INGENIERÍA DE SOFTWARE AVANZADA

(SESIÓN 2)

1. LA AUDITORÍA INFORMÁTICA

1.1. Metodologías.

1.2. Técnicas.

Objetivo: Entender la necesidad de hacer auditorias informáticas que garanticen la seguridad de la información siguiendo metodologías y aplicando diversas técnicas.

1.1 Metodologías

La palabra metodología tiene tres raíces de origen griego: "Meto" que significa más allá, "odos" que significa camino y "logos" que significa estudio. El método es un plan bien trazado que al seguir una secuencia de pasos da un resultado. La metodología es su conjunto estudia los métodos.

En nuestro tema principal, el de las auditorías, vale la pena señalar que se requiere de metodologías que de manera ordenada sistematicen los procesos y permitan el alcance eficaz de la meta que toda auditoria persigue.

En otras palabras, establecer una metodología de trabajo al poner en marcha un proceso de auditoría que buscará errores o fallas y hará recomendaciones garantiza que la auditoría no interfiera causando más problemas de los que llegue a encontrar.

Las metodologías son necesarias para desarrollar cualquier proyecto que nos propongamos de manera ordenada y eficaz.

La auditoria informática solo identifica el nivel de "exposición" por la falta de controles mientras el análisis de riesgos facilita la evaluación de los riesgos y recomienda acciones en base al costo-beneficio de la misma.

Todas las metodologías existentes en seguridad de sistemas van encaminadas a establecer y mejorar un entramado de contramedidas que garanticen que la productividad de que las amenazas se materialicen en hechos sea lo mas baja posible o al menos quede reducida de una forma razonable en costo-beneficio.

Todas las metodologías existentes desarrolladas y utilizadas en la auditoría y el control informático, se puede agrupar en dos grandes familias:

Cualitativas: Basadas en el criterio y raciocinio humano capaz de definir un proceso de trabajo, para seleccionar en base al experiencia acumulada. Puede excluir riesgos significantes desconocidos (depende de la capacidad del profesional para usar el check-list/guía). Basadas en métodos estadísticos y lógica borrosa, que requiere menos recursos humanos / tiempo que las metodologías cuantitativas.

Ventajas:

- Enfoque lo amplio que se desee.
- Plan de trabajo flexible y reactivo.
- Se concentra en la identificación de eventos.

Desventajas

- Depende fuertemente de la habilidad y calidad del personal involucrado.
- Identificación de eventos reales más claros al no tener que aplicarles probabilidades complejas de calcular.
- Dependencia profesional.

Cuantitativas: Basadas en un modelo matemático numérico que ayuda a la realización del trabajo, están diseñadas par producir una lista de riesgos que pueden compararse entre sí con facilidad por tener asignados unos valores numérico. Están diseñadas para producir una lista de riesgos que pueden compararse entre si con facilidad por tener asignados unos valores numéricos.

Estos valores son datos de probabilidad de ocurrencia de un evento que se debe extraer de un riesgo de incidencias donde el número de incidencias tiende al infinito.

Metodologías en Auditoría Informática.

Las metodologías de auditoría informática son de tipo cualitativo/subjetivo. Se puede decir que son subjetivas por excelencia. Están basadas en profesionales de gran nivel de experiencia y formación, capaces de dictar recomendaciones técnicas, operativas y jurídicas, que exigen en gran profesionalidad y formación continua. Solo existen dos tipos de metodologías para la auditoría informática:

- **Controles Generales.-** Son el producto estándar de los auditores profesionales. El objetivo aquí es dar una opinión sobre la fiabilidad de los datos del computador para la auditoría financiera, es resultado es escueto y forma parte del informe de auditoría, en donde se hacen notar las vulnerabilidades encontradas. Están desprestigiadas ya que dependen en gran medida de la experiencia de los profesionales que las usan.

