La Auditoria informatica dentro de las etapas de Análisis de Sistemas Administrativos

Indice

1. Introducción

A finales del siglo XX, los Sistemas Informáticos se han constituido en las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial, los Sistemas de Información de la empresa.

La Informática hoy, está subsumida en la gestión integral de la empresa, y por eso las normas y estándares propiamente informáticos deben estar, por lo tanto, sometidos a los generales de la misma. En consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado el "management" o gestión de la empresa. Cabe aclarar que la Informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, pero no decide por sí misma. Por ende, debido a su importancia en el funcionamiento de una empresa, existe la Auditoría Informática.

El término de Auditoría se ha empleado incorrectamente con frecuencia ya que se ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas. A causa de esto, se ha tomado la frase "Tiene Auditoría" como sinónimo de que, en dicha entidad, antes de realizarse la auditoría, ya se habían detectado fallas.

El concepto de auditoría es mucho más que esto.

La palabra auditoría proviene del latín auditorius, y de esta proviene la palabra auditor, que se refiere a todo aquel que tiene la virtud de oír.

Por otra parte, el diccionario Español Sopena lo define como: Revisor de Cuentas colegiado. En un principio esta definición carece de la explicación del objetivo fundamental que persigue todo auditor: evaluar la eficiencia y eficacia.

Si consultamos el Boletín de Normas de auditoría del Instituto mexicano de contadores nos dice: " La auditoría no es una actividad meramente mecánica que implique la aplicación de ciertos procedimientos cuyos resultados, una vez llevado a cabo son de carácter indudable."

De todo esto sacamos como deducción que la auditoría es un examen crítico pero no mecánico, que no implica la preexistencia de fallas en la entidad auditada y que persigue el fin de evaluar y mejorar la eficacia y eficiencia de una sección o de un organismo.

El auditor informático ha de velar por la correcta utilización de los amplios recursos que la empresa pone en juego para disponer de un eficiente y eficaz Sistema de Información. Claro está, que para la realización de una auditoría informática eficaz, se debe entender a la empresa en su más amplio sentido, ya que una Universidad, un Ministerio o un Hospital son tan empresas como una Sociedad Anónima o empresa Pública. Todos utilizan la informática para gestionar sus "negocios" de forma rápida y eficiente con el fin de obtener beneficios económicos y reducción de costes.

Por eso, al igual que los demás órganos de la empresa (Balances y Cuentas de Resultados, Tarifas, Sueldos, etc.), los Sistemas Informáticos están sometidos al control correspondiente, o al menos debería estarlo. La importancia de llevar un control de esta herramienta se puede deducir de varios aspectos. He aquí algunos:

- Las computadoras y los Centros de Proceso de Datos se convirtieron en blancos apetecibles no solo para el espionaje, sino para la delincuencia y el terrorismo. En este caso interviene la Auditoría Informática de Seguridad.
- Las computadoras creadas para procesar y difundir resultados o información elaborada pueden producir resultados o información errónea si dichos datos son, a su vez, erróneos. Este concepto obvio es a veces olvidado por las mismas empresas que terminan perdiendo de vista la naturaleza y calidad de los datos de entrada a sus Sistemas Informáticos, con la posibilidad de que se provoque un efecto cascada y afecte a Aplicaciones independientes. En este caso interviene la Auditoría Informática de Datos.
- Un Sistema Informático mal diseñado puede convertirse en una herramienta harto peligrosa para la empresa: como las maquinas obedecen ciegamente a las órdenes recibidas y la modelización de la empresa está determinada por las computadoras que materializan los Sistemas de Información, la gestión y la organización de la empresa no puede depender de un Software y Hardware mal diseñados. Estos son solo algunos de los varios inconvenientes que puede presentar un Sistema Informático, por eso, la necesidad de la Auditoría de Sistemas.

2. Auditoría

La auditoría nace como un órgano de control de algunas instituciones estatales y privadas. Su función inicial es estrictamente económico-financiero, y los casos inmediatos se encuentran en las peritaciones judiciales y las contrataciones de contables expertos por parte de Bancos Oficiales.
La función auditora debe ser absolutamente independiente; no tiene carácter ejecutivo, ni son vinculantes sus conclusiones. Queda a cargo de la empresa tomar las decisiones pertinentes. La auditoría contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones. Aunque pueden aparecer sugerencias y planes de acción para eliminar las disfunciones y debilidades antedichas; estas sugerencias plasmadas en el Informe final reciben el nombre de Recomendaciones.
Las funciones de análisis y revisión que el auditor informático realiza, puede chocar con la psicología del auditado, ya que es un informático y tiene la necesidad de realizar sus tareas con racionalidad y eficiencia. 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 su tarea.
Además del chequeo de los Sistemas, el auditor somete al auditado a una serie de cuestionario. Dichos cuestionarios, llamados Check List, son guardados celosamente por las empresas auditoras, ya que son activos importantes de su actividad. Las Check List tienen que ser comprendidas por el auditor al pie de la letra, ya que si son mal aplicadas y mal recitadas se pueden llegar a obtener resultados distintos a los esperados por la empresa auditora. La Check List puede llegar a explicar cómo ocurren los hechos pero no por qué ocurren. El cuestionario debe estar subordinado a la regla, a la norma, al método. Sólo una metodología precisa puede desentrañar las causas por las cuales se realizan actividades teóricamente inadecuadas o se omiten otras correctas.
El auditor sólo puede emitir un juicio global o parcial basado en hechos y situaciones incontrovertibles, careciendo de poder para modificar la situación analizada por él mismo.

3. Auditoría Interna y Auditoría Externa

La auditoría interna es la realizada con recursos materiales y personas que pertenecen a la empresa auditada. Los empleados que realizan esta tarea son remunerados económicamente. La auditoría interna existe por expresa decisión de la Empresa, o sea, que puede optar por su disolución en cualquier momento.
Por otro lado, la auditoría externa es realizada por personas afines a la empresa auditada; es siempre remunerada. Se presupone una mayor objetividad que en la Auditoría Interna, debido al mayor distanciamiento entre auditores y auditados.
La auditoría informática interna cuenta con algunas ventajas adicionales muy importantes respecto de la auditoría externa, las cuales no son tan perceptibles como en las auditorías convencionales. La auditoría interna tiene la ventaja de que puede actuar periódicamente realizando Revisiones globales, como parte de su Plan Anual y de su actividad normal. Los auditados conocen estos planes y se habitúan a las Auditorías, especialmente cuando las consecuencias de las Recomendaciones habidas benefician su trabajo.
En una empresa, los responsables de Informática escuchan, orientan e informan sobre las posibilidades técnicas y los costes de tal Sistema. Con voz, pero a menudo sin voto, Informática trata de satisfacer lo más adecuadamente posible aquellas necesidades. La empresa necesita controlar su Informática y ésta necesita que su propia gestión esté sometida a los mismos Procedimientos y estándares que el resto de aquella. La conjunción de ambas necesidades cristaliza en la figura del auditor interno informático.

En cuanto a empresas se refiere, solamente las más grandes pueden poseer una Auditoría propia y permanente, mientras que el resto acuden a las auditorías externas. Puede ser que algún profesional informático sea trasladado desde su puesto de trabajo a la Auditoría Interna de la empresa cuando ésta existe. Finalmente, la propia Informática requiere de su propio grupo de Control Interno, con implantación física en su estructura, puesto que si se ubicase dentro de la estructura Informática ya no sería independiente. Hoy, ya existen varias organizaciones Informáticas dentro de la misma empresa, y con diverso grado de autonomía, que son coordinadas por órganos corporativos de Sistemas de Información de las Empresas.

Una Empresa o Institución que posee auditoría interna puede y debe en ocasiones contratar servicios de auditoría externa. Las razones para hacerlo suelen ser:

- Necesidad de auditar una materia de gran especialización, para la cual los servicios propios no están suficientemente capacitados.
- Contrastar algún Informe interno con el que resulte del externo, en aquellos supuestos de emisión interna de graves recomendaciones que chocan con la opinión generalizada de la propia empresa.
- Servir como mecanismo protector de posibles auditorías informáticas externas decretadas por la misma empresa.
- Aunque la auditoría interna sea independiente del Departamento de Sistemas, sigue siendo la misma empresa, por lo tanto, es necesario que se le realicen auditorías externas como para tener una visión desde afuera de la empresa.

La auditoría informática, tanto externa como interna, debe ser una actividad exenta de cualquier contenido o matiz "político" ajeno a la propia estrategia y política general de la empresa. La función auditora puede actuar de oficio, por iniciativa del propio órgano, o a instancias de parte, esto es, por encargo de la dirección o cliente.

4. Alcance de la Auditoría Informática

El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoría informática, se complementa con los objetivos de ésta. El alcance ha de figurar expresamente en el Informe Final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas. Ejemplo: ¿Se someterán los registros grabados a un control de integridad exhaustivo*? ¿Se comprobará que los controles de validación de errores son adecuados y suficientes*? La indefinición de los alcances de la auditoría compromete el éxito de la misma.

*Control de integridad de registros:

Hay Aplicaciones que comparten registros, son registros comunes. Si una Aplicación no tiene integrado un registro común, cuando lo necesite utilizar no lo va encontrar y, por lo tanto, la aplicación no funcionaría como debería.

*Control de validación de errores:

Se corrobora que el sistema que se aplica para detectar y corregir errores sea eficiente.

5. Características de la Auditoría Informática

La información de la empresa y para la empresa, siempre importante, se ha convertido en un Activo Real de la misma, como sus Stocks o materias primas si las hay. Por ende, han de realizarse inversiones informáticas, materia de la que se ocupa la Auditoría de Inversión Informática.

Del mismo modo, los Sistemas Informáticos han de protegerse de modo global y particular: a ello se debe la existencia de la Auditoría de Seguridad Informática en general, o a la auditoría de Seguridad de alguna de sus áreas, como pudieran ser Desarrollo o Técnica de Sistemas.

Cuando se producen cambios estructurales en la Informática, se reorganiza de alguna forma su función: se está en el campo de la Auditoría de Organización Informática.

Estos tres tipos de auditorías engloban a las actividades auditoras que se realizan en una auditoría parcial. De otra manera: cuando se realiza una auditoria del área de Desarrollo de Proyectos de la Informática de una empresa, es porque en ese Desarrollo existen, además de ineficiencias, debilidades de organización, o de inversiones, o de seguridad, o alguna mezcla de ellas.

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 con 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

[Los datos son propiedad inicialmente de la organización que los genera. Los datos de personal son especialmente confidenciales]

- 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.
- 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.

*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 Backups 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 Telecom, a las oficinas paralelas, Telefónica. 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.

6. Tipos y clases de Auditorías

El departamento de Informática posee una actividad proyectada al exterior, al usuario, aunque el "exterior" siga siendo la misma empresa. He aquí, la Auditoría Informática de Usuario. Se hace esta distinción para contraponerla a la informática interna, en donde se hace la informática cotidiana y real. En consecuencia, existe una Auditoría Informática de Actividades Internas.

El control del funcionamiento del departamento de informática con el exterior, con el usuario se realiza por medio de la Dirección. Su figura es importante, en tanto en cuanto es capaz de interpretar las necesidades de la Compañía. Una informática eficiente y eficaz requiere el apoyo continuado de su Dirección frente al "exterior". Revisar estas interrelaciones constituye el objeto de la Auditoría Informática de Dirección. Estas tres auditorías, mas la auditoría de Seguridad, son las cuatro Areas Generales de la Auditoría Informática más importantes.

