el compromiso que tiene la función de auditoría en las organizaciones. La auditoría debe tener una participación contundente en el logro de los objetivos de una organización y por ende estar comprometida con ellos hasta sus últimas consecuencias.
- **Emite un juicio sobre el cumplimiento de los objetivos**, esta idea indica que el auditor tiene la responsabilidad de emitir su opinión sobre el nivel de cumplimiento de los objetivos institucionales evaluados. "El auditor debe ampliar su visión y adoptar una actitud proactiva, aportando un valor agregado a su función."
- **Efectúa recomendaciones**, esta última idea representa la aportación intelectual que el auditor debe realizar a la empresa con el propósito de apoyar el cumplimiento de sus objetivos institucionales. El compromiso del auditor no debe limitarse a opinar sobre dichos objetivos, sino que debe contribuir con sugerencias sobre mejoras a los métodos de trabajo, a la estructura de la organización, el empleo competitivo y eficiente de tecnología y aspectos relacionados con recursos humanos, entre otros elementos.

Por tratarse de una especialización (de la auditoría general), la auditoría de tecnología de información hereda todas las características de la definición básica de auditoría que hemos visto.

Podríamos considerar que la auditoría de tecnología de información ***es la disciplina que mediante técnicas y procedimientos aplicados en una organización por personal independiente a la operación de la misma, evalúa la función de tecnología de información y su aportación al cumplimiento de los objetivos institucionales; emite una opinión al respecto y efectúa recomendaciones para mejorar el nivel de apoyo al cumplimiento de dichos objetivos.***

Evidentemente, este tipo de auditoría se enfocará de manera específica a los aspectos relativos a sistemas de información (normalmente con un alto componente de tecnología) pero sin perder de vista su contexto institucional, mismo que dará los elementos para proporcionar un valor agregado en sus servicios.

Por último, no podemos dejar de mencionar la definición clásica y resumida de auditoría. La auditoría es un control por excepción que mide otros controles, su eficacia y su eficiencia.
Se puede decir que la auditoría es el "Control de controles"

Clasificación

Existen varias formas de clasificar a la auditoría; simplemente si pensamos en las áreas de especialización, éstas nos darían una clasificación extensa y válida. Sin embargo, sólo mencionaremos dos tipos, las cuales pueden aportar elementos de interés en su posterior estudio.

Clasificación con base en quien realiza la auditoría

La clasificación presenta dos grupos claramente definidos, la auditoría externa y la auditoría interna.

Auditoría externa: es aquella que realiza un auditor o grupo de auditores que son independientes a la empresa auditada y su relación con la misma se limita a un contrato o convenio de servicios profesionales establecido entre la empresa auditada y su auditor.

La auditoría externa es una actividad profesional sumamente antigua y exitosa, algunas firmas tienen más de 100 años de operaciones.
El éxito de este tipo de organizaciones se debe a varios factores, de entre los cuales sobresalen los siguientes:

a) Las firmas de auditores independientes, a través de los años, han alcanzado un elevado nivel técnico, han acumulado experiencia profesional en distintas industrias y han perfeccionado eficientes métodos de trabajo que difícilmente podrían ser desarrollados en forma interna por la mayoría de las empresas.
b) El hecho de ser independientes a las empresas que auditan, les otorga un mayor nivel de credibilidad a su opinión profesional, por lo que muchas empresas recurren a sus servicios como forma de contar con un aval reconocido por la sociedad y autoridades.
c) Indudablemente que otro factor determinante en el espectacular éxito de las firmas de auditores externos, es el hecho de que muchos gobiernos, a través de su legislación tributaria o de los requisitos de participación en Bolsa de Valores, hacen obligatorio que las empresas utilicen los servicios de auditores independientes para presentar estados financieros dictaminados o informes especiales.

Por muchos años, unas cuantas firmas dominaron el panorama mundial de la auditoría externa: Arthur Andersen, Price Waterhouse, Arthur Young, Coopers and Lybrand, Deloitte, Haskings and Sells, Touch Ross, Peat Marwick y Ernst and Whinney.
A finales de los ochentas comenzaron una serie de fusiones entre las firmas, respondiendo a las necesidades de globalización y a las agresivas estrategiss de mercado que han caracterizado a estas organizaciones. Actualmente, existen sólo cinco de las ocho firmas originales, las cuales son: Arthur Andersen, PriceWaterhouseCoopers, Ernst and Young, KPMG – Peat Marwick y Deloitte and Touch.

Auditoría Interna: es aquella que realiza un auditor o grupo de auditores empleados formalmente por una empresa, pero que sus funciones son ajenas totalmente a la

operación de la misma. La auditoría interna se considera uno de los elementos fundamentales de un buen sistema de administración.

