# CAPITULO IV

# IV. EVALUACIÓN DE LOS SISTEMAS

## Introducción

Es el primer paso práctico del auditor en informática dentro de las empresas o instituciones al efectuar un proyecto de auditoría en informática. Se busca la opinión de la alta dirección para estimar el grado de satisfacción y confianza que tiene en los productos, servicios y recursos de informática del negocio; asimismo, es posible detectar las fortalezas, aciertos y apoyo que brinda dicha función desde la perspectiva de los directivos del negocio.

Un punto importante que debe quedar plasmado en esta fase son las áreas de oportunidad que tiene informática para hacer más competitivo y rentable el negocio, sea este soporte directo o indirecto, en alto o menor grado.

Es conveniente aclarar que no se debe tratar esta etapa como un conjunto de tareas que requieren muchos recursos involucrados ni un tiempo considerable; es simplemente un aspecto necesario y generalizado para entender los puntos débiles y fuertes de la función de informática desde un punto de vista de los usuarios clave y la alta dirección.

Todas las actividades del auditor en informática deben estar claramente definidas en todos los componentes formales que integran cualquier trabajo dentro de una organización.

Los aspectos por evaluar son al menos los tres mencionados a continuación. Ahora bien, si el auditor considera .que la complejidad del negocio, la fusión o compra de la empresa, la informalidad palpable en informática o alguna consideración específica para el líder de proyectos o a petición de la alta dirección requieren más puntos por considerar y un tiempo más prolongado, conviene que los integre en esta fase, ya que aquí se detectan los primeros síntomas de informática que, a la postre, pueden ser los más relevantes.

Los temas evaluación de los sistemas, objetivos específicos de la evaluación de los sistemas, evaluación del sistema lógico, evaluación del desarrollo de sistemas y auditoría informática de comunicaciones y redes entre otros, corresponden a las obras elaboradas por Oscar Toro, Núñez de Balboa, Eduardo Horacio Quinn y Julián Gutiérrez Melo.

## IV.1 Evaluación de los sistemas

Fuente: http://www.monografias.com/trabajos/maudisist/maudisist.shtml

La elaboración de sistemas debe ser evaluada con mucho detalle, para lo cual se debe revisar si existen realmente sistemas entrelazados como un todo o bien si existen programas aislados. Otro de los factores a evaluar es si existe un plan estratégico para la elaboración de los sistemas o si se están elaborados sin el adecuado señalamiento de prioridades y de objetivos.

El plan estratégico deberá establecer los servicios que se presentarán en un futuro contestando preguntas como las siguientes:

¿Cuáles servicios se implementarán?
¿Cuándo se pondrán a disposición de los usuarios?

¿Qué características tendrán?
¿Cuántos recursos se requerirán?

La estrategia de desarrollo deberá establecer las nuevas aplicaciones, recursos y la arquitectura en que estarán fundamentados:

¿Qué aplicaciones serán desarrolladas y cuando?
¿Qué tipo de archivos se utilizarán y cuando?
¿Qué bases de datos serán utilizarán y cuando?
¿Qué lenguajes se utilizarán y en que software?
¿Qué tecnología será utilizada y cuando se implementará?
¿Cuantos recursos se requerirán aproximadamente?
¿Cuál es aproximadamente el monto de la inversión en hardware y software?

En lo referente a la consulta a los usuarios, el plan estratégico debe definir los requerimientos de información de la dependencia.

¿Qué estudios van a ser realizados al respecto?
¿Qué metodología se utilizará para dichos estudios?
¿Quién administrará y realizará dichos estudios?

En el área de auditoría interna debe evaluarse cuál ha sido la participación del auditor y los controles establecidos.

Por último, el plan estratégico determina la planeación de los recursos.

¿Contempla el plan estratégico las ventajas de la nueva tecnología?
¿Cuál es la inversión requerida en servicios, desarrollo y consulta a los usuarios?

El proceso de planeación de sistemas deberá asegurarse de que todos los recursos requeridos estén claramente identificados en el plan de desarrollo de aplicaciones y datos. Estos recursos (hardware, software y comunicaciones) deberán ser compatibles con la arquitectura y la tecnología, conque se cuenta actualmente.

Los sistemas deben evaluarse de acuerdo con el ciclo de vida que normalmente siguen: requerimientos del usuario, estudio de factibilidad, diseño general, análisis, diseño lógico, desarrollo físico, pruebas, implementación, evaluación, modificaciones, instalación, mejoras. Y se vuelve nuevamente al ciclo inicial. el cual a su vez debe comenzar con el de factibilidad.