Dentro de las áreas generales, se establecen las siguientes divisiones de Auditoría Informática: de Explotación, de Sistemas, de Comunicaciones y de Desarrollo de Proyectos. Estas son las Areas Especificas de la Auditoría Informática más importantes.

Areas Específicas	Areas Generales			
	Interna	Dirección	Usuario	Seguridad
Explotación				
Desarrollo				
Sistemas				
Comunicaciones				
Seguridad				

Cada Area Especifica puede ser auditada desde los siguientes criterios generales:

- Desde su propio funcionamiento interno.
- Desde el apoyo que recibe de la Dirección y, en sentido ascendente, del grado de cumplimiento de las directrices de ésta.
- Desde la perspectiva de los usuarios, destinatarios reales de la informática.
- Desde el punto de vista de la seguridad que ofrece la Informática en general o la rama auditada.

Estas combinaciones pueden ser ampliadas y reducidas según las características de la empresa auditada.

7. Objetivo fundamental de la auditoría informática

Operatividad

La operatividad es una función de mínimos consistente en que la organización y las maquinas funcionen, siquiera mínimamente. No es admisible detener la maquinaria informática para descubrir sus fallos y comenzar de nuevo. La auditoría debe iniciar su actividad cuando los Sistemas están operativos, es el principal objetivo el de mantener tal situación. Tal objetivo debe conseguirse tanto a nivel global como parcial.

La operatividad de los Sistemas ha de constituir entonces la principal preocupación del auditor informático. Para conseguirla hay que acudir a la realización de Controles Técnicos Generales de Operatividad y Controles Técnicos Específicos de Operatividad, previos a cualquier actividad de aquel.

- Los Controles Técnicos Generales son los que se realizan para verificar la compatibilidad de funcionamiento simultaneo del Sistema Operativo y el Software de base con todos los subsistemas existentes, así como la compatibilidad del Hardware y del Software instalados. Estos controles son importantes en las instalaciones que cuentan con varios competidores, debido a que la profusión de entornos de trabajo muy diferenciados obliga a la contratación de diversos productos de Software básico, con el consiguiente riesgo de abonar más de una vez el mismo producto o desaprovechar parte del Software abonado. Puede ocurrir también con los productos de Software básico desarrollados por el personal de Sistemas Interno, sobre todo cuando los diversos equipos están ubicados en Centros de Proceso de Datos geográficamente alejados. Lo negativo de esta situación es que puede producir la inoperatividad del conjunto. Cada Centro de Proceso de Datos tal vez sea operativo trabajando independientemente, pero no será posible la interconexión e intercomunicación de todos los Centros de Proceso de Datos si no existen productos comunes y compatibles.
- Los Controles Técnicos Específicos, de modo menos acusado, son igualmente necesarios para lograr la Operatividad de los Sistemas. Un ejemplo de lo que se puede encontrar mal son parámetros de asignación automática de espacio en disco* que dificulten o impidan su utilización posterior por una Sección distinta de la que lo generó. También, los periodos de retención de ficheros comunes a varias Aplicaciones pueden estar definidos con distintos plazos en cada una de ellas, de modo que la pérdida de información es un hecho que podrá producirse con facilidad, quedando inoperativa la explotación de alguna de las Aplicaciones mencionadas.

*Parámetros de asignación automática de espacio en disco:

Todas las Aplicaciones que se desarrollan son super-parametrizadas , es decir, que tienen un montón de parámetros que permiten configurar cual va a ser el comportamiento del Sistema. Una Aplicación va a usar para tal y tal cosa cierta cantidad de espacio en disco. Si uno no analizó cual es la operatoria y el tiempo que le va a llevar ocupar el espacio asignado, y se pone un valor muy chico, puede ocurrir que

un día la Aplicación reviente, se caiga. Si esto sucede en medio de la operatoria y la Aplicación se cae, el volver a levantarla, con la nueva asignación de espacio, si hay que hacer reconversiones o lo que sea, puede llegar a demandar muchísimo tiempo, lo que significa un riesgo enorme.

8. Revisión de Controles de la Gestión Informática

Una vez conseguida la Operatividad de los Sistemas, el segundo objetivo de la auditoría es la verificación de la observancia de las normas teóricamente existentes en el departamento de Informática y su coherencia con las del resto de la empresa. Para ello, habrán de revisarse sucesivamente y en este orden:

1. Las Normas Generales de la Instalación Informática. Se realizará una revisión inicial sin estudiar a fondo las contradicciones que pudieran existir, pero registrando las áreas que carezcan de normativa, y sobre todo verificando que esta Normativa General Informática no está en contradicción con alguna Norma General no informática de la empresa.
2. Los Procedimientos Generales Informáticos. Se verificará su existencia, al menos en los sectores más importantes. Por ejemplo, la recepción definitiva de las máquinas debería estar firmada por los responsables de Explotación. Tampoco el alta de una nueva Aplicación podría producirse si no existieran los Procedimientos de Backup y Recuperación correspondientes.
3. Los Procedimientos Específicos Informáticos. Igualmente, se revisara su existencia en las áreas fundamentales. Así, Explotación no debería explotar una Aplicación sin haber exigido a Desarrollo la pertinente documentación. Del mismo modo, deberá comprobarse que los Procedimientos Específicos no se opongan a los Procedimientos Generales. En todos los casos anteriores, a su vez, deberá verificarse que no existe contradicción alguna con la Normativa y los Procedimientos Generales de la propia empresa, a los que la Informática debe estar sometida.

9. Auditoría Informática de Explotación

La Explotación Informática se ocupa de producir resultados informáticos de todo tipo: listados impresos, ficheros soportados magnéticamente para otros informáticos, ordenes automatizadas para lanzar o modificar procesos industriales, etc. La explotación informática se puede considerar como una fabrica con ciertas peculiaridades que la distinguen de las reales. Para realizar la Explotación Informática se dispone de una materia prima, los Datos, que es necesario transformar, y que se someten previamente a controles de integridad y calidad. La transformación se realiza por medio del Proceso informático, el cual está gobernado por programas. Obtenido el producto final, los resultados son sometidos a varios controles de calidad y, finalmente, son distribuidos al cliente, al usuario.

Auditar Explotación consiste en auditar las secciones que la componen y sus interrelaciones. La Explotación Informática se divide en tres grandes áreas: Planificación, Producción y Soporte Técnico, en la que cada cual tiene varios grupos.

Control de Entrada de Datos:

Se analizará la captura de la información en soporte compatible con los Sistemas, el cumplimiento de plazos y calendarios de tratamientos y entrega de datos; la correcta transmisión de datos entre entornos diferentes. Se verificará que los controles de integridad y calidad de datos se realizan de acuerdo a Norma.

Planificación y Recepción de Aplicaciones:

Se auditarán las normas de entrega de Aplicaciones por parte de Desarrollo, verificando su cumplimiento y su calidad de interlocutor único. Deberán realizarse muestreos selectivos de la Documentación de las Aplicaciones explotadas. Se inquirirá sobre la anticipación de contactos con Desarrollo para la planificación a medio y largo plazo.

Centro de Control y Seguimiento de Trabajos:

Se analizará cómo se prepara, se lanza y se sigue la producción diaria. Básicamente, la explotación Informática ejecuta procesos por cadenas o lotes sucesivos (Batch*), o en tiempo real (Tiempo Real*). Mientras que las Aplicaciones de Teleproceso están permanentemente activas y la función de Explotación se limita a vigilar y recuperar incidencias, el trabajo Batch absorbe una buena parte de los efectivos de Explotación. En muchos Centros de Proceso de Datos, éste órgano recibe el nombre de Centro de Control de Batch. Este grupo determina el éxito de la explotación, en cuanto que es uno de los factores más importantes en el mantenimiento de la producción.

*Batch y Tiempo Real:

Las Aplicaciones que son Batch son Aplicaciones que cargan mucha información durante el día y durante la noche se corre un proceso enorme que lo que hace es relacionar toda la información, calcular cosas y obtener como salida, por ejemplo, reportes. O sea, recolecta información durante el día, pero todavía no procesa nada. Es solamente un tema de "Data Entry" que recolecta información, corre el proceso Batch (por lotes), y calcula todo lo necesario para arrancar al día siguiente.

Las Aplicaciones que son Tiempo Real u Online, son las que, luego de haber ingresado la información correspondiente, inmediatamente procesan y devuelven un resultado. Son Sistemas que tienen que responder en Tiempo Real.

Operación. Salas de Ordenadores:

Se intentarán analizar las relaciones personales y la coherencia de cargos y salarios, así como la equidad en la asignación de turnos de trabajo. Se verificará la existencia de un responsable de Sala en cada turno de trabajo. Se analizará el grado de automatización de comandos, se verificara la existencia y grado de uso de los Manuales de Operación. Se analizará no solo la existencia de planes de formación, sino el cumplimiento de los mismos y el tiempo transcurrido para cada Operador desde el último Curso recibido. Se estudiarán los montajes diarios y por horas de cintas o cartuchos, así como los tiempos transcurridos entre la petición de montaje por parte del Sistema hasta el montaje real. Se verificarán las líneas de papel impresas diarias y por horas, así como la manipulación de papel que comportan.

Centro de Control de Red y Centro de Diagnosis (Help Desk):

El Centro de Control de Red suele ubicarse en el área de producción de Explotación. Sus funciones se refieren exclusivamente al ámbito de las Comunicaciones, estando muy relacionado con la organización de Software de Comunicaciones de Técnicas de Sistemas. Debe analizarse la fluidez de esa relación y el grado de coordinación entre ambos. Se verificará la existencia de un punto focal único, desde el cual sean perceptibles todos las líneas asociadas al Sistema. El Centro de Diagnosis (Help Desk) es el ente en donde se atienden las llamadas de los usuarios-clientes que han sufrido averías o incidencias, tanto de Software como de Hardware. El Centro de Diagnosis está especialmente indicado para informáticos grandes y con usuarios dispersos en un amplio territorio. Es uno de los elementos que más contribuyen a configurar la imagen de la Informática de la empresa. Debe ser auditada desde esta perspectiva, desde la sensibilidad del usuario sobre el servicio que se le dispone. No basta con comprobar la eficiencia técnica del Centro, es necesario analizarlo simultáneamente en el ámbito de Usuario.

Auditoría Informática de Desarrollo de Proyectos o Aplicaciones:

La función de Desarrollo es una evolución del llamado Análisis y Programación de Sistemas y Aplicaciones. A su vez, engloba muchas áreas, tantas como sectores informatizables tiene la empresa. Muy escuetamente, una Aplicación recorre las siguientes fases:

- Prerequisitos del Usuario (único o plural) y del entorno
- Análisis funcional
- Diseño
- Análisis orgánico (Preprogramación y Programación)
- Pruebas
- Entrega a Explotación y alta para el Proceso.

Estas fases deben estar sometidas a un exigente control interno, caso contrario, además del disparo de los costes, podrá producirse la insatisfacción del usuario. Finalmente, la auditoría deberá comprobar la seguridad de los programas en el sentido de garantizar que los ejecutados por la maquina sean exactamente los previstos y no otros.