Una organización puede crear un departamento de auditoría interna cuyos integrantes trabajarán permanentemente en dicha organización, pero sus actividades se limitarán a las directamente relacionadas con auditoría, sin asumir responsabilidades en otras áreas o actividades de la empresa pues esto estaría en conflicto con el requisito de independencia que debe tener todo auditor.

Los auditores internos están limitados para efectuar cierto tipo de trabajo, tal como la dictaminación de estados financieros, primordialmente porque su opinión no tiene valor oficial para las autoridades. Por tal razón y por el nivel de conocimiento que pueden adquirir sobre las operaciones de la empresa, los auditores internos se abocan primordialmente a funciones relacionadas con la eficiencia operativa y con el cumplimiento de normatividad que sea aplicable a la empresa.

Los auditores internos reportan normalmente al Consejo de Administración o al presidente de éste, ya que las funciones del director general son objeto de evaluación por parte del auditor.
Una derivación de la auditoría interna que comparte algunas características con la externa es el **outsourcing de auditoría interna**. Este concepto, consiste en que una empresa decide crear un área de auditoría interna, pero no con empleados propios de la organización, sino mediante la contratación de este servicio a una firma profesional independiente. La firma que realiza el outsourcing desempeña todas las labores y asume toda la responsabilidad de una auditoría interna, trabajando prácticamente tiempo completo en la empresa auditada.

Este esquema se diferencia de la auditoría externa en el sentido de que se está imposibilitado para emitir informes y dictámenes que tengan reconocimiento oficial por parte de las autoridades fiscales y bursátiles.

Clasificación con base en los objetivos que se persiguen

Auditoría financiera: se realiza con el objetivo primario de emitir una opinión sobre los estados financieros de una organización; consecuentemente se dirige a la evaluación de aspectos de integridad y veracidad de la información. Esta opinión se conoce como dictaminación de estados financieros y , para efectos legales, sólo es válida cuando es emitida por auditores externos.

Auditoría administrativa: se orienta a la evaluación de aspectos relacionados con la eficiencia y productividad de las operaciones de una empresa. Este tipo de auditoría puede ser desempeñada tanto por auditores externos como auditores internos.

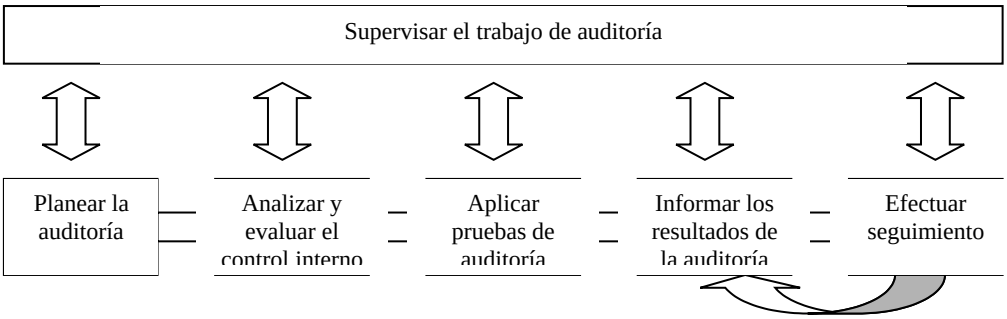
Auditoría integral: se realiza con el fin de evaluar en su totalidad los objetivos que existen en una organización, es decir, los relacionados con información financiera, salvaguarda de activos, eficiencia y normatividad (entre otros). Este tipo de auditoría

puede ser realizada tanto por auditores externos, como auditores internos. Sin embargo, debido a su estrecha familiarización con la empresa, los auditores internos cuentan con mejores elementos para efectuar este trabajo en forma eficiente.

Como se puede ver, en ninguna de las clasificaciones anteriores se mencionó de manera específica a la auditoría en tecnología de información.
Lo anterior se debe a que esta disciplina no es excluyente de ninguna de las auditorías mencionadas, por el contrario, todas ellas pueden (y normalmente lo hacen) integrar la auditoría en tecnología de información para efectuar revisiones específicas derivadas del empleo de tecnología en las empresas.

Proceso

La auditoría en forma general e independientemente del tipo de auditoría de que se trate, desarrolla las actividades que se muestran en la siguiente figura y que se describen posteriormente.



Planear la auditoría

Aún cuando la planeación se presenta como la primera actividad de la auditoría, en realidad el auditor debe haber recibido previamente a la planeación, un requerimiento para desarrollar un trabajo de auditoría; en este requerimiento se deben especificar los objetivos del trabajo y las condiciones generales del mismo. Con esta información, el auditor debe proceder a obtener un conocimiento general de la empresa que va a ser auditada, sus características de negocio, su infraestructura tecnológica, sus sistemas de información, sus áreas de riesgo, sus objetivos estratégicos y cualquier asunto de interés específico sobre la auditoría a realizar.