La primera etapa a evaluar del sistema es el estudio de factibilidad, el cual debe analizar si el sistema es factible de realizarse, cuál es su relación costo/beneficio y si es recomendable elaborarlo.

Se deberá solicitar el estudio de factibilidad de los diferentes sistemas que se encuentren en operación, así como los que estén en la fase de análisis para evaluar si se considera la disponibilidad y características del equipo, los sistemas operativos y lenguajes disponibles, la necesidad de los usuarios, las formas de utilización de los sistemas, el costo y los beneficios que reportará el sistema, el efecto que producirá en quiénes lo usarán y el efecto que éstos tendrán sobre el sistema y la congruencia de los diferentes sistemas.

En el caso de sistemas que estén funcionando, se deberá comprobar si existe el estudio de factibilidad con los puntos señalados y compararse con la realidad con lo especificado en el estudio de factibilidad.

Por ejemplo en un sistema que el estudio de factibilidad señaló determinado costo y una serie de beneficios de acuerdo con las necesidades del usuario, debemos comparar cual fue su costo real y evaluar si se satisficieron las necesidades indicadas como beneficios del sistema.

Para investigar el costo de un sistema se debe considerar, con una exactitud razonable, el costo de los programas, el uso de los equipos (compilaciones, programas, pruebas, paralelos), tiempo, personal y operación, cosa que en fa práctica son costos directos, indirectos y de operación.

Los beneficios que justifiquen el desarrollo de un sistema pueden ser el ahorro en los costos de operación, la reducción del tiempo de proceso de un sistema. Mayor exactitud, mejor servicio, una mejoría en los procedimientos de control, mayor confiabilidad y seguridad.

Fuente: http://html.rincondelvago.com/auditoria-de-Ios-sistemas-de-informacion.html

Se encarga de llevar a cabo la evaluación de normas, técnicas y procedimientos que se tiene establecidos en una empresa para lograr confiabilidad, oportunidad, seguridad y confidencialidad de la información que se procesa a través de los sistemas de información. La auditoría de sistemas es una rama especializada de la auditoria que promueve y aplica conceptos de auditoría en el área de sistemas de información.

El objetivo final que tiene el auditor de sistemas es dar recomendaciones a la alta gerencia para mejorar o lograr un adecuado control interno en ambientes de tecnología informática con el fin de lograr mayor eficiencia operacional y administrativa.

## IV.2 Objetivos específicos de la auditoría de sistemas:

1. Participación en el desarrollo de nuevos sistemas:
    a. Evaluación de controles
    b. Cumplimiento de la metodología.
2. Evaluación de la seguridad en el área Informática.
3. Evaluación de suficiencia en los planes de contingencia.
    a. Respaldos, prever qué va a pasar si se presentan fallas.
4. Opinión de la utilización de los recursos informáticos.
    a. Resguardo y protección de activos. .
5. Control de modificación a las aplicaciones existentes.
    a. Fraudes
    b. Control a las modificaciones de los programas.
6. Participación en la negociación de contratos con los proveedores.
7. Revisión de la utilización del sistema operativo y los programas.
    a. Utilitarios
    b. Control sobre la utilización de los sistemas operativos
    c. Programas utilitarios.
8. Auditoría de la base de datos.
    a. Estructura sobre la cual se desarrollan las aplicaciones.
9. Auditoria de la red de teleprocesos
10. Desarrollo de software de auditoría.

Es el objetivo final de una auditoria de sistemas bien implementada, desarrollar software capaz de estar ejerciendo un control continuo de las operaciones del área de procesamiento de datos.

Fines de la auditoría de sistemas:

1. Fundamentar la opinión del auditor interno (externo) sobre la confiabilidad de los sistemas de información,
2. Expresar la opinión sobre la eficiencia de las operaciones en el área de TI.

Fuente: (http://www.inforarea.es/servicio7.htm) Núñez de Balboa.

Desde un Web site, una biblioteca, un archivo a un Centro de documentación, cualquier sistema de información puede ser evaluado para comprobar en que medida cumple con los objetivos para los que fue creado y detectar áreas de mejora en las que centrar las intervenciones futuras.

En nuestras evaluaciones seguimos una metodología adaptada a cada situación concreta que fundamentalmente recoge las siguientes fases:

Identificación y elección de los indicadores que permiten la medición de los distintos aspectos a evaluar

Recogida de datos mediante los medios mas adecuados a cada situación (encuestas, cuestionarios on-line, entrevistas, observación directa, test de usabilidad, trabajo en grupo, etc.)