Una auditoría de Aplicaciones pasa indefectiblemente por la observación y el análisis de cuatro consideraciones:

1. Revisión de las metodologías utilizadas: Se analizaran éstas, de modo que se asegure la modularidad de las posibles futuras ampliaciones de la Aplicación y el fácil mantenimiento de las mismas.
2. Control Interno de las Aplicaciones: se deberán revisar las mismas fases que presuntamente han debido seguir el área correspondiente de Desarrollo:

- Estudio de Vialidad de la Aplicación. [importante para Aplicaciones largas, complejas y caras]
- Definición Lógica de la Aplicación. [se analizará que se han observado los postulados lógicos de actuación, en función de la metodología elegida y la finalidad que persigue el proyecto]
- Desarrollo Técnico de la Aplicación. [Se verificará que éste es ordenado y correcto. Las herramientas técnicas utilizadas en los diversos programas deberán ser compatibles]
- Diseño de Programas. [deberán poseer la máxima sencillez, modularidad y economía de recursos]
- Métodos de Pruebas. [Se realizarán de acuerdo a las Normas de la Instalación. Se utilizarán juegos de ensayo de datos, sin que sea permisible el uso de datos reales]
- Documentación. [cumplirá la Normativa establecida en la Instalación, tanto la de Desarrollo como la de entrega de Aplicaciones a Explotación]

- Equipo de Programación. [Deben fijarse las tareas de análisis puro, de programación y las intermedias. En Aplicaciones complejas se producirían variaciones en la composición del grupo, pero estos deberán estar previstos]

1. Satisfacción de usuarios: Una Aplicación técnicamente eficiente y bien desarrollada, deberá considerarse fracasada si no sirve a los intereses del usuario que la solicitó. La aquiescencia del usuario proporciona grandes ventajas posteriores, ya que evitará reprogramaciones y disminuirá el mantenimiento de la Aplicación.
2. Control de Procesos y Ejecuciones de Programas Críticos: El auditor no debe descartar la posibilidad de que se esté ejecutando un módulo que no se corresponde con el programa fuente que desarrolló, codificó y probó el área de Desarrollo de Aplicaciones. Se ha de comprobar la correspondencia biunívoca y exclusiva entre el programa codificado y su compilación. Si los programas fuente y los programa módulo no coincidieran podríase provocar, desde errores de bulto que producirían graves y altos costes de mantenimiento, hasta fraudes, pasando por acciones de sabotaje, espionaje industrial-informativo, etc. Por ende, hay normas muy rígidas en cuanto a las Librerías de programas; aquellos programas fuente que hayan sido dados por bueno por Desarrollo, son entregados a Explotación con el fin de que éste:
    1. Copie el programa fuente en la Librería de Fuentes de Explotación, a la que nadie más tiene acceso
    2. Compile y monte ese programa, depositándolo en la Librería de Módulos de Explotación, a la que nadie más tiene acceso.
    3. Copie los programas fuente que les sean solicitados para modificarlos, arreglarlos, etc. en el lugar que se le indique. Cualquier cambio exigirá pasar nuevamente por el punto 1.

Como este sistema para auditar y dar el alta a una nueva Aplicación es bastante ardua y compleja, hoy (algunas empresas lo usarán, otras no) se utiliza un sistema llamado U.A.T (User Acceptance Test). Este consiste en que el futuro usuario de esta Aplicación use la Aplicación como si la estuviera usando en Producción para que detecte o se denoten por sí solos los errores de la misma. Estos defectos que se encuentran se van corrigiendo a medida que se va haciendo el U.A.T. Una vez que se consigue el U.A.T., el usuario tiene que dar el Sign Off ("Esto está bien"). Todo este testeo, auditoría lo tiene que controlar, tiene que evaluar que el testeo sea correcto, que exista un plan de testeo, que esté involucrado tanto el cliente como el desarrollador y que estos defectos se corrijan. Auditoría tiene que corroborar que el U.A.T. prueba todo y que el Sign Off del usuario sea un Sign Off por **todo**.
Es aconsejable que las Empresas cuenten con un Departamento QA (Quality Assurance – Aseguramiento de la Calidad) que tendría la función de controlar que el producto que llegue al usuario sea el correcto en cuanto a funcionamiento y prestaciones, antes del U.A.T.

Auditoría Informática de Sistemas:

Se ocupa de analizar la actividad que se conoce como Técnica de Sistemas en todas sus facetas. Hoy, la importancia creciente de las telecomunicaciones ha propiciado que las Comunicaciones, Líneas y Redes de las instalaciones informáticas, se auditen por separado, aunque formen parte del entorno general de Sistemas.

Sistemas Operativos:

Engloba los Subsistemas de Teleproceso, Entrada/Salida, etc. Debe verificarse en primer lugar que los Sistemas están actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones si las hubiera. El análisis de las versiones de los Sistemas Operativos permite descubrir las posibles incompatibilidades entre otros productos de Software Básico adquiridos por la instalación y determinadas versiones de aquellas. Deben revisarse los parámetros variables de las Librerías más importantes de los Sistemas, por si difieren de los valores habituales aconsejados por el constructor.

Software Básico:

Es fundamental para el auditor conocer los productos de software básico que han sido facturados aparte de la propia computadora. Esto, por razones económicas y por razones de comprobación de que la computadora podría funcionar sin el producto adquirido por el cliente. En cuanto al Software desarrollado por el personal informático de la empresa, el auditor debe verificar que éste no agreda ni condiciona al Sistema. Igualmente, debe considerar el esfuerzo realizado en términos de costes, por si hubiera alternativas más económicas.

Software de Teleproceso (Tiempo Real):

No se incluye en Software Básico por su especialidad e importancia. Las consideraciones anteriores son válidas para éste también.

Tunning:

Es el conjunto de técnicas de observación y de medidas encaminadas a la evaluación del comportamiento de los Subsistemas y del Sistema en su conjunto. Las acciones de tunning deben diferenciarse de los controles habituales que realiza el personal de Técnica de Sistemas. El tunning

posee una naturaleza más revisora, estableciéndose previamente planes y programas de actuación según los síntomas observados. Se pueden realizar:

- Cuando existe sospecha de deterioro del comportamiento parcial o general del Sistema
- De modo sistemático y periódico, por ejemplo cada 6 meses. En este caso sus acciones son repetitivas y están planificados y organizados de antemano.

El auditor deberá conocer el número de Tunning realizados en el último año, así como sus resultados. Deberá analizar los modelos de carga utilizados y los niveles e índices de confianza de las observaciones.

Optimización de los Sistemas y Subsistemas:

Técnica de Sistemas debe realizar acciones permanentes de optimización como consecuencia de la realización de tunnings preprogramados o específicos. El auditor verificará que las acciones de optimización* fueron efectivas y no comprometieron la Operatividad de los Sistemas ni el plan crítico de producción diaria de Explotación.

*Optimización:

Por ejemplo: cuando se instala una Aplicación, normalmente está vacía, no tiene nada cargado adentro. Lo que puede suceder es que, a medida que se va cargando, la Aplicación se va poniendo cada vez más lenta; porque todas las referencias a tablas es cada vez más grande, la información que está moviendo es cada vez mayor, entonces la Aplicación se tiende a poner lenta. Lo que se tiene que hacer es un análisis de performance, para luego optimizarla, mejorar el rendimiento de dicha Aplicación.

Administración de Base de Datos:

El diseño de las Bases de Datos, sean relaciones o jerárquicas, se ha convertido en una actividad muy compleja y sofisticada, por lo general desarrollada en el ámbito de Técnica de Sistemas, y de acuerdo con las áreas de Desarrollo y usuarios de la empresa. Al conocer el diseño y arquitectura de éstas por parte de Sistemas, se les encomienda también su administración. Los auditores de Sistemas han observado algunas disfunciones derivadas de la relativamente escasa experiencia que Técnica de Sistemas tiene sobre la problemática general de los usuarios de Bases de Datos.

La administración tendría que estar a cargo de Explotación. El auditor de Base de Datos debería asegurarse que Explotación conoce suficientemente las que son accedidas por los Procedimientos que ella ejecuta. Analizará los Sistemas de salvaguarda existentes, que competen igualmente a Explotación. Revisará finalmente la integridad y consistencia de los datos, así como la ausencia de redundancias entre ellos.

Investigación y Desarrollo:

Como empresas que utilizan y necesitan de informáticas desarrolladas, saben que sus propios efectivos están desarrollando Aplicaciones y utilidades que, concebidas inicialmente para su uso interno, pueden ser susceptibles de adquisición por otras empresas, haciendo competencia a las Compañías del ramo. La auditoría informática deberá cuidar de que la actividad de Investigación y Desarrollo no interfiera ni dificulte las tareas fundamentales internas.

<La propia existencia de aplicativos para la obtención de estadísticas desarrollados por los técnicos de Sistemas de la empresa auditada, y su calidad, proporcionan al auditor experto una visión bastante exacta de la eficiencia y estado de desarrollo de los Sistemas>

10. Auditoría Informática de Comunicaciones y Redes

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 sí, y está 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 significaría 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.

Auditoría de la Seguridad informática:

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También puede ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional. Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos.

En la actualidad y principalmente en las computadoras personales, se ha dado otro factor que hay que considerar: el llamado "virus" de las computadoras, el cual, aunque tiene diferentes intenciones, se encuentra principalmente para paquetes que son copiados sin autorización ("piratas") y borra toda la información que se tiene en un disco. Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus. El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.

La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica. La seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc.

La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

Un método eficaz para proteger sistemas de computación es el software de control de acceso. Dicho simplemente, los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial. Dichos paquetes han sido populares desde hace muchos años en el mundo de las computadoras grandes, y los principales proveedores ponen a disposición de clientes algunos de estos paquetes.

Ejemplo: Existe una Aplicación de Seguridad que se llama SEOS, para Unix, que lo que hace es auditar el nivel de Seguridad en todos los servidores, como ser: accesos a archivos, accesos a directorios, que usuario lo hizo, si tenía o no tenía permiso, si no tenía permiso porque falló, entrada de usuarios a cada uno de los servidores, fecha y hora, accesos con password equivocada, cambios de password, etc. La Aplicación lo puede graficar, tirar en números, puede hacer reportes, etc.

La seguridad informática se la puede dividir como Area General y como Area Especifica (seguridad de Explotación, seguridad de las Aplicaciones, etc.). Así, se podrán efectuar auditorías de la Seguridad Global de una Instalación Informática –Seguridad General- y auditorías de la Seguridad de un área informática determinada – Seguridad Especifica -.

Con el incremento de agresiones a instalaciones informáticas en los últimos años, se han ido originando acciones para mejorar la Seguridad Informática a nivel físico. Los accesos y conexiones indebidos a través de las Redes de Comunicaciones, han acelerado el desarrollo de productos de Seguridad lógica y la utilización de sofisticados medios criptograficos.

El sistema integral de seguridad debe comprender:

- Elementos administrativos
- Definición de una política de seguridad
- Organización y división de responsabilidades
- Seguridad física y contra catástrofes (incendio, terremotos, etc.)
- Prácticas de seguridad del personal
- Elementos técnicos y procedimientos
- Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales.
- Aplicación de los sistemas de seguridad, incluyendo datos y archivos
- El papel de los auditores, tanto internos como externos
- Planeación de programas de desastre y su prueba.