Con esta información, el auditor debe realizar un trabajo de planeación en el que determine el tipo de procedimientos de revisión que deberá emplear, el personal responsable del desarrollo de las actividades y las fechas y duración aproximada del trabajo.

Analizar y evaluar el control interno

Con la información contenida en el plan de auditoría, el auditor preparará programas de trabajo específicos que le permitan obtener información sobre los procedimientos de control (elementos de administración) que la empresa tiene establecidos para apoyar sus objetivos de negocio. Esta información es obtenida mediante entrevistas, observación o inspección documental y debe ser documentada para servir como referencia y como fuente de consulta.

La información obtenida deberá ser empleada para fundamentar un análisis sobre la probable efectividad y eficiencia del sistema de control para lograr sus objetivos, cualesquiera que estos sean (integridad de la información, salvaguarda de activos, continuidad de operaciones, imagen, posicionamiento competitivo, etc.).

Aquí existe una premisa: *Entre mejor sea el sistema de control, mayor será la probabilidad de que los objetivos sean alcanzados en forma satisfactoria.*

Aplicar pruebas de auditoría

Con base en el análisis del control interno de la empresa, el auditor puede optar por aplicar dos tipos de pruebas. Las primeras se conocen como "pruebas de cumplimiento" y permiten verificar la efectividad de los procedimientos de control es decir, son técnicas de prueba que evalúan los "procesos de trabajo" existentes en la empresa.
Los resultados de estas pruebas podrán ratificar o rectificar el juicio preliminar sobre lo adecuado del control y sentar las bases para que el auditor aplique un segundo tipo de pruebas, estas últimas llamadas "pruebas sustantivas".
Las pruebas sustantivas están orientadas más bien a los "productos" de los procesos de trabajo y no a los procesos en sí. Los resultados de los pruebas sustantivas generalmente se expresan en información.

Específicamente cuando se trata de una auditoría en TI, las pruebas pueden implicar la utilización de sistemas de software desarrollados específicamente para tal efecto, ya sea para efectuar pruebas a la información (paquetes como ACL, IDEA, etc.), o para efectuar pruebas a los componentes de la infraestructura de la tecnología.

Los resultados de las pruebas deben proporcionar al auditor elementos para fundamentar dos tipos de conclusiones:

a) Sobre lo adecuado y confiable del sistema de control interno (los procesos de trabajo) de la empresa. Esta conclusión se fundamenta en gran medida en los resultados de las pruebas de cumplimiento.
b) Sobre la medida en que han alcanzado los objetivos de la empresa a cuyo cumplimiento están orientados los procedimientos de control. Esta conclusión se fundamenta en los resultados de las pruebas sustantivas.

Informar sobre los resultados de la auditoría

Una vez realizadas las pruebas y analizados los resultados, el auditor debe preparar un informe sobre su trabajo, los resultados del mismo, las conclusiones correspondientes y las sugerencias que el auditor presente para mejorar las deficiencias encontradas. El auditor debe indicar claramente cuál es el nivel de involucramiento y responsabilidad en el trabajo realizado.

Dependiendo de los resultados y objetivos de su revisión, el auditor puede abstenerse de presentar una opinión cuando considere que no tiene elementos suficientes para sustentarla o puede presentar una opinión negativa, es decir, informar específicamente que los objetivos evaluados no han sido alcanzados en forma satisfactoria.

El auditor también debe informar si se presentaron limitaciones importantes que evitaran que realizara su trabajo de acuerdo con las normas establecidas por su profesión.

Efectuar su seguimiento

Típicamente, una revisión arroja deficiencias o debilidades de control en la empresa, las que a su vez pueden representar oportunidades de mejora. Con base en estas oportunidades, el auditor emite recomendaciones que se convierten en compromisos para los responsables de las áreas auditadas.

El auditor deberá efectuar revisiones de seguimiento para evaluar el nivel de cumplimiento de dichos compromisos o el impacto que esto pueda tener para la empresa.
Los resultados de este tipo de trabajos también se deberán informar de manera adecuada a quién corresponda.

Supervisar el trabajo

En todo momento el auditor deberá ejercer una adecuada supervisión del trabajo, especialmente de aquel realizado por personal con menor experiencia, ya que en última instancia, el auditor será el principal responsable de su trabajo ante cualquier persona que lo utilice.

Procedimientos

Los procedimientos de auditoría representan al conjunto de técnicas de trabajo que el auditor aplica en el desarrollo de sus actividades. Los procedimientos son aplicados a los largo de todo el proceso de auditoría. Sin embargo, la fase en donde su empleo se vuelve característico es la aplicación de las pruebas, ya sea pruebas de cumplimento o sustantivas.
En realidad, los procedimientos pueden ser muy variados como distintas sean las empresas y proyectos que se desarrollen. Sin embargo, existe un grupo de técnicas básicas que el auditor utiliza adecuándolas a cada caso en particular.