Análisis de los indicadores
Detección de áreas de mejora
Propuestas de mejora

En muchos casos utilizamos la evaluación comparativa, que permite situar el sistema evaluado con respecto al mejor (benchmarking) o comparar el sistema con un grupo de sistemas similares para situarlo dentro de una escala.

## IV.3 Evaluación del Diseño Lógico del Sistema

Fuente: (http://www.itapizaco.edu.mx/paginas/maudisist.html) Toro Oscar.

En esta etapa se deberán analizar las especificaciones del sistema.

¿Qué deberá hacer?, ¿Cómo lo deberá hacer?, ¿Secuencia Y ocurrencia de los datos, el proceso y salida de reportes?

Una vez que hemos analizado estas partes, se deberá estudiar la participación que tuvo el usuario en la identificación del nuevo sistema, la participación de auditoría interna en el diseño de los controles y la determinación de los procedimientos de operación y decisión.

Al tener el análisis del diseño lógico del sistema debemos compararlo con lo que realmente se está obteniendo en la cual debemos evaluarlo planeado, cómo fue planeado y lo que realmente se está obteniendo.

Los puntos a evaluar son:

- Entradas.
- Salidas.
- Procesos.
- Especificaciones de datos.
- Especificaciones de proceso.
- Métodos de acceso.
- Operaciones.
- Manipulación de datos (antes y después del proceso electrónico de datos).
- Proceso lógico necesario para producir informes.
- Identificación de archivos, tamaño de los campos y registros.
- Proceso en línea o lote y su justificación.
- Frecuencia y volúmenes de operación.
- Sistemas de seguridad.
- Sistemas de control.
- Responsables.
- Número de usuarios.

Dentro del estudio de los sistemas en uso se deberá solicitar:

- Manual del usuario.
- Descripción de flujo de información y/o procesos.
- Descripción y distribución de información.
- Manual de formas.
- Manual de reportes.
- Lista de archivos y especificaciones.

Lo que se debe determinar en el sistema:
En el procedimiento:

- ¿Quién hace, cuando y como?
- ¿Qué formas se utilizan en el sistema?
- ¿Son necesarias, se usan, están duplicadas?
- ¿El número de copias es el adecuado?
- ¿Existen puntos de controlo faltan?

En la gráfica de flujo de información:

- ¿Es fácil de usar?
- ¿Es lógica?
- ¿Se encontraron lagunas?
- ¿Hay faltas de control?

En el diseño:

- ¿Cómo se usará la herramienta de diseño si existe?
- ¿Qué también se ajusta la herramienta al procedimiento?

## IV.4 Evaluación del desarrollo del Sistema

Fuente: (http://www.ilustrados.com/publicaciones/EpyppFZZkpIJTHHuCg.php) Toro Oscar.

En esta etapa del sistema se deberán auditar los programas, su diseño, el leguaje utilizado, interconexión entre los programas y características del hardware empleado (total o parcial) para el desarrollo del sistema. Al evaluar un sistema de información se tendrá presente que todo sistema debe proporcionar información para planear, organizar y controlar de manera eficaz y oportuna, para reducir la duplicidad de datos y de reportes y obtener una mayor seguridad en la forma más económica posible. De ese modo contará con los mejores elementos para una adecuada toma de decisiones. Al tener un proceso distribuido, es preciso considerar la seguridad del movimiento de la información entre nodos. El proceso de planeación de sistemas debe definir la red óptima de comunicaciones, los tipos de mensajes requeridos, el trafico esperado en las líneas de comunicación y otros factores que afectan el diseño. Es importante considerar las variables que afectan a un sistema: ubicación en los niveles de la organización, el tamaño y los recursos que utiliza. Las características que deben evaluarse en los sistemas son:

- Dinámicos (susceptibles de modificarse).
- Estructurados (las interacciones de sus componentes o subsistemas deben actuar como un todo)
- Integrados (un solo objetivo). En él habrá sistemas que puedan ser interrelacionados y no programas aislados.
- Accesibles (que estén disponibles).
- Necesarios (que se pruebe su utilización).
- Comprensibles (que contengan todos los atributos).
- Oportunos (que esté la información en el momento que se requiere).
- Funcionales (que proporcionen la información adecuada a cada nivel).
- Estándar (que la información tenga la misma interpretación en los distintos niveles).
- Modulares (facilidad para ser expandidos o reducidos).
- Jerárquicos (por niveles funcionales).
- Seguros (que sólo las personas autorizadas tengan acceso).
- Únicos (que no duplique información).