La decisión de abordar una Auditoría Informática de Seguridad Global en una empresa, se fundamenta en el estudio cuidadoso de los riesgos potenciales a los que está sometida. Se elaboran "matrices de riesgo", en donde se consideran los factores de las "Amenazas" a las que está sometida una instalación y los "Impactos" que aquellas puedan causar cuando se presentan. Las matrices de riesgo se representan en cuadros de doble entrada <<Amenaza-Impacto>>, en donde se evalúan las probabilidades de ocurrencia de los elementos de la matriz.

Ejemplo:

Impacto	Amenaza				1: Improbable 2: Probable 3: Certeza -: Despreciable
	Error	Incendio	Sabotaje	……..	
Destrucción de Hardware	-	1	1		
Borrado de Información	3	1	1		

El cuadro muestra que si por error codificamos un parámetro que ordene el borrado de un fichero, éste se borrará con certeza.

El caso de los Bancos en la República Argentina:

En la Argentina, el Banco Central (BCRA) les realiza una Auditoría de Seguridad de Sistemas a todos los Bancos, minoritarios y mayoristas. El Banco que es auditado le prepara a los auditores del BCRA un "demo" para que estos vean cual es el flujo de información dentro del Banco y que Aplicaciones están involucradas con ésta. Si los auditores detectan algún problema o alguna cosa que según sus normas no está bien, y en base a eso, emiten un informe que va, tanto a la empresa, como al mercado. Este, principalmente, es uno de los puntos básicos donde se analiza el riesgo de un banco, más allá de cómo se maneja. Cada Banco tiene cierto riesgo dentro del mercado; por un lado, está dado por como se mueve éste dentro del mercado (inversiones, réditos, etc.) y por otro lado, el como funcionan sus Sistemas. Por esto, todos los Bancos tienen auditoría interna y auditoría externa; y se los audita muy frecuentemente.

Herramientas y Técnicas para la Auditoría Informática:

Cuestionarios:

Las auditorías informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

Para esto, suele ser lo habitual comenzar solicitando la cumplimentación de cuestionarios preimpresos que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar.

Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación, y muy cuidados en su fondo y su forma.

Sobre esta base, se estudia y analiza la documentación recibida, de modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor. El cruzamiento de ambos tipos de información es una de las bases fundamentales de la auditoría.

Cabe aclarar, que esta primera fase puede omitirse cuando los auditores hayan adquirido por otro medios la información que aquellos preimpresos hubieran proporcionado.

Entrevistas:

El auditor comienza a continuación las relaciones personales con el auditado. Lo hace de tres formas:

1. Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.
2. Mediante "entrevistas" en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.
3. Por medio de entrevistas en las que el auditor sigue un método preestablecido de antemano y busca unas finalidades concretas.

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

Aparte de algunas cuestiones menos importantes, la entrevista entre auditor y auditado se basa fundamentalmente en el concepto de interrogatorio; es lo que hace un auditor, interroga y se interroga a sí mismo. El auditor informático experto entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con pulcritud a una serie de preguntas variadas,

también sencillas. Sin embargo, esta sencillez es solo aparente. Tras ella debe existir una preparación muy elaborada y sistematizada, y que es diferente para cada caso particular.

Checklist:

El auditor profesional y experto es aquél que reelabora muchas veces sus cuestionarios en función de los escenarios auditados. Tiene claro lo que necesita saber, y por qué. Sus cuestionarios son vitales para el trabajo de análisis, cruzamiento y síntesis posterior, lo cual no quiere decir que haya de someter al auditado a unas preguntas estereotipadas que no conducen a nada. Muy por el contrario, el auditor conversará y hará preguntas "normales", que en realidad servirán para la cumplimentación sistemática de sus Cuestionarios, de sus Checklists.

Hay opiniones que descalifican el uso de las Checklists, ya que consideran que leerle una pila de preguntas recitadas de memoria o leídas en voz alta descalifica al auditor informático. Pero esto no es usar Checklists, es una evidente falta de profesionalismo. El profesionalismo pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente.

El conjunto de estas preguntas recibe el nombre de Checklist. Salvo excepciones, las Checklists deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma.

Según la claridad de las preguntas y el talante del auditor, el auditado responderá desde posiciones muy distintas y con disposición muy variable. El auditado, habitualmente informático de profesión, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, precisamente a través de las preguntas que éste le formula. Esta percepción configura el principio de autoridad y prestigio que el auditor debe poseer.

Por ello, aun siendo importante tener elaboradas listas de preguntas muy sistematizadas, coherentes y clasificadas por materias, todavía lo es más el modo y el orden de su formulación. Las empresas externas de Auditoría Informática guardan sus Checklists, pero de poco sirven si el auditor no las utiliza adecuada y oportunamente. No debe olvidarse que la función auditora se ejerce sobre bases de autoridad, prestigio y ética.

El auditor deberá aplicar el Checklist de modo que el auditado responda clara y escuetamente. Se deberá interrumpir lo menos posible a éste, y solamente en los casos en que las respuestas se aparten sustancialmente de la pregunta. En algunas ocasiones, se hará necesario invitar a aquél a que exponga con mayor amplitud un tema concreto, y en cualquier caso, se deberá evitar absolutamente la presión sobre el mismo.

Algunas de las preguntas de las Checklists utilizadas para cada sector, deben ser repetidas. En efecto, bajo apariencia distinta, el auditor formulará preguntas equivalentes a las mismas o a distintas personas, en las mismas fechas, o en fechas diferentes. De este modo, se podrán descubrir con mayor facilidad los puntos contradictorios; el auditor deberá analizar los matices de las respuestas y reelaborar preguntas complementarias cuando hayan existido contradicciones, hasta conseguir la homogeneidad.

El entrevistado no debe percibir un excesivo formalismo en las preguntas. El auditor, por su parte, tomará las notas imprescindibles en presencia del auditado, y nunca escribirá cruces ni marcará cuestionarios en su presencia.

Los cuestionarios o Checklists responden fundamentalmente a dos tipos de "filosofía" de calificación o evaluación:

a. Checklist de rango

   Contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido (por ejemplo, de 1 a 5, siendo 1 la respuesta más negativa y el 5 el valor más positivo)

   Ejemplo de Checklist de rango:

   Se supone que se está realizando una auditoría sobre la seguridad física de una instalación y, dentro de ella, se analiza el control de los accesos de personas y cosas al Centro de Cálculo. Podrían formularse las preguntas que figuran a continuación, en donde las respuestas tiene los siguientes significados:

   1 : Muy deficiente.
   2 : Deficiente.
   3 : Mejorable.
   4 : Aceptable.
   5 : Correcto.

   Se figuran posibles respuestas de los auditados. Las preguntas deben sucederse sin que parezcan encorsetadas ni clasificadas previamente. Basta con que el auditor lleve un pequeño guión. La cumplimentación del Checklist no debe realizarse en presencia del auditado.

   -¿Existe personal específico de vigilancia externa al edificio?

-No, solamente un guarda por la noche que atiende además otra instalación adyacente.
<Puntuación: 1>
-Para la vigilancia interna del edificio, ¿Hay al menos un vigilante por turno en los aledaños del Centro de Cálculo?
-Si, pero sube a las otras 4 plantas cuando se le necesita.
<Puntuación: 2>
-¿Hay salida de emergencia además de la habilitada para la entrada y salida de máquinas?
-Si, pero existen cajas apiladas en dicha puerta. Algunas veces las quitan.
<Puntuación: 2>
-El personal de Comunicaciones, ¿Puede entrar directamente en la Sala de Computadoras?
-No, solo tiene tarjeta el Jefe de Comunicaciones. No se la da a su gente salvo causa muy justificada, y avisando casi siempre al Jefe de Explotación.
<Puntuación: 4>
El resultado sería el promedio de las puntuaciones: (1 + 2 + 2 + 4) /4 = 2,25 Deficiente.

b. Checklist Binaria

Es la constituida por preguntas con respuesta única y excluyente: Si o No. Aritméticamente, equivalen a 1(uno) o 0(cero), respectivamente.
Ejemplo de Checklist Binaria:
Se supone que se está realizando una Revisión de los métodos de pruebas de programas en el ámbito de Desarrollo de Proyectos.
-¿Existe Normativa de que el usuario final compruebe los resultados finales de los programas?
<Puntuación: 1>
-¿Conoce el personal de Desarrollo la existencia de la anterior normativa?
<Puntuación: 1>
-¿Se aplica dicha norma en todos los casos?
<Puntuación: 0>
-¿Existe una norma por la cual las pruebas han de realizarse con juegos de ensayo o copia de Bases de Datos reales?
<Puntuación: 0>
Obsérvese como en este caso están contestadas las siguientes preguntas:
-¿Se conoce la norma anterior?
<Puntuación: 0>
-¿Se aplica en todos los casos?
<Puntuación: 0>
Los Checklists de rango son adecuados si el equipo auditor no es muy grande y mantiene criterios uniformes y equivalentes en las valoraciones. Permiten una mayor precisión en la evaluación que en los checklist binarios. Sin embargo, la bondad del método depende excesivamente de la formación y competencia del equipo auditor.
Los Checklists Binarios siguen una elaboración inicial mucho más ardua y compleja. Deben ser de gran precisión, como corresponde a la suma precisión de la respuesta. Una vez construidas, tienen la ventaja de exigir menos uniformidad del equipo auditor y el inconveniente genérico del <si o no> frente a la mayor riqueza del intervalo.
No existen Checklists estándar para todas y cada una de las instalaciones informáticas a auditar. Cada una de ellas posee peculiaridades que hacen necesarios los retoques de adaptación correspondientes en las preguntas a realizar.

Trazas y/o Huellas:

Con frecuencia, el auditor informático debe verificar que los programas, tanto de los Sistemas como de usuario, realizan exactamente las funciones previstas, y no otras. Para ello se apoya en productos Software muy potentes y modulares que, entre otras funciones, rastrean los caminos que siguen los datos a través del programa.
Muy especialmente, estas "Trazas" se utilizan para comprobar la ejecución de las validaciones de datos previstas. Las mencionadas trazas no deben modificar en absoluto el Sistema. Si la herramienta auditora produce incrementos apreciables de carga, se convendrá de antemano las fechas y horas más adecuadas para su empleo.
Por lo que se refiere al análisis del Sistema, los auditores informáticos emplean productos que comprueban los valores asignados por Técnica de Sistemas a cada uno de los parámetros variables de las Librerías más importantes del mismo. Estos parámetros variables deben estar dentro de un intervalo marcado por el fabricante. A modo de ejemplo, algunas instalaciones descompensan el número de iniciadores de trabajos de determinados entornos o toman criterios especialmente restrictivos o

permisivos en la asignación de unidades de servicio según cuales tipos carga. Estas actuaciones, en principio útiles, pueden resultar contraproducentes si se traspasan los límites.
No obstante la utilidad de las Trazas, ha de repetirse lo expuesto en la descripción de la auditoría informática de Sistemas: el auditor informático emplea preferentemente la amplia información que proporciona el propio Sistema: Así, los ficheros de <Accounting> o de <contabilidad>, en donde se encuentra la producción completa de aquél, y los <Log*> de dicho Sistema, en donde se recogen las modificaciones de datos y se pormenoriza la actividad general.
Del mismo modo, el Sistema genera automáticamente exacta información sobre el tratamiento de errores de maquina central, periféricos, etc.
[La auditoría financiero-contable convencional emplea trazas con mucha frecuencia. Son programas encaminados a verificar lo correcto de los cálculos de nóminas, primas, etc.].
*Log:
El log vendría a ser un historial que informa que fue cambiando y cómo fue cambiando (información). Las bases de datos, por ejemplo, utilizan el log para asegurar lo que se llaman las transacciones. Las transacciones son unidades atómicas de cambios dentro de una base de datos; toda esa serie de cambios se encuadra dentro de una transacción, y todo lo que va haciendo la Aplicación (grabar, modificar, borrar) dentro de esa transacción, queda grabado en el log. La transacción tiene un principio y un fin, cuando la transacción llega a su fin, se vuelca todo a la base de datos. Si en el medio de la transacción se cortó por x razón, lo que se hace es volver para atrás. El log te permite analizar cronológicamente que es lo que sucedió con la información que está en el Sistema o que existe dentro de la base de datos.