Clasificaremos a las técnicas de auditoría en los siguientes grupos:

- **Técnicas manuales:** Estas técnicas son en esencia las mismas que se aplican en otros tipos de auditoría u otras actividades que requieren una labor de análisis y/o evaluación. Las técnicas más utilizadas son las siguientes:

    a) **Inspección documental**. Esta técnica se utiliza cuando es necesario efectuar el análisis de procedimientos de control que implican documentación, ya sea la documentación del propio procedimiento o la documentación de sus resultados. Ejemplos: inspección de manuales, actas de comités, contratos, documentación de sistemas, planes de contingencia, etc.
    b) **Entrevistas.** Esta es una de las técnicas más ampliamente utilizada por el auditor y consiste simplemente en la obtención de información mediante entrevistas a personal que posea conocimiento o experiencia de interés para los objetivos del proyecto de auditoría.
    c) **Encuestas.** Esta es una técnica poco utilizada actualmente en las auditorías. Su propósito es la obtención de información mediante la aplicación de cuestionarios predefinidos a un grupo de personas sobre un aspecto particular. Típicamente, esta técnica es utilizada para determinar niveles de satisfacción respecto al servicio proporcionado por un sistema o por el área de Sistemas o por servicios prestados por la empresa que empleen un soporte de tecnología de información.
    d) **Sesiones facilitadas.** Esta es otra técnica pocas veces utilizada. Consiste en el desarrollo de una sesión de trabajo en la cual un “facilitador” aplica técnicas específicas (técnicas de facilitación) para obtener información de un grupo de expertos en algún tema. Este tipo de técnica puede emplearse para validar elementos de estrategia de la empresa, proponer soluciones a problemas específicos o para obtener conocimiento sobre segmentos de procesos que no se encuentran debidamente documentados y/o en los cuales participan varios departamentos.
    e) **Certificación.** Esta es una técnica que se utiliza para apoyar el juicio del auditor con la opinión de algún experto.
    f) **Confirmación.** Esta técnica se utiliza para confirmar información que la empresa presenta, mediante la respuesta de una persona ajena a la

compañía, como puede ser un cliente, un proveedor o un acreedor. Cuando esta confirmación es masiva, se conoce como “circularización”.

g) **Técnicas de ingeniería de información.** Estas técnicas se emplean tanto en la evaluación de controles generales como en los controles específicos. Evidentemente, su empleo requiere de conocimientos de tecnología en información , mismos que serán necesarios para evaluar los sistemas en sí y los procesos de desarrollo, de mantenimiento y de integración de paquetes, entre otros.

Estas técnicas han sido incluidas bajo la clasificación de “técnicas manuales” porque no es indispensable un soporte automatizado para su aplicación. Sin embargo, es muy probable que se apliquen mediante el uso de herramientas CASE (Computer Aided Software Engineering).

- **Técnicas aplicadas a la tecnología:** Estas técnicas son aplicadas en un ambiente de tecnología con el propósito de evaluar el funcionamiento de los componentes tecnológicos del control interno y no sus productos o resultados. Ejemplos: evaluación de la capacidad para manejar altos volúmenes de transacciones de un computador, la velocidad y consistencia de transmisión de un canal de comunicación, la efectividad de una planta de energía alterna, etc.

- **Técnicas asistidas por tecnología:** Este tipo de técnicas utilizan a la tecnología como un habilitador, pero su objetivo no es evaluar a la tecnología en sí sino la efectividad del control interno mediante el examen de sus productos o resultados. Estas técnicas son conocidas como CAATs (Computer Assisted Audit Techniques) y pueden ser implementadas básicamente de dos formas:
    1. utilizando el equipo de cómputo e instalaciones de la propia empresa mediante programas de utilería, reporteadores, lenguajes de programación o software especializado de auditoría, o
    2. utilizando paquetes de auditoría que operan en microcomputadores y que “importan” archivos de datos del computador central (tales como, ACL Plus, IDEA, APPLAUDE-Audit, PANAUDIT Plus, PC-FOCAUDIT, CARS, etc.).