- **Metodologías de los auditores internos.-** Están formuladas por recomendaciones de plan de trabajo y de todo el proceso que se debe seguir. También se define el objetivo de la misma, que habrá que describirlo en el memorando de apertura al auditado. De la misma forma se describe en forma de cuestionarios genéricos, con una orientación de los controles a revisar. El auditor interno debe crear sus metodologías necesarias para auditar los distintos aspectos o áreas en el plan auditor.

METODOLOGÍA ROA Risk Oriented Approach

En la actualidad existen tres tipos de metodologías de auditoria informática:

- R.O.A. (RISK ORIENTED APPROACH), diseñada por Arthur Andersen.
- CHECKLIST o cuestionarios.
- AUDITORIA DE PRODUCTOS (por ejemplo, Red Local Windows NT; sistemas de Gestión de base de Datos DB2; paquete de seguridad RACF, etc.).

En sí las tres metodologías están basadas en la minimización de los riesgos, que se conseguirá en función de que existan los controles y de que éstos funcionen. En consecuencia el auditor deberá revisar estos controles y su funcionamiento.

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.***

Definición de Alcance y Objetivos

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.

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

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 remoto, 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

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

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.
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 recursos de la auditoría Informática

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

b. Recursos materiales Hardware

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.

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 dependen 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.

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 ala 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 de la Auditoría Informática

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.

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.

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.
2 – Consecuencias del hecho
3 – Repercusión del hecho
4 – Conclusión del hecho
5 – Recomendación del auditor informático

- Ha de ser relevante para el auditor y pera el cliente. - Ha de ser exacto, y además convincente.
- No deben existir hechos repetidos.
- Las consecuencias deben redactarse de modo que sean directamente deducibles del hecho.
- Se redactará las influencias directas que el hecho pueda tener sobre otros aspectos informáticos u otros

ámbitos de la empresa.
- No deben redactarse conclusiones más que en los
casos en que la exposición haya sido muy extensa o compleja.
- 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.

1.2 Técnicas

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. Fuente:

http://www.academia.edu/7336888/Auditoria_de_Sistemas_de_Informacion

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 la 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 tienen 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 de la Checklist no debe realizarse en presencia del auditado.

-¿Existe personal específico de vigilancia externa al edificio?
-No, solamente un guardia 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 mas que por 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>
Las Checklists de rango son adecuadas 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 la checklist binaria. Sin embargo, la bondad del método depende excesivamente de la formación y competencia del equipo auditor.

Las Checklists Binarias 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 para 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.

Modelo conceptual de la exposición del informe final:

[recopilado de
https://www.google.com.mx/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0CCYQFjAB&url=http%3A%2F%2Fitchetumal.edu.mx%2Fv2014%2Fpaginasvar%2FMaestros%2Fmduran%2FPresentaciones%2FUn3_Informe%2520final%2520de%2520la%2520Auditoria%2520de%2520sistemas.pps&ei=I_wpVLOsGYyzyASxuIHwCQ&usg=AFQjCNGWVoxCm6eYsRNr-iQFbTLKedNraw&sig2=Lc1-6CSq2nl66NlTpFb43A&bvm=bv.76247554,d.aWw]

Fases de la Auditoría
https://www.google.com.mx/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&cad=rja&uact=8&ved=0CDcQFjAG&url=http%3A%2F%2Fwww.trituradorausada.com%2Fore%2F19125.php&ei=nPwpVMTTIMeoyATg1oLoBg&usg=AFQjCNFcrpmVxvvZDPRmbUg0Smpzlfkutw&sig2=a1w0iBuOU_DBuRxgc6LfvA

Metodología de Trabajo de Auditoría Informática
https://www.google.com.mx/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CBsQFjAA&url=http%3A%2F%2Fwww.academia.edu%2F7663795%2FArea_Academica_Licenciatura_en_Sistemas_Computacionales_Materia_Auditoria_en_Informatica&ei=Jv0pVPjqAY-2yAT5goLIBA&usg=AFQjCNGopkVI9z9xRLGNhBSJIz3tbD0DIw&sig2=gKROcVhpjqD5kcmYFQ_cgA&bvm=bv.76247554,d.b2U