Software de Interrogación:

Hasta hace ya algunos años se han utilizado productos software llamados genéricamente <paquetes de auditoría>, capaces de generar programas para auditores escasamente cualificados desde el punto de vista informático.
Más tarde, dichos productos evolucionaron hacia la obtención de muestreos estadísticos que permitieran la obtención de consecuencias e hipótesis de la situación real de una instalación.
En la actualidad, los productos Software especiales para la auditoría informática se orientan principalmente hacia lenguajes que permiten la interrogación de ficheros y bases de datos de la empresa auditada. Estos productos son utilizados solamente por los auditores externos, por cuanto los internos disponen del software nativo propio de la instalación.
Del mismo modo, la proliferación de las redes locales y de la filosofía "Cliente-Servidor", han llevado a las firmas de software a desarrollar interfaces de transporte de datos entre computadoras personales y mainframe, de modo que el auditor informático copia en su propia PC la información más relevante para su trabajo.
Cabe recordar, que en la actualidad casi todos los usuarios finales poseen datos e información parcial generada por la organización informática de la Compañía.
Efectivamente, conectados como terminales al "Host", almacenan los datos proporcionados por este, que son tratados posteriormente en modo PC. El auditor se ve obligado (naturalmente, dependiendo del alcance de la auditoría) a recabar información de los mencionados usuarios finales, lo cual puede realizar con suma facilidad con los polivalentes productos descritos. Con todo, las opiniones más autorizadas indican que el trabajo de campo del auditor informático debe realizarse principalmente con los productos del cliente.
Finalmente, ha de indicarse la conveniencia de que el auditor confeccione personalmente determinadas partes del Informe. Para ello, resulta casi imprescindible una cierta soltura en el manejo de Procesadores de Texto, paquetes de Gráficos, Hojas de Cálculo, etc.

11. Metodología de Trabajo de Auditoría Informática

El método de trabajo del auditor pasa por las siguientes etapas:

- Alcance y Objetivos de la Auditoría Informática.
- Estudio inicial del entorno auditable.
- Determinación de los recursos necesarios para realizar la auditoría.
- Elaboración del plan y de los Programas de Trabajo.
- Actividades propiamente dichas de la auditoría.
- Confección y redacción del Informe Final.
- Redacción de la Carta de Introducción o Carta de Presentación del Informe final.

Alcance y Objetivos de la Auditoría Informática

El alcance de la auditoría expresa los límites de la misma. Debe existir un acuerdo muy preciso entre auditores y clientes sobre las funciones, las materias y las organizaciones a auditar.
A los efectos de acotar el trabajo, resulta muy beneficioso para ambas partes expresar las excepciones de alcance de la auditoría, es decir cuales materias, funciones u organizaciones no van a ser auditadas.
Tanto los alcances como las excepciones deben figurar al comienzo del Informe Final.
Las personas que realizan la auditoría han de conocer con la mayor exactitud posible los objetivos a los que su tarea debe llegar. Deben comprender los deseos y pretensiones del cliente, de forma que las metas fijadas puedan ser cumplidas.
Una vez definidos los objetivos (objetivos específicos), éstos se añadirán a los objetivos generales y comunes de a toda auditoría Informática: La operatividad de los Sistemas y los Controles Generales de Gestión Informática.

Estudio Inicial del entorno auditable

Para realizar dicho estudio ha de examinarse las funciones y actividades generales de la informática.
Para su realización el auditor debe conocer lo siguiente:

Organización

Para el equipo auditor, el conocimiento de quién ordena, quién diseña y quién ejecuta es fundamental. Para realizar esto en auditor deberá fijarse en:

1) Organigrama:

El organigrama expresa la estructura oficial de la organización a auditar.

Si se descubriera que existe un organigrama fáctico diferente al oficial, se pondrá de manifiesto tal circunstancia.

2) Departamentos:

Se entiende como departamento a los órganos que siguen inmediatamente a la Dirección. El equipo auditor describirá brevemente las funciones de cada uno de ellos.

3) Relaciones Jerárquicas y funcionales entre órganos de la Organización:

El equipo auditor verificará si se cumplen las relaciones funcionales y Jerárquicas previstas por el organigrama, o por el contrario detectará, por ejemplo, si algún empleado tiene dos jefes.

Las de Jerarquía implican la correspondiente subordinación. Las funcionales por el contrario, indican relaciones no estrictamente subordinables.

4) Flujos de Información:

Además de las corrientes verticales intradepartamentales, la estructura organizativa cualquiera que sea, produce corrientes de información horizontales y oblicuas extradepartamentales.

Los flujos de información entre los grupos de una organización son necesarios para su eficiente gestión, siempre y cuando tales corrientes no distorsionen el propio organigrama.

En ocasiones, las organizaciones crean espontáneamente canales alternativos de información, sin los cuales las funciones no podrían ejercerse con eficacia; estos canales alternativos se producen porque hay pequeños o grandes fallos en la estructura y en el organigrama que los representa.

Otras veces, la aparición de flujos de información no previstos obedece a afinidades personales o simple comodidad. Estos flujos de información son indeseables y producen graves perturbaciones en la organización.

5) Número de Puestos de trabajo

El equipo auditor comprobará que los nombres de los Puesto de los Puestos de Trabajo de la organización corresponden a las funciones reales distintas.

Es frecuente que bajo nombres diferentes se realicen funciones idénticas, lo cual indica la existencia de funciones operativas redundantes.

Esta situación pone de manifiesto deficiencias estructurales; los auditores darán a conocer tal circunstancia y expresarán el número de puestos de trabajo verdaderamente diferentes.

6) Número de personas por Puesto de Trabajo

Es un parámetro que los auditores informáticos deben considerar. La inadecuación del personal determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.

Entorno Operacional

El equipo de auditoría informática debe poseer una adecuada referencia del entorno en el que va a desenvolverse.
Este conocimiento previo se logra determinando, fundamentalmente, los siguientes extremos:

a. Situación geográfica de los Sistemas:

Se determinará la ubicación geográfica de los distintos Centros de Proceso de Datos en la empresa. A continuación, se verificará la existencia de responsables en cada unos de ellos, así como el uso de los mismos estándares de trabajo.

b. Arquitectura y configuración de Hardware y Software:
Cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado. La configuración de los sistemas esta muy ligada a las políticas de seguridad lógica de las compañías.
Los auditores, en su estudio inicial, deben tener en su poder la distribución e interconexión de los equipos.

c. Inventario de Hardware y Software:
El auditor recabará información escrita, en donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto a Hardware figurarán las CPUs, unidades de control local y remotas, periféricos de todo tipo, etc.
El inventario de software debe contener todos los productos lógicos del Sistema, desde el software básico hasta los programas de utilidad adquiridos o desarrollados internamente. Suele ser habitual clasificarlos en facturables y no facturables.

d. Comunicación y Redes de Comunicación:
En el estudio inicial los auditores dispondrán del número, situación y características principales de las líneas, así como de los accesos a la red pública de comunicaciones.
Igualmente, poseerán información de las Redes Locales de la Empresa.

Aplicaciones bases de datos y ficheros

El estudio inicial que han de realizar los auditores se cierra y culmina con una idea general de los procesos informáticos realizados en la empresa auditada. Para ello deberán conocer lo siguiente:

a. Volumen, antigüedad y complejidad de las Aplicaciones
b. Metodología del Diseño

Se clasificará globalmente la existencia total o parcial de metodología en el desarrollo de las aplicaciones. Si se han utilizados varias a lo largo del tiempo se pondrá de manifiesto.

c. Documentación

La existencia de una adecuada documentación de las aplicaciones proporciona beneficios tangibles e inmediatos muy importantes.
La documentación de programas disminuye gravemente el mantenimiento de los mismos.

d. Cantidad y complejidad de Bases de Datos y Ficheros.

El auditor recabará información de tamaño y características de las Bases de Datos, clasificándolas en relación y jerarquías. Hallará un promedio de número de accesos a ellas por hora o días. Esta operación se repetirá con los ficheros, así como la frecuencia de actualizaciones de los mismos.
Estos datos proporcionan una visión aceptable de las características de la carga informática.

Determinación de los recursos necesarios para realizar la auditoría

Mediante los resultados del estudio inicial realizado se procede a determinar los recursos humanos y materiales que han de emplearse en la auditoría.

Recursos materiales

Es muy importante su determinación, por cuanto la mayoría de ellos son proporcionados por el cliente. Las herramientas software propias del equipo van a utilizarse igualmente en el sistema auditado, por lo que han de convenirse en lo posible las fechas y horas de uso entre el auditor y cliente.
Los recursos materiales del auditor son de dos tipos:

a. Recursos materiales Software

Programas propios de la auditoria: Son muy potentes y Flexibles. Habitualmente se añaden a las ejecuciones de los procesos del cliente para verificarlos.
Monitores: Se utilizan en función del grado de desarrollo observado en la actividad de Técnica de Sistemas del auditado y de la cantidad y calidad de los datos ya existentes.

b. Recursos materiales Hardware

Los recursos hardware que el auditor necesita son proporcionados por el cliente. Los procesos de control deben efectuarse necesariamente en las Computadoras del auditado.
Para lo cuál habrá de convenir, tiempo de maquina, espacio de disco, impresoras ocupadas, etc.

Recursos Humanos
La cantidad de recursos depende del volumen auditable. Las características y perfiles del personal seleccionado depende de la materia auditable.
Es igualmente reseñable que la auditoría en general suele ser ejercida por profesionales universitarios y por otras personas de probada experiencia multidisciplinaria.

12. Perfiles Profesionales de los auditores informáticos

Profesión	Actividades y conocimientos deseables
Informático Generalista	Con experiencia amplia en ramas distintas. Deseable que su labor se haya desarrollado en Explotación y en Desarrollo de Proyectos. Conocedor de Sistemas.
Experto en Desarrollo de Proyectos	Amplia experiencia como responsable de proyectos. Experto analista. Conocedor de las metodologías de Desarrollo más importantes.
Técnico de Sistemas	Experto en Sistemas Operativos y Software Básico. Conocedor de los productos equivalentes en el mercado. Amplios conocimientos de Explotación.
Experto en Bases de Datos y Administración de las mismas.	Con experiencia en el mantenimiento de Bases de Datos. Conocimiento de productos compatibles y equivalentes. Buenos conocimientos de explotación
Experto en Software de Comunicación	Alta especialización dentro de la técnica de sistemas. Conocimientos profundos de redes. Muy experto en Subsistemas de teleproceso.
Experto en Explotación y Gestión de CPD´S	Responsable de algún Centro de Cálculo. Amplia experiencia en Automatización de trabajos. Experto en relaciones humanas. Buenos conocimientos de los sistemas.
Técnico de Organización	Experto organizador y coordinador. Especialista en el análisis de flujos de información.
Técnico de evaluación de Costes	Economista con conocimiento de Informática. Gestión de costes.