  Independientemente de la forma de implementación, las técnicas de auditoría más utilizadas son las siguientes:

  a) **Comparación de programas.** Esta técnica se emplea para efectuar una comparación de código (fuente, objeto o comandos de proceso –JCL-) entre la versión de un programa catalogado en operación y la versión de un programa que ha sido analizado y que debe permanecer en custodia para garantizar que no ha sido modificado en forma indebida.
  b) **Mapeo y rastreo de programas.** Esta técnica emplea un software especializado que permite analizar los programas en ejecución , indicando el número de veces que cada línea de código es procesada e indicando también las condiciones de las variables de memoria que estuvieron presentes. También indica las líneas de código que no se utilizan durante el

proceso. Esta técnica es especialmente útil para detectar problemas como las “bombas de tiempo”.

c) **Análisis de código de programas.** Esta técnica se emplea para analizar los programas de una aplicación. El análisis puede efectuarse en forma manual (análisis de código fuente de los programas) o utilizando software especial (análisis tanto de código fuente como de código ejecutable). Esta técnica es útil para obtener un conocimiento del funcionamiento de un sistema o para verificar que el programa incluye todos y exclusivamente los procesos autorizados por el usuario de la aplicación.

d) **Datos de prueba.** Esta técnica se emplea para verificar que los procedimientos de control incluidos en los programas de una aplicación funcionan correctamente. Los datos de prueba consisten en la preparación de una serie de transacciones que contienen tanto datos correctos como datos con errores predeterminados. Estas transacciones son alimentadas al sistema con la intención de que los filtros de control detecten los errores, al mismo tiempo que procesan adecuadamente la información que no contiene errores.

e) **Datos de prueba integrados** (ITF – Integrated Test Facilities). Esta es un técnica muy similar a la anterior, con la diferencia de que ésta debe crear una entidad “falsa” dentro de los sistemas de información. En los datos de prueba se trabaja normalmente con copias de programas y con respaldo de archivos.

f) **Análisis de bitácoras.** Existen varios tipos de bitácoras que pueden ser analizadas por el auditor, ya sea en forma manual o por medio de programas especializados, tales como bitácoras de uso del equipo, bitácoras de accesos no autorizados, bitácoras de procesos ejecutados, etc. Las bitácoras contienen información histórica que permite al auditor efectuar análisis de utilización de recursos o detectar desviaciones a políticas o procedimientos de control establecidos.

g) **Simulación paralela.** Esta es una técnica y consiste en desarrollar programas o módulos que emulen a los programas de un sistema en producción. El objetivo es procesar los dos programas o módulos en forma paralela e identificar diferencias entre los resultados de ambos.

h) **Código integrado** (embedded code). Tal vez esta es la técnica más representativa de lo que debería ser una auditoría permanente, ya que se trata precisamente de incluir en los programas de un sistema rutinas con técnicas de auditoría, las cuales no tienen otra función más que detectar anomalías o desviaciones en los parámetros o criterios aceptados por el sistema.

i) **Análisis de datos.** Esta técnica permite efectuar análisis de la información almacenada en archivos o bases de datos. Para este efecto se pueden utilizar queries, comandos SQL o lenguajes de desarrollo. El objetivo es identificar cualquier desviación a los parámetros permitidos para los registros de la base de datos, efectuar cálculos utilizando los datos contenidos en los archivos y/o generar reportes de auditoría.

j) **Programas de utilerías** (utility programs). Esta, más que una técnica en sí es la posibilidad de emplear los propios recursos de la instalación con fines

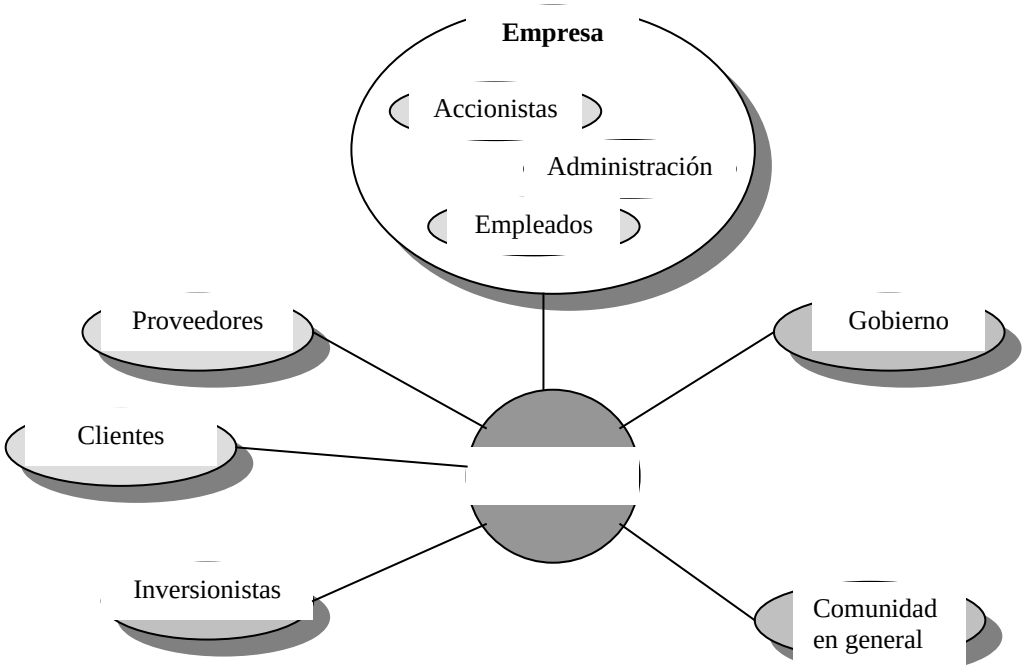
de auditoría, tales como los comandos COPY, DUMP, SORT o reporteadores para explorar archivos.