## IV.5 Auditoría informática de comunicaciones y redes

Fuente: (http:/www.monografias.com/trabajos5/audi/audi.shtml#redeS) Horacio Quinn Eduardo.

Para el informático Y para el auditor informático, el entramado conceptual que constituyen las Redes Nodales, Líneas, Concentradores, Multiplexores, Redes Locales, etc. no son sino el soporte físico-lógico del Tiempo Real. El auditor tropieza con la dificultad técnica del entorno, pues ha de analizar situaciones y hechos alejados entre si, y esté condicionado a la participación del monopolio telefónico que presta el soporte. Como en otros casos, la auditoría de este sector requiere un equipo de especialistas, expertos simultáneamente en Comunicaciones y en Redes Locales (no hay que olvidarse que en entornos geográficos reducidos, algunas empresas optan por el uso interno de Redes Locales, diseñadas y cableadas con recursos propios).

El auditor de Comunicaciones deberá inquirir sobre los índices de utilización de las líneas contratadas con información abundante sobre tiempos de desuso. Deberá proveerse de la topología de la Red de Comunicaciones, actualizada, ya que la desactualización de esta documentación significarla una grave debilidad. La inexistencia de datos sobre cuantas líneas existen, cómo son y donde están instaladas, supondría que se bordea la inoperatividad

Informática. Sin embargo, las debilidades más frecuentes o importantes se encuentran en las disfunciones organizativas. La contratación e instalación de líneas va asociada a la instalación de los Puestos de Trabajo correspondientes (Pantallas, Servidores de Redes Locales, Computadoras con tarjetas de Comunicaciones, impresoras, etc.). Todas estas actividades deben estar muy coordinadas y de ser posible, dependientes de una sola organización.

## IV.6 Auditoría de comunicaciones

Fuente: (http://monografias.com/trabajos10/auap/auap.shtml#au) Gutiérrez Melo Julián.

Ha de verse:

- La gestión de red = los equipos y su conectividad.
- La monitorización de las comunicaciones.
- La revisión de costes y la asignación formal de proveedores.
- Creación y aplicabilidad de estándares.

Cumpliendo como objetivos de control:

- Tener una gerencia de comunicaciones con plena autoridad de voto y acción.
- Llevar un registro actualizado de módems, controladores, terminales, líneas y todo equipo relacionado con las comunicaciones.
- Mantener una vigilancia constante sobre cualquier acción en la red.
- Registrar un coste de comunicaciones y reparto a encargados.
- Mejorar el rendimiento y la resolución de problemas presentados en la red.

Para lo cual se debe comprobar:

- El nivel de acceso a diferentes funciones dentro de la red.
- Coordinación de la organización de comunicación de datos y voz.
- Han de existir normas de comunicación en:
  - Tipos de equipamiento como adaptadores LAN.
  - Autorización de nuevo equipamiento, tanto dentro, como fuera de las horas laborales.
  - Uso de conexión digital con el exterior como Internet.
  - Instalación de equipos de escucha como Sniffers (exploradores físicos) o Traceadores (exploradores lógicos).

La responsabilidad en los contratos de proveedores.
La creación de estrategias de comunicación a largo plazo.
Los planes de comunicación a alta velocidad como fibra óptica y ATM ( técnica de conmutación de paquetes usada en redes MAN e ISDN).
Planificación de cableado.
Planificación de la recuperación de las comunicaciones en caso de desastre.
Ha de tenerse documentación sobre el diagramado de la red.
Se deben hacer pruebas sobre los nuevos equipos.
Se han de establecer las tasas de rendimiento en tiempo de respuesta de las terminales y la tasa de errores.
Vigilancia sobre toda actividad on-line.
La facturación de los transportistas y vendedores ha de revisarse regularmente.

## IV.7 Auditoría de la red física

Se debe garantizar que exista:

- Áreas de equipo de comunicación con control de acceso.
- Protección y tendido adecuado de cables y líneas de comunicación para evitar accesos físicos.
- Control de utilización de equipos de prueba de comunicaciones para monitorizar la red y el tráfico en ella.
- Prioridad de recuperación del sistema.
- Control de las líneas telefónicas.