Elaboración del Plan y de los programas de trabajo

Una vez asignados los recursos, el responsable de la auditoría y sus colaboradores establecen un plan de trabajo. Decidido éste, se procede a la programación del mismo.
El plan se elabora teniendo en cuenta, entre otros criterios, los siguientes:

a) Si la Revisión debe realizarse por áreas generales o áreas específicas. En el primer caso, la elaboración es más compleja y costosa.

b) Si la auditoría es global, de toda la Informática, o parcial. El volumen determina no solamente el número de auditores necesarios, sino las especialidades necesarias del personal.

- En el plan no se consideran calendarios, porque se manejan recursos genéricos y no específicos.
- En el Plan se establecen los recursos y esfuerzos globales que van a ser necesarios.
- En el Plan se establecen las prioridades de materias auditables, de acuerdo siempre con las prioridades del cliente.
- El Plan establece disponibilidad futura de los recursos durante la revisión.
- El Plan estructura las tareas a realizar por cada integrante del grupo.

- En el Plan se expresan todas las ayudas que el auditor ha de recibir del auditado.

Una vez elaborado el Plan, se procede a la Programación de actividades. Esta ha de ser lo suficientemente como para permitir modificaciones a lo largo del proyecto.

Actividades propiamente dichas de la Auditoría

Auditoría por temas generales o por áreas específicas:
La auditoría Informática general se realiza por áreas generales o por áreas específicas. Si se examina por grandes temas, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos.

Cuando la auditoría se realiza por áreas específicas, se abarcan de una vez todas las peculiaridades que afectan a la misma, de forma que el resultado se obtiene más rápidamente y con menor calidad.

Técnicas de Trabajo:
- Análisis de la información recabada del auditado.
- Análisis de la información propia.
- Cruzamiento de las informaciones anteriores.
- Entrevistas.
- Simulación.
- Muestreos.

Herramientas:
- Cuestionario general inicial.
- Cuestionario Checklist.
- Estándares.
- Monitores.
- Simuladores (Generadores de datos).
- Paquetes de auditoría (Generadores de Programas).
- Matrices de riesgo.

Confección y redacción del Informe Final

La función de la auditoría se materializa exclusivamente por escrito. Por lo tanto la elaboración final es el exponente de su calidad.
Resulta evidente la necesidad de redactar borradores e informes parciales previos al informe final, los que son elementos de contraste entre opinión entre auditor y auditado y que pueden descubrir fallos de apreciación en el auditor.
Estructura del informe final:
El informe comienza con la fecha de comienzo de la auditoría y la fecha de redacción del mismo. Se incluyen los nombres del equipo auditor y los nombres de todas las personas entrevistadas, con indicación de la jefatura, responsabilidad y puesto de trabajo que ostente.
Definición de objetivos y alcance de la auditoría.
Enumeración de temas considerados:
Antes de tratarlos con profundidad, se enumerarán lo más exhaustivamente posible todos los temas objeto de la auditoría.
Cuerpo expositivo:
Para cada tema, se seguirá el siguiente orden a saber:

a) Situación actual. Cuando se trate de una revisión periódica, en la que se analiza no solamente una situación sino además su evolución en el tiempo, se expondrá la situación prevista y la situación real.
b) Tendencias. Se tratarán de hallar parámetros que permitan establecer tendencias futuras.
c) Puntos débiles y amenazas.
d) Recomendaciones y planes de acción. Constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la auditoría informática.
e) Redacción posterior de la Carta de Introducción o Presentación.

13. Modelo conceptual de la exposición del informe final

- El informe debe incluir solamente hechos importantes.

La inclusión de hechos poco relevantes o accesorios desvía la atención del lector.

- El Informe debe consolidar los hechos que se describen en el mismo.

El término de "hechos consolidados" adquiere un especial significado de verificación objetiva y de estar documentalmente probados y soportados. La consolidación de los hechos debe satisfacer, al menos los siguientes criterios:

1. El hecho debe poder ser sometido a cambios.

2. Las ventajas del cambio deben superar los inconvenientes derivados de mantener la situación.
3. No deben existir alternativas viables que superen al cambio propuesto.
4. La recomendación del auditor sobre el hecho debe mantener o mejorar las normas y estándares existentes en la instalación.

La aparición de un hecho en un informe de auditoría implica necesariamente la existencia de una debilidad que ha de ser corregida.

Flujo del hecho o debilidad:

1 – Hecho encontrado.
- Ha de ser relevante para el auditor y pera el cliente.
- Ha de ser exacto, y además convincente.
- No deben existir hechos repetidos.

2 – Consecuencias del hecho
- Las consecuencias deben redactarse de modo que sean directamente deducibles del hecho.

3 – Repercusión del hecho
- Se redactará las influencias directas que el hecho pueda tener sobre otros aspectos informáticos u otros ámbitos de la empresa.

4 – Conclusión del hecho
- No deben redactarse conclusiones más que en los casos en que la exposición haya sido muy extensa o compleja.

5 – Recomendación del auditor informático
- Deberá entenderse por sí sola, por simple lectura.
- Deberá estar suficientemente soportada en el propio texto.
- Deberá ser concreta y exacta en el tiempo, para que pueda ser verificada su implementación.
- La recomendación se redactará de forma que vaya dirigida expresamente a la persona o personas que puedan implementarla.

Carta de introducción o presentación del informe final:

La carta de introducción tiene especial importancia porque en ella ha de resumirse la auditoría realizada. Se destina exclusivamente al responsable máximo de la empresa, o a la persona concreta que encargo o contrato la auditoría.

Así como pueden existir tantas copias del informe Final como solicite el cliente, la auditoría no hará copias de la citada carta de Introducción.

La carta de introducción poseerá los siguientes atributos:

- Tendrá como máximo 4 folios.
- Incluirá fecha, naturaleza, objetivos y alcance.
- Cuantificará la importancia de las áreas analizadas.
- Proporcionará una conclusión general, concretando las áreas de gran debilidad.
- Presentará las debilidades en orden de importancia y gravedad.
- En la carta de Introducción no se escribirán nunca recomendaciones.

CRMR (Computer resource management review)

14. Definición de la metodología CRMR

CRMR son las siglas de <<Computer resource management review>>; su traducción más adecuada, Evaluación de la gestión de recursos informáticos. En cualquier caso, esta terminología quiere destacar la posibilidad de realizar una evaluación de eficiencia de utilización de los recursos por medio del management.

Una revisión de esta naturaleza no tiene en sí misma el grado de profundidad de una auditoría informática global, pero proporciona soluciones más rápidas a problemas concretos y notorios.

Supuestos de aplicación:

En función de la definición dada, la metodología abreviada CRMR es aplicable más a deficiencias organizativas y gerenciales que a problemas de tipo técnico, pero no cubre cualquier área de un Centro de Procesos de Datos.

El método CRMR puede aplicarse cuando se producen algunas de las situaciones que se citan:

- Se detecta una mala respuesta a las peticiones y necesidades de los usuarios.
- Los resultados del Centro de Procesos de Datos no están a disposición de los usuarios en el momento oportuno.
- Se genera con alguna frecuencia información errónea por fallos de datos o proceso.
- Existen sobrecargas frecuentes de capacidad de proceso.
- Existen costes excesivos de proceso en el Centro de Proceso de Datos.

Efectivamente, son éstas y no otras las situaciones que el auditor informático encuentra con mayor frecuencia. Aunque pueden existir factores técnicos que causen las debilidades descritas, hay que convenir en la mayor incidencia de fallos de gestión.

Areas de aplicación:

Las áreas en que el método CRMR puede ser aplicado se corresponden con las sujetas a las condiciones de aplicación señaladas en punto anterior:

- Gestión de Datos.
- Control de Operaciones.
- Control y utilización de recursos materiales y humanos.
- Interfaces y relaciones con usuarios.
- Planificación.
- Organización y administración.

Ciertamente, el CRMR no es adecuado para evaluar la procedencia de adquisición de nuevos equipos (Capacity Planning) o para revisar muy a fondo los caminos críticos o las holguras de un Proyecto complejo.

Objetivos:

CRMR tiene como objetivo fundamental evaluar el grado de bondad o ineficiencia de los procedimientos y métodos de gestión que se observan en un Centro de Proceso de Datos. Las Recomendaciones que se emitan como resultado de la aplicación del CRMR, tendrán como finalidad algunas de las que se relacionan:

- Identificar y fijas responsabilidades.
- Mejorar la flexibilidad de realización de actividades.
- Aumentar la productividad.
- Disminuir costes
- Mejorar los métodos y procedimientos de Dirección.

Alcance

Se fijarán los límites que abarcará el CRMR, antes de comenzar el trabajo.
Se establecen tres clases:

1. Reducido. El resultado consiste en señalar las áreas de actuación con potencialidad inmediata de obtención de beneficios.
2. Medio. En este caso, el CRMR ya establece conclusiones y Recomendaciones, tal y como se hace en la auditoría informática ordinaria.
3. Amplio. El CRMR incluye Planes de Acción, aportando técnicas de implementación de las Recomendaciones, a la par que desarrolla las conclusiones.

15. Información necesaria para la evaluación del CRMR

Se determinan en este punto los requisitos necesarios para que esta simbiosis de auditoría y consultoría pueda llevarse a cabo con éxito.

1. El trabajo de campo del CRMR ha de realizarse completamente integrado en la estructura del Centro de Proceso de Datos del cliente, y con los recursos de éste.
2. Se deberá cumplir un detallado programa de trabajo por tareas.
3. El auditor-consultor recabará determinada información necesaria del cliente.

Se tratan a continuación los tres requisitos expuestos:

1. Integración del auditor en el Centro de Procesos de Datos a revisar
   No debe olvidarse que se están evaluando actividades desde el punto de vista gerencial. El contacto permanente del auditor con el trabajo ordinario del Centro de Proceso de Datos permite a aquél determinar el tipo de esquema organizativo que se sigue.
2. Programa de trabajo clasificado por tareas

Todo trabajo habrá de ser descompuesto en tareas. Cada una de ellas se someterá a la siguiente sistemática:

- Identificación de la tarea.
- Descripción de la tarea.
- Descripción de la función de dirección cuando la tarea se realiza incorrectamente.
- Descripción de ventajas, sugerencias y beneficios que puede originar un cambio o modificación de tarea
- Test para la evaluación de la práctica directiva en relación con la tarea.

- Posibilidades de agrupación de tareas.
- Ajustes en función de las peculiaridades de un departamento concreto.
- Registro de resultados, conclusiones y Recomendaciones.