Compromiso ético y Naturaleza ecléctica

Compromiso ético

La auditoría es una actividad profesional cuyos compromisos éticos rebasan en muchas ocasiones a las obligaciones que tiene con sus clientes directos. Para explicar esta idea podríamos recurrir a un término inglés que refleja con mayor fidelidad la magnitud de este concepto, este término es ***Stake Holder.***
Un Stake Holder, es una persona, grupo de personas o una institución que tienen interés en el buen funcionamiento de una empresa, razón por la cual en algunos textos en español se traduce como "interesados".

Una compañía, adicionalmente a su concepción como empresa generadora de utilidades o satisfactores para sus dueños, es una entidad que agrupa seres humanos, dándoles empleo y la posibilidad de desarrollo profesional y personal; es una entidad que puede tener impacto económico en una comunidad al generar empleos directos e indirectos; es una fuente de contribución al gasto público a través del pago de sus impuestos; es un "socio" con el que proveedores y clientes establecerán relaciones comerciales y puede ser una alternativa de inversión para personas que deseen adquirir aciones de la compañía y en última instancia, representa una serie de recursos asignados a una administración para que dichos recursos sean utilizados en forma adecuada para alcanzar los objetivos de la empresa. La siguiente figura representa esta idea.



Pensemos ahora, que el informe de un auditor puede ser utilizado por cualquiera de estos grupos de interés para tomar decisiones que resultan trascendentales dentro de su contexto de actuación. Por ello precisamente, la responsabilidad y compromiso ético de

un auditor sobrepasa las obligaciones de un contrato laboral o de prestación de servicios profesionales.

Naturaleza ecléctica

Ecléctico, en un sentido amplio, significa la interacción de distintas ciencias o áreas de conocimiento en la resolución de un problema que resulta demasiado complejo para una de ellas actuando en forma aislada.

Esto es precisamente lo que hace la auditoría en TI y es también lo que la hace una disciplina tan compleja para ser desempeñada por un solo individuo.
El desarrollo de un trabajo de auditoría en TI requiere de profundos conocimientos en distintas disciplinas, que en forma coordinada permitan obtener los resultados deseados. Normalmente, este tipo de auditorías son desarrolladas por equipos multidisciplinarios, pues resulta muy difícil que un solo individuo reúna todos los conocimientos y cuente con profundidad necesaria en cada uno de ellos para ejecutar el trabajo.

Veamos algunos ejemplos de estas disciplinas:

Sistemas de información
Un auditor en TI requiere conocimientos sobre aspectos como el ciclo de vida de desarrollo de sistemas, técnicas de análisis, diseño y programación; teoría de comunicación, técnicas de obtención de información, empleo de herramientas CASE, etc., ya que una de sus funciones principales será, no sólo determinar si otras personas desarrollan en forma adecuada actividades que utilizan este conjunto de conocimientos, sino emitir recomendaciones que permitan mejorar dichas actividades.

Procesamiento electrónico de datos
Aún cuando un sistema de información no implica necesariamente el empleo de equipos de procesamiento electrónico de datos (EDP), la realidad es que actualmente es casi imposible concebir un sistema de información que sea efectivo y eficiente sin el uso de equipos de EDP.
El auditor debe poseer conocimientos sobre sistemas operativos, administradores de bases de datos, compiladores, procesadores, tipos de memoria y equipos periféricos como terminales, impresoras, unidades de almacenamiento secundario, entre otros elementos.

Telecomunicaciones
Al igual que el concepto anterior, esta área de conocimiento es una de las que mayor nivel técnico requiere para su evaluación. El desarrollo de los sistemas de información se ha visto impulsado enormemente por los adelantos en la tecnología de telecomunicaciones, por lo que su importancia relativa dentro de un ambiente de tecnología de información ha aumentado de manera dramática.
La forma en que las empresas trabajan ha evolucionado en forma significativa y conceptos como *EFT* (transferencia electrónica de fondos o electronic fund transfer), *eMail* (correo electrónico o electronic mail), *eComerce* (comercio electrónico), *voice*

mail (correo de voz), *videoconferencias* o simplemente *Internet*, se vuelven más y más, elementos cotidianos en la vida de las organizaciones y de las personas. Un sistema de información normalmente hace uso extensivo de las telecomunicaciones y por ende el conocimiento sobre esta materia se convierte de gran interés para un auditor en TI.