Comprobando que:

- El equipo de comunicaciones ha de estar en un lugar cerrado y con acceso limitado.
- la seguridad física del equipo de comunicaciones sea adecuada.
- Se tomen medidas para separar las actividades de los electricistas y de cableado de líneas telefónicas.
- las líneas de comunicaci6n estén fuera de la vista.
- Se dé un código a cada línea, en vez de una descripción física de la misma.
- Haya procedimientos de protecci6n de los cables y las bocas de conexión para evitar pinchazos a la red.
- Existan revisiones periódicas de la red buscando pinchazos a la misma.
- El equipo de prueba de comunicaciones ha de tener unos propósitos y funciones específicas.
- Existan alternativas de respaldo de las comunicaciones.
- Con respecto a las líneas telefónicas: No debe darse el número como público y tenerlas configuradas con retrollamada, código de conexión o interruptores.

## IV.8 Auditoria de la red lógica

En ésta, debe evitarse un daño Interno, como por ejemplo, inhabilitar un equipo que empieza a enviar mensajes hasta que satura por completo la red. Para éste tipo de situaciones:

- Se deben dar contraseñas de acceso.
- Controlar los errores.
- Garantizar que en una transmisión, ésta solo sea recibida por el destinatario. Para esto, regularmente se cambia la ruta de acceso de la informaci6n a la red.
- Registrar las actividades de los usuarios en la red.
- Encriptar la información pertinente.
- Evitar la importación y exportación de datos.

Que se comprueban si: El sistema pidió el nombre de usuario y la contraseña para cada sesión: En cada sesión de usuario, se debe revisar que no acceda a ningún sistema sin autorización, ha de inhabilitarse al usuario que tras un número establecido de veces errar en dar correctamente su propia contraseña, se debe obligar a los usuarios a cambiar su contraseña regularmente, las contraseñas no deben ser mostradas en pantalla tras digitarlas,

para cada usuario, se debe dar información sobre su última conexión a fin de evitar suplantaciones.

- Inhabilitar el software o hardware con acceso libre.
- Generar estadísticas de las tasas de errores y transmisión.
- Crear protocolos con detección de errores.
- Los mensajes lógicos de transmisión han de llevar origen, fecha, hora y receptor.
- El software de comunicación, ha de tener procedimientos correctivos y de control ante mensajes duplicados, fuera de orden, perdidos o retrasados.
- Los datos sensibles, solo pueden ser impresos en una impresora especificada y ser vistos desde una terminal debidamente autorizada.
- Se debe hacer un análisis del riesgo de aplicaciones en los procesos.
- Se debe hacer un análisis de la conveniencia de cifrar los canales de transmisión entre diferentes organizaciones.
- Asegurar que los datos que viajan por Internet vayan cifrados.
- Si en la LAN hay equipos con modem entonces se debe revisar el control de seguridad asociado para impedir el acceso de equipos foráneos a la red.
- Deben existir políticas que prohíban la instalación de programas o equipos personales en la red.
- Los accesos a servidores remotos han de estar inhabilitados.
- La propia empresa generara propios ataques para probar solidez de la red y encontrar posibles fallos en cada una de las siguientes facetas:
  - Servidores = Desde dentro del servidor y de la red interna.
  - Servidores web.
  - Intranet = Desde dentro.
  - Firewall = Desde dentro.
  - Accesos del exterior y/o Internet.

# Bibliografía Capitulo IV

05/11/1999. “Auditoría Informática”.
http://www.monografias.com/trabajos/audotoinfo/auditoinfo.shtml

Toro Oscar. 26/12/1999. “Manual de auditoría de sistemas”.
http://www.monografias.com/trabajos/maudisist/maudisist.shtml

http://html.rincondelvago.com/auditoria-de-Ios-sistemas-de-informacion.html

Núñez de Balboa. “Evaluación de los sistemas de información”.
http://www.inforarea.es/servicio7.htm

Toro Oscar. 04/08/2003. “Manual de auditoría de sistemas”.
http://www.itapizaco.edu.mx/paginas/maudisist.html

Toro Oscar. 04/08/2003. “Manual de auditoría de sistemas”.
http://www.ilustrados.com/publicaciones/EpyppFZZkpIJTHHuCg.php

Horacio Quinn Eduardo. 08/11/2000. “La Auditoria informática dentro de las etapas de análisis de sistemas administrativos”.
http://www.monografias.com/trabajos5/audi/audi.shtml#redeS

Gutiérrez Melo Julián. 27/12/2001. “Auditoria aplicada a la seguridad en redes de computadores”.
http://www.monografias.com/trabajos10/auap/auap.shtml#au