1. Información necesaria para la realización del CRMR

El cliente es el que facilita la información que el auditor contrastará con su trabajo de campo.
Se exhibe a continuación una Checklist completa de los datos necesarios para confeccionar el CRMR:

- Datos de mantenimiento preventivo de Hardware.
- Informes de anomalías de los Sistemas.
- Procedimientos estándar de actualización.
- Procedimientos de emergencia.
- Monitarización de los Sistemas.
- Informes del rendimiento de los Sistemas.
- Mantenimiento de las Librerías de Programas.
- Gestión de Espacio en disco.
- Documentación de entrega de Aplicaciones a Explotación.
- Documentación de alta de cadenas en Explotación.
- Utilización de CPU, canales y discos.
- Datos de paginación de los Sistemas.
- Volumen total y libre de almacenamiento.
- Ocupación media de disco.
- Manuales de Procedimientos de Explotación.

Esta información cubre ampliamente el espectro del CRMR y permite ejercer el seguimiento de las Recomendaciones realizadas.

Caso Práctico de una Auditoría de Seguridad Informática <<Ciclo de Seguridad>>

A continuación, un caso de auditoría de área general para proporcionar una visión más desarrollada y amplia de la función auditora.
Es una auditoría de Seguridad Informática que tiene como misión revisar tanto la seguridad física del Centro de Proceso de Datos en su sentido más amplio, como la seguridad lógica de datos, procesos y funciones informáticas más importantes de aquél.

Ciclo de Seguridad

El objetivo de esta auditoría de seguridad es revisar la situación y las cuotas de eficiencia de la misma en los órganos más importantes de la estructura informática.
Para ello, se fijan los supuestos de partida:
El área auditada es la Seguridad. El área a auditar se divide en: Segmentos.
Los segmentos se dividen en: Secciones.
Las secciones se dividen en: Subsecciones.
De este modo la auditoría se realizara en 3 niveles.
Los segmentos a auditar, son:

- Segmento 1: Seguridad de cumplimiento de normas y estándares.
- Segmento 2: Seguridad de Sistema Operativo.
- Segmento 3: Seguridad de Software.
- Segmento 4: Seguridad de Comunicaciones.
- Segmento 5: Seguridad de Base de Datos.
- Segmento 6: Seguridad de Proceso.
- Segmento 7: Seguridad de Aplicaciones.
- Segmento 8: Seguridad Física.

Se darán los resultados globales de todos los segmentos y se realizará un tratamiento exhaustivo del Segmento 8, a nivel de sección y subsección.
Conceptualmente la auditoria informática en general y la de Seguridad en particular, ha de desarrollarse en seis fases bien diferenciadas:
Fase 0. Causas de la realización del ciclo de seguridad.
Fase 1. Estrategia y logística del ciclo de seguridad.
Fase 2. Ponderación de sectores del ciclo de seguridad.
Fase 3. Operativa del ciclo de seguridad.
Fase 4. Cálculos y resultados del ciclo de seguridad.
Fase 5. Confección del informe del ciclo de seguridad.
A su vez, las actividades auditoras se realizan en el orden siguiente:

0. Comienzo del proyecto de Auditoría Informática.
1. Asignación del equipo auditor.
2. Asignación del equipo interlocutor del cliente.
3. Cumplimentación de formularios globales y parciales por parte del cliente.
4. Asignación de pesos técnicos por parte del equipo auditor.
5. Asignación de pesos políticos por parte del cliente.
6. Asignación de pesos finales a segmentos y secciones.
7. Preparación y confirmación de entrevistas.
8. Entrevistas, confrontaciones y análisis y repaso de documentación.
9. Calculo y ponderación de subsecciones, secciones y segmentos.
10. Identificación de áreas mejorables.
11. Elección de las áreas de actuación prioritaria.
12. Preparación de recomendaciones y borrador de informe
13. Discusión de borrador con cliente.
14. Entrega del informe.

Fase 0. Causas de realización de una Auditoría de Seguridad

Esta constituye la FASE 0 de la auditoría y el orden 0 de actividades de la misma.
El equipo auditor debe conocer las razones por las cuales el cliente desea realizar el Ciclo de Seguridad. Puede haber muchas causas: Reglas internas del cliente, incrementos no previstos de costes, obligaciones legales, situación de ineficiencia global notoria, etc.
De esta manera el auditor conocerá el entorno inicial. Así, el equipo auditor elaborará el Plan de Trabajo.

Fase 1. Estrategia y logística del ciclo de Seguridad

Se desarrolla en las siguientes actividades:
1. Designación del equipo auditor.
2. Asignación de interlocutores, validadores y decisores del cliente.
3. Cumplimentación de un formulario general por parte del cliente, para la realización del estudio inicial.

Con las razones por las cuales va a ser realizada la auditoría (Fase 0), el equipo auditor diseña el proyecto de Ciclo de Seguridad con arreglo a una estrategia definida en función del volumen y complejidad del trabajo a realizar, que constituye la Fase 1 del punto anterior.
Para desarrollar la estrategia, el equipo auditor necesita recursos materiales y humanos. La adecuación de estos se realiza mediante un desarrollo logístico, en el que los mismos deben ser determinados con exactitud. La cantidad, calidad, coordinación y distribución de los mencionados recursos, determina a su vez la eficiencia y la economía del Proyecto.
Los planes del equipo auditor se desarrolla de la siguiente manera:
1. Eligiendo el responsable de la auditoria su propio equipo de trabajo. Este ha de ser heterogéneo en cuanto a especialidad, pero compacto.
2. Recabando de la empresa auditada los nombres de las personas de la misma que han de relacionarse con los auditores, para las peticiones de información, coordinación de entrevistas, etc.
3. Mediante un estudio inicial, del cual forma parte el análisis de un formulario exhaustivo, también inicial, que los auditores entregan al cliente para su cumplimentación.
   Según los planes marcados, el equipo auditor, cumplidos los requisitos 1, 2 y 3, estará en disposición de comenzar la "tarea de campo", la operativa auditora del Ciclo de Seguridad.

Fase 2. Ponderación de los Sectores Auditados

Engloba las siguientes actividades:
1. Asignación de pesos técnicos. Se entienden por tales las ponderaciones que el equipo auditor hace de los segmentos y secciones, en función de su importancia.
2. Asignación de pesos políticos. Son las mismas ponderaciones anteriores, pero evaluadas por el cliente.
3. Asignación de pesos finales a los Segmentos y Secciones. El peso final es el promedio del peso técnico y del peso político. La Subsecciones se calculan pero no se ponderan.
   Se pondera la importancia relativa de la seguridad en los diversos sectores de la organización informática auditada.
   Las asignaciones de pesos a Secciones y Segmentos del área de seguridad que se audita, se realizan del siguiente modo:
   Pesos técnicos
   Son los coeficientes que el equipo auditor asigna a los Segmentos y a las Secciones.

Pesos políticos
Son los coeficientes o pesos que el cliente concede a cada Segmento y a cada Sección del Ciclo de Seguridad.

Ciclo de Seguridad. Suma Pesos Segmentos = 100 (con independencia del número de segmentos consideradas)			
Segmentos	Pesos Técnicos	Pesos Políticos	Pesos Finales
Seg1. Normas y Estándares	12	8	10
Seg2. Sistema Operativo	10	10	10
Seg3. Software Básico	10	14	12
Seg4. Comunicaciones	12	12	12
Seg5. Bases de Datos	12	12	12
Seg6. Procesos	16	12	14
Seg7. Aplicaciones	16	16	16
Seg8. Seguridad Física	12	16	14
TOTAL	**100**	**100**	**100**

Pesos finales
Son el promedio de los pesos anteriores.
El total de los pesos de los 8 segmentos es 100. Este total de 100 puntos es el que se ha asignado a la totalidad del área de Seguridad, como podría haberse elegido otro cualquiera. El total de puntos se mantiene cualquiera que hubiera sido el número de segmentos. Si hubieran existido cinco segmentos, en lugar de 8, la suma de los cinco habría de seguir siendo de 100 puntos.

Suma Peso Secciones = 20 (con independencia del número de Secciones consideradas)			
Secciones	**Pesos Técnicos**	**Pesos Políticos**	**Pesos Finales**
Secc1. Seg. Física de Datos	6	6	6
Secc2. Control de Accesos	5	3	4
Secc3. Equipos	6	4	5
Secc4. Documentos	2	4	3
Secc5. Suministros	1	3	2
TOTAL	20	20	20

Puede observarse la diferente apreciación de pesos por parte del cliente y del equipo auditor. Mientras éstos estiman que las Normas y Estándares y los Procesos son muy importantes, el cliente no los considera tanto, a la vez que prima, tal vez excesivamente, el Software Básico.
Del mismo modo, se concede a todos los segmentos el mismo valor total que se desee, por ejemplo 20, con absoluta independencia del número de Secciones que tenga cada Segmento. En este caso, se han definido y pesado cinco Secciones del Segmento de Seguridad Física. Cabe aclarar, solo se desarrolló un solo Segmento a modo de ejemplo.

Fase 3. Operativa del ciclo de Seguridad

Una vez asignados los pesos finales a todos los Segmentos y Secciones, se comienza la Fase 3, que implica las siguientes actividades:

1. Preparación y confirmación de entrevistas.
2. Entrevistas, pruebas, análisis de la información, cruzamiento y repaso de la misma.

Las entrevistas deben realizarse con exactitud. El responsable del equipo auditor designará a un encargado, dependiendo del área de la entrevista. Este, por supuesto, deberá conocer a fondo la misma.
La realización de entrevistas adecuadas constituye uno de los factores fundamentales del éxito de la auditoría. La adecuación comienza con la completa cooperación del entrevistado. Si esta no se produce, el responsable lo hará saber al cliente.
Deben realizarse varias entrevistas del mismo tema, al menos a dos o tres niveles jerárquicos distintos. El mismo auditor puede, y en ocasiones es conveniente, entrevistar a la misma persona sobre distintos

temas. Las entrevistas deben realizarse de acuerdo con el plan establecido, aunque se pueden llegar a agregar algunas adicionales y sin planificación.
La entrevista concreta suele abarcar Subsecciones de una misma Sección tal vez una sección completa. Comenzada la entrevista, el auditor o auditores formularán preguntas al/los entrevistado/s. Debe identificarse quien ha dicho qué, si son más de una las personas entrevistadas.
Las Checklist's son útiles y en muchos casos imprescindibles. Terminadas las entrevistas, el auditor califica las respuestas del auditado (no debe estar presente) y procede al levantamiento de la información correspondiente.
Simultáneamente a las entrevistas, el equipo auditor realiza pruebas planeadas y pruebas sorpresa para verificar y cruzar los datos solicitados y facilitados por el cliente. Estas pruebas se realizan ejecutando trabajos propios o repitiendo los de aquél, que indefectiblemente deberán ser similares si se han reproducido las condiciones de carga de los Sistemas auditados. Si las pruebas realizadas por el equipo auditor no fueran consistentes con la información facilitada por el auditado, se deberá recabar nueva información y reverificar los resultados de las pruebas auditoras.
La evaluación de las Checklists, las pruebas realizadas, la información facilitada por el diente y el análisis de todos los datos disponibles, configuran todos los elementos necesarios para calcular y establecer los resultados de la auditoria, que se materializarán en el informe final.
A continuación, un ejemplo de auditoría de la Sección de Control de Accesos del Segmento de Seguridad Física:
Vamos a dividir a la Sección de Control de Accesos en cuatro Subsecciones:

1. Autorizaciones
2. Controles Automáticos
3. Vigilancia
4. Registros

En las siguientes Checklists, las respuestas se calificarán de 1 a 5, siendo1 la más deficiente y 5 la máxima puntuación.