Teoría general de sistemas

Muchos de los aspectos relacionados con sistemas de información tuvieron su origen o se vieron influenciados por la Teoría General de Sistemas (TGS), concepto acuñado por Von Bertalanfy. Esta teoría resalta la importancia de la interacción de distintos elementos para lograr un fin común (sistema), la interacción de este grupo de elementos con su medio ambiente (sistemas abiertos), la necesidad de mantener un equilibrio interno entre los componentes de un sistema (entropía positiva) y el incremento en los beneficios como consecuencia de un trabajo conjunto de los elementos de un sistema (sinergia), entre otros componentes.

Todos estos conceptos son de aplicación en las empresas y su conocimiento y utilización, habitualmente ayudan a comprender mejor el comportamiento de las organizaciones, a identificar problemáticas y a fundamentar recomendaciones.

Ciencias del comportamiento humano

No podemos olvidar que al final de cada sistema se encuentran seres humanos que asumirán roles de usuarios o proveedores de información del mismo.

Algunos estudios han mostrado que la mayoría de los fracasos en proyectos de sistemas de información se debe al elemento humano y no a aspectos de tecnología o procesos de trabajo. Por tanto, es conveniente que el auditor en TI tenga adecuado conocimiento sobre comportamiento humano, para estar en posibilidad de evaluar los componentes de la administración del cambio en un proyecto de tecnología de información.

Administración de empresas

La tecnología de información es sólo uno de varios recursos que una empresa debe administrar para lograr una elevada productividad en sus operaciones y una adecuada competitividad en su mercado.

La teoría de administración incluye muchos conceptos de importancia tales como: el propio proceso administrativo (planear, dirigir, coordinar, supervisar y controlar), estructuras de organización, capacitación, políticas y procedimientos, administración de proyectos, etc.

Resulta claro que todos estos conceptos pueden tener relación directa o indirecta con la tecnología de información y que el auditor de esta disciplina debe contar con un adecuado conocimiento sobre administración en general para poder realizar su trabajo de evaluación.

Métodos numéricos

En muchas ocasiones, el auditor deberá basar conclusiones o fundamentar sus decisiones utilizando métodos numéricos. Estadística descriptiva, probabilidad, muestreo e investigación de operaciones son algunos ejemplos de aplicación de métodos que el auditor puede utilizar para desarrollar sus actividades.

Finanzas y contabilidad

No debemos olvidar que la auditoría en TI tuvo su origen en la auditoría de sistemas de información contables y debido a la incorporación de tecnología a dichos sistemas se vio la necesidad de incursionar en el mundo de la tecnología bajo una perspectiva de auditoría y control.
Aún hoy en día, la mayoría de los sistemas tienen un gran impacto en la información financiera de las empresas, misma que es registrada y presentada mediante principios de contabilidad.
Es por ende, que un conocimiento prácticamente indispensable para un auditor en TI lo representan los conceptos de finanzas, costos, y contabilidad necesarios para comprender los sistemas de información financiera de una empresa y las relaciones que otros sistemas deben tener con éstos.

Auditoría
Finalmente, y como elemento que integra y da sentido a todos los demás componentes del conocimiento, se encuentran los conceptos sobre auditoría, su proceso, su normatividad, sus técnicas, sus compromisos, etc.
Los conocimientos de auditoría fungirán como la “columna vertebral” del cuerpo ecléctico de conocimientos, dando forma y orden a los elementos necesarios para llevar a cabo las funciones de auditoría en TI con niveles mínimos de calidad.

Organismos Colegiados

Existe una asociación internacional denominada ***ISACA*** (*Information Systems Audit and Control Association*), cuyas oficinas generales tienen sede en la ciudad de Chicago.
Esta asociación tiene como misión proporcionar capacitación, estándares y desarrollo profesional a sus miembros y a través de la fundación ***ISACF*** (*Information Systems Audit and Control Foundation*), procurar un desarrollo de la comunidad profesional en general.

En su informe anual de 1996 la asociación reporta la siguiente información, misma que puede dar una idea de trascendencia a nivel mundial:

Membresía: La asociación cuenta con capítulos en 50 países y con miembros en más de 100 países, totalizando casi 17000 miembros a nivel mundial.

Certificación: Se cuenta con más de 10000 auditores certificados a nivel internacional. El examen se presenta en nueve idiomas (inglés, alemán, francés, hebreo, holandés, italiano, japonés, coreano y español).

Educación: Se imparten en forma anual cursos y conferencias en todo el mundo: la conferencia internacional y las conferencias de Computer Audit, Control and Security en Norteamérica, Europa Asia, y Latinoamérica.