Control de Accesos: **Autorizaciones**		
Preguntas	Respuestas	Puntos
¿Existe un único responsable de implementar la política de autorizaciones de entrada en el Centro de Cálculo?	Si, el Jefe de Explotación, pero el Director puede acceder a la Sala con acompañantes sin previo aviso.	4
¿Existe alguna autorización permanente de estancia de personal ajeno a la empresa?	Una sola. El técnico permanente de la firma suministradora.	5
¿Quiénes saben cuales son las personas autorizadas?	El personal de vigilancia y el Jefe de Explotación.	5
Además de la tarjeta magnética de identificación, ¿hay que pasar otra especial?	No, solamente la primera.	4
¿Se pregunta a las visitas si piensan visitar el Centro de Cálculo?	No, vale la primera autorización.	3
¿Se preveen las visitas al Centro de Cálculo con 24 horas al menos?	No, basta que vayan acompañados por el Jefe de Explotación o Director	3
TOTAL AUTORIZACIONES		**24/30 80%**

Control de Accesos: **Controles Automáticos**		
Preguntas	Respuestas	Puntos
¿Cree Ud. que los Controles Automáticos son adecuados?	Si, aunque ha de reconocerse que a pie puede llegarse por la noche hasta el edificio principal.	3
¿Quedan registradas todas las entradas y salidas del Centro de Cálculo?	No, solamente las del personal ajeno a Operación.	3
Al final de cada turno, ¿Se controla el número de entradas y salidas del personal de Operación?	Sí, y los vigilantes los reverifican.	5
¿Puede salirse del Centro de Cálculo sin tarjeta magnética?	Si, porque existe otra puerta de emergencia que puede abrirse desde adentro	3
TOTAL CONTROLES AUTOMATICOS		**14/20 70%**

Control de Accesos: **Vigilancia**		
Preguntas	Respuestas	Puntos
¿Hay vigilantes las 24 horas?	Sí.	5
¿Existen circuitos cerrados de TV exteriores?	Sí.	5
Identificadas las visitas, ¿Se les acompaña hasta la persona que desean ver?	No.	2
¿Conocen los vigilantes los terminales que deben quedar encendidos por la noche?	No, sería muy complicado.	2
TOTAL VIGILANCIA		**14/20 70%**

Control de Accesos: **Registros**		
Preguntas	Respuestas	Puntos
¿Existe una adecuada política de registros?	No, reconocemos que casi nunca, pero hasta ahora no ha habido necesidad.	1
¿Se ha registrado alguna vez a una persona?	Nunca.	1
¿Se abren todos los paquetes dirigidos a personas concretas y no a Informática?	Casi nunca.	1
¿Hay un cuarto para abrir los paquetes?	Si, pero no se usa siempre.	3
TOTAL REGISTROS		**6/20 30%**

Fase 4. Cálculos y Resultados del Ciclo de Seguridad

1. Cálculo y ponderación de Secciones y Segmentos. Las Subsecciones no se ponderan, solo se calculan.
2. Identificación de materias mejorables.
3. Priorización de mejoras.

En el punto anterior se han realizado las entrevistas y se han puntuado las respuestas de toda la auditoría de Seguridad.

El trabajo de levantamiento de información está concluido y contrastado con las pruebas. A partir de ese momento, el equipo auditor tiene en su poder todos los datos necesarios para elaborar el informe final. Solo faltaría calcular el porcentaje de bondad de cada área; éste se obtiene calculando el sumatorio de las respuestas obtenidas, recordando que deben afectarse a sus pesos correspondientes.

Una vez realizado los cálculos, se ordenaran y clasificaran los resultados obtenidos por materias mejorables, estableciendo prioridades de actuación para lograrlas.

Cálculo del ejemplo de las Subsecciones de la Sección de Control de Accesos:

Autorizaciones 80%

Controles Automáticos 70%

Vigilancia 70%

Registros 30%

Promedio de Control de Accesos 62,5%

Cabe recordar, que dentro del Segmento de Seguridad Física, la Sección de Control de Accesos tiene un peso final de 4.
Prosiguiendo con el ejemplo, se procedió a la evaluación de las otras cuatro Secciones, obteniéndose los siguientes resultados:

Ciclo de Seguridad: **Segmento 8, Seguridad Física.**		
Secciones	Peso	Puntos
Sección 1. Datos	6	57,5%
Sección 2. Control de Accesos	4	62,5%
Sección 3. Equipos (Centro de Cálculo)	5	70%
Sección 4. Documentos	3	52,5%
Sección 5. Suministros	2	47,2%

Conocidas los promedios y los pesos de las cinco Secciones, se procede a calcular y ponderar el Segmento 8 de Seguridad Física:
Seg. 8 = PromedioSección1 * peso + PromedioSecc2 * peso + PromSecc3 * peso + PromSecc4 * peso + PromSecc5 * peso / (peso1 + peso2 + peso3 + peso4 + peso5)
ó
Seg. 8 = (57,5 * 6) + (62,5 * 4) + (70 * 5) + (52,5 * 3) + (47,2 * 2) / 20
Seg. 8 = 59,85%
A continuación, la evaluación final de los demás Segmentos del ciclo de Seguridad:

Ciclo de Seguridad. Evaluación y pesos de Segmentos		
Segmentos	Pesos	Evaluación
Seg1. Normas y Estándares	10	61%
Seg2. Sistema Operativo	10	90%
Seg3. Software Básico	12	72%
Seg4. Comunicaciones	12	55%
Seg5. Bases de Datos	12	77,5%
Seg6. Procesos	14	51,2%
Seg7. Aplicaciones	16	50,5%
Seg8. Seguridad Física	14	59,8%
Promedio Total Area de Seguridad	**100**	**63,3%**

Sistemática seguida para el cálculo y evaluación del Ciclo de Seguridad:

a. Valoración de las respuestas a las preguntas específicas realizadas en las entrevistas y a los cuestionarios formulados por escrito.
b. Cálculo matemático de todas las subsecciones de cada sección, como media aritmética (promedio final) de las preguntas específicas. Recuérdese que las subsecciones no se ponderan.
c. Cálculo matemático de la Sección, como media aritmética (promedio final) de sus Subsecciones. La Sección calculada tiene su peso correspondiente.
d. Cálculo matemático del Segmento. Cada una de las Secciones que lo componen se afecta por su peso correspondiente. El resultado es el valor del Segmento, el cual, a su vez, tiene asignado su peso.
e. Cálculo matemático de la auditoría. Se multiplica cada valor de los Segmentos por sus pesos correspondientes, la suma total obtenida se divide por el valor fijo asignado a priori a la suma de los pesos de los segmentos.

Finalmente, se procede a mostrar las áreas auditadas con gráficos de barras, exponiéndose primero los Segmentos, luego las Secciones y por último las Subsecciones. En todos los casos sé referenciarán respecto a tres zonas: roja, amarilla y verde.
La zona roja corresponde a una situación de debilidad que requiere acciones a corto plazo. Serán las más prioritarias, tanto en la exposición del Informe como en la toma de medidas para la corrección.
La zona amarilla corresponde a una situación discreta que requiere acciones a medio plazo, figurando a continuación de las contenidas en la zona roja.
La zona verde requiere solamente alguna acción de mantenimiento a largo plazo.

Fase 5. Confección del Informe del Ciclo de Seguridad

1. Preparación de borrador de informe y Recomendaciones.
2. Discusión del borrador con el cliente.
3. Entrega del Informe y Carta de Introducción.

Ha de resaltarse la importancia de la discusión de los borradores parciales con el cliente. La referencia al cliente debe entenderse como a los responsables directos de los segmentos. Es de destacar que si hubiese acuerdo, es posible que el auditado redacte un contrainforme del punto cuestionado. Este acta se incorporará al Informe Final.

Las Recomendaciones del Informe son de tres tipos:

1. Recomendaciones correspondientes a la zona roja. Serán muy detalladas e irán en primer lugar, con la máxima prioridad. La redacción de las recomendaciones se hará de modo que sea simple verificar el cumplimiento de la misma por parte del cliente.
2. Recomendaciones correspondientes a la zona amarilla. Son las que deben observarse a medio plazo, e igualmente irán priorizadas.
3. Recomendaciones correspondientes a la zona verde. Suelen referirse a medidas de mantenimiento. Pueden ser omitidas. Puede detallarse alguna de este tipo cuando una acción sencilla y económica pueda originar beneficios importantes.

16. Empresas que realizan auditorías externas

Arthur Andersen:

Tiene 420 oficinas en todo el mundo, casi 40.000 profesionales, y factura alrededor de 2,8 billones de dólares anuales. Invierte 250 millones de dólares por año en educación y capacitación a medida. Menos del uno por ciento del presupuesto para entrenamiento se gasta fuera de la organización, aunque la cuota de educación que cada profesional recibe es prácticamente equivalente a un "master" norteamericano. Se dictan los cursos de la compañía en el multimillonario Centro para la Capacitación Profesional que Arthur Andersen posee cerca de Chicago, con capacidad para 1.700 estudiantes con cama y comida. En la Argentina, como en muchos otros mercados complejos, Arthur Andersen combina el tradicional papel de auditor con un rol más creativo como consejero, en el cual la firma ayuda a sus clientes a mejorar sus operaciones a través de la generación de ideas nuevas y mejoras en sistemas y prácticas comerciales. Este punto de vista en materia auditora permite que las dos unidades de la firma puedan, en muchos casos, trabajar juntas en la elaboración de proyectos especiales para empresas/clientes.

Price Waterhouse:

De llegar a fusionarse con la empresa consultora Coopers & Lybrand, tendrían una fuerza de trabajo de 135.000 personas, 8.500 socios y una facturación anual superior a los 13.000 millones de dólares.
Además, el gigante Andersen pasaría a ocupar el segundo lugar en el ránking de los Seis Grandes Internacionales.

Ernst & Young, etc.

17. Conclusión

Principalmente, con la realización de este trabajo práctico, la principal conclusión a la que hemos podido llegar, es que toda empresa, pública o privada, que posean Sistemas de Información medianamente complejos, deben de someterse a un control estricto de evaluación de eficacia y eficiencia. Hoy en día, el 90 por ciento de las empresas tienen toda su información estructurada en Sistemas Informáticos, de aquí, la vital importancia que los sistemas de información funcionen correctamente. La empresa hoy, debe/precisa informatizarse. El éxito de una empresa depende de la eficiencia de sus sistemas de información. Una empresa puede tener un staff de gente de primera, pero tiene un sistema informático propenso a errores, lento, vulnerable e inestable; si no hay un balance entre estas dos cosas, la empresa nunca saldrá a adelante. En cuanto al trabajo de la auditoría en sí, podemos remarcar que se precisa de gran conocimiento de Informática, seriedad, capacidad, minuciosidad y responsabilidad; la auditoría de Sistemas debe hacerse por gente altamente capacitada, una auditoría mal hecha puede acarrear consecuencias drásticas para la empresa auditada, principalmente económicas.