La ISACA es la única asociación profesional verdaderamente global, compartiendo un mismo programa de certificación, de educación continua, estándares y código de ética profesional.

Programa de certificación
Existe una certificación avalada por la ISACA, que otorga a los auditores en sistemas de información el reconocimiento de poseer capacidad técnica y experiencia en el área de auditoría en TI. Uno de los requisitos para obtener el título ***CISA*** (*Certified Information Systems Auditor*) es un examen de conocimientos, el cual es aplicado por la asociación a nivel mundial. Adicionalmente, los CISAs deben probar experiencia profesional en las áreas de auditoría, seguridad, control o tecnología de información.

Programa de educación continua
Todos los poseedores de la certificación CISA están obligados a respetar un programa de educación continua para conservar la certificación, el cual consiste en cubrir como mínimo 120 horas en un período de 3 años.

Normatividad

La ISACA ha emitido un código de ética profesional y un cuerpo de estándares de auditoría en tecnología de información, los cuales establecen los lineamientos de actuación que debe respetar todo auditor de sistemas. A continuación se presenta una traducción del documento que contiene estos pronunciados.

Código de ética profesional para los auditores en tecnología de información.

"Los auditores en tecnología de información deben:

1. Sustentar el establecimiento y cumplimiento apropiado de los estándares, procedimientos y controles de los sistemas de información.

2. Dar cumplimiento a los estándares de auditoría en TI adoptados por la ISACF.

3. Servir en beneficio de sus empleados, accionistas, clientes y público en general en una forma diligente, leal y honesta y no pertenecer bajo conocimiento, a ninguna sociedad ilegal o de actividades impropias.

4. Mantener la confidencialidad de la información obtenida durante el transcurso de sus deberes. Esta información no deberá ser utilizada en beneficio personal ni deberá ser entregada a grupos inapropiados.

5. Realizar sus tareas en forma independiente y objetiva. Deberán evitar actividades que amenacen o que pretendan amenazar su independencia.

6. Mantener la competencia en campos interrelacionados con la auditoría en TI mediante la participación en actividades de desarrollo profesional.

7. Actuar con precaución en la obtención de documentación suficiente de hechos en los cuales se basa para conclusiones y recomendaciones.

8. Informar a las partes apropiadas sobre los resultados del trabajo de auditoría realizado.

9. Promover la educación de la gerencia, clientes y público en general para reforzar su entendimiento sobre la auditoría en TI.

10. Mantener alto estándares de conducta y carácter, tanto en las actividades personales como profesionales."

Estándares generales para la auditoría en tecnología de información.

Independencia

Estándar general No.1. *Actitud y apariencia.* En todos los aspectos relacionados con la auditoría, el auditor en TI debe ser independiente del auditado tanto en actitud como en apariencia.

Estándar general No.2. *Relación organizacional.* La función de auditoría en TI debe ser suficientemente independiente del área a ser auditada para permitir el cumplimiento de los objetivos de la auditoría.

Estándar general No.3. *Código de Ética Profesional.* El auditor de tecnología en información debe adherirse al código de Ética profesional de la ISACF.

Competencia técnica

Estándar general No.4. *Habilidades y conocimiento.* El auditor de tecnología en información debe ser técnicamente competente y debe poseer las habilidades y conocimientos necesarios en la realización del trabajo de auditoría.

Estándar general No.5. *Educación profesional continua.* El auditor de tecnología de información debe mantener competencia técnica mediante una apropiada capacitación continua.

Realización del trabajo

Estándar general No.6. *Planeación y supervisión.* Las auditorías de tecnología de información deben ser planeadas y supervisadas para prever el aseguramiento de alcanzar y cumplir los objetivos de la auditoría conforme al resto de los estándares.

Estándar general No.7. *Requerimiento de evidencia.* Durante el transcurso de la auditoría, el auditor de tecnología de información, deberá obtener evidencia suficiente para fundamentar hallazgos y conclusiones reportadas.

Estándar general No.8. *Cuidado profesional.* Debido al cuidado profesional que debe ser ejercido en todos los aspectos del trabajo del auditor, se deben respetar los estándares de auditoría aplicables.

Generación de reportes

Estándar general No.9. *Reportar la cobertura de la auditoría.* En la preparación de reportes, el auditor de tecnología de información debe establecer los objetivos de la auditoría, el período de cobertura, la naturaleza y la extensión del trabajo a realizar.

Estándar general No.10. *Reporte de hallazgos y conclusiones.* En la preparación de reportes, el auditor de tecnología de información debe definir los hallazgos y conclusiones concernientes al trabajo de auditoría realizado y cualquier reserva o calificación que el auditor juzgue pertinente sobre la auditoría.

Bibliografía

Reingeniería de la Auditoría Informática. Gustavo Adolfo Solís Montes. Capitulo Segundo – Pág. 33.