INGENIERÍA DE SOFTWARE AVANZADA

(SESIÓN 3)

1.3. Procedimientos.

1.4. Tecnologías.

Objetivo: Entender la necesidad de hacer auditorias informáticas que garanticen la seguridad de la información. Conocer los principales procedimientos y las más actualizadas tecnologías empleadas

1.3 Procedimientos

PROCEDIMIENTOS Y TÉCNICAS DE AUDITORIA.

Se requieren varios pasos para realizar una auditoría. El auditor de sistemas debe evaluar los riesgos globales y luego desarrollar un programa de auditoría que consta de objetivos de control y procedimientos de auditoría que deben satisfacer esos objetivos.

El proceso de auditoría exige que el auditor de sistemas reúna evidencia, evalúe fortalezas y debilidades de los controles existentes basado en la evidencia recopilada, y que prepare un informe de auditoría que presente esos temas en forma objetiva a la gerencia.

[tomado de https://www.google.com.mx/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0CCcQFjAC&url=http%3A%2F%2Fwww.hacienda.go.cr%2Fcentro%2Fdatos%2FArticulo%2FCONCEPTOS%2520DE%2520AUDITORIA%2520DE%2520SISTEMAS%2520DE%2520LA%2520INFORMACION.doc&ei=MP4pVIPuN8KtyATl24DYDg&usg=AFQjCNGvckIFJ9w4OmIYI1pYVwYXvRp-Vg&sig2=3MdQzHQe7BqKY1JKsIkWqA&bvm=bv.76477589,bs.1,d.cGU]

Asimismo, la gerencia de auditoría debe garantizar una disponibilidad y asignación adecuada de recursos para realizar el trabajo de auditoría además de las revisiones de seguimiento sobre las acciones correctivas emprendidas por la gerencia.

Planificación de la auditoría

Una planificación adecuada es el primer paso necesario para realizar auditorías de sistema eficaces. El auditor de sistemas debe comprender el ambiente del negocio en el

que se ha de realizar la auditoría así como los riesgos del negocio y control asociado.

A continuación se menciona algunas de las áreas que deben ser cubiertas durante la planificación de la auditoría:

a) Comprensión del negocio y de su ambiente.
b) Riesgo y materialidad de auditoría.
c) Técnicas de evaluación de Riesgos.
d) Objetivos de controles y objetivos de auditoría.
e) Procedimientos de auditoría.
[basado en http://www.oas.org/juridico/spanish/mesicic3_nic_nagun.pdf]

a) Comprensión del negocio y de su ambiente.
Al planificar una auditoría, el auditor de sistemas debe tener una comprensión de suficiente del ambiente total que se revisa. Debe incluir una comprensión general de las diversas prácticas comerciales y funciones relacionadas con el tema de la auditoría, así como los tipos de sistemas que se utilizan.
El auditor de sistemas también debe comprender el ambiente normativo en el que opera el negocio. Por ejemplo, a un banco se le exigirá requisitos de integridad de sistemas de información y de control que no están presentes en una empresa manufacturera.
Los pasos que puede llevar a cabo un auditor de sistemas para obtener una comprensión del negocio son: Recorrerlas instalaciones del ente. Lectura de material sobre antecedentes que incluyan publicaciones sobre esa industria, memorias e informes financieros.
Entrevistas a gerentes claves para comprender los temas comerciales esenciales. Estudio de los informes sobre normas o reglamentos. Revisión de planes estratégicos a largo plazo. Revisión de informes de auditorías anteriores.

b) Riesgo y materialidad de auditoría.
Se puede definir los riesgos de auditoría como aquellos riesgos de que la información pueda tener errores materiales o que el auditor de sistemas no pueda detectar un error que ha ocurrido. Los riesgos en auditoría pueden clasificarse de la siguiente manera:

Riesgo inherente: Cuando un error material no se puede evitar que suceda por

que no existen controles compensatorios relacionados que se puedan establecer.

Riesgo de Control: Cuando un error material no puede ser evitado o detectado en forma oportuna por el sistema de control interno.

Riesgo de detección: Es el riesgo de que el auditor realice pruebas exitosas a partir de un procedimiento inadecuado.

[Fuente: https://www.google.com.mx/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=0CDEQFjAD&url=http%3A%2F%2Fauditor2006.comunidadcoomeva.com%2Fblog%2Fuploads%2Fprocedimientos-auditoria.doc&ei=lv8pVIalBo-iyATYqIKoBQ&usg=AFQjCNEEkNrS8_BKsBtPwxInF2DIk01XhA&sig2=YPpFIMJxg3Y4jpFQx3Hy8w&bvm=bv.76477589,d.aWw]

c) Técnicas de evaluación de Riesgos.

Al determinar que áreas funcionales o temas de auditoría que deben auditarse, el auditor de sistemas puede enfrentarse ante una gran variedad de temas candidatos a la auditoría, el auditor de sistemas debe evaluar esos riesgos y determinar cuales de esas áreas de alto riesgo debe ser auditada.

d) Objetivos de controles y objetivos de auditoría.

El objetivo de un control es anular un riesgo siguiendo alguna metodología, el objetivo de auditoría es verificar la existencia de estos controles y que estén funcionando de manera eficaz, respetando las políticas de la empresa y los objetivos de la empresa.

Así pues tenemos por ejemplo como objetivos de auditoría de sistemas los siguientes: La información de los sistemas de información deberá estar resguardada de acceso incorrecto y se debe mantener actualizada. Cada una de las transacciones que ocurren en los sistemas es autorizada y es ingresada una sola vez.

Los cambios a los programas deben ser debidamente aprobados y probados. Los objetivos de auditoría se consiguen mediante los procedimientos de auditoría.

e) Procedimientos de auditoría.

Algunos ejemplos de procedimientos de auditoría son: Revisión de la documentación de sistemas e identificación de los controles existentes. Entrevistas con los especialistas técnicos a fin de conocer las técnicas y controles aplicados. Utilización de software de

manejo de base de datos para examinar el contenido de los archivos de datos. Técnicas de diagramas de flujo para documentar aplicaciones automatizadas.

Desarrollo del programa de auditoría.

Un programa de auditoría es un conjunto documentado de procedimientos diseñados para alcanzar los objetivos de auditoría planificados. El esquema típico de un programa de auditoría incluye lo siguiente:

Tema de auditoría: Donde se identifica el área a ser auditada.

Objetivos de Auditoría: Donde se indica el propósito del trabajo de auditoría a realizar.

Alcances de auditoría: Aquí se identifica los sistemas específicos o unidades de organización que se han de incluir en la revisión en un período de tiempo determinado.

Planificación previa: Donde se identifica los recursos y destrezas que se necesitan para realizar el trabajo así como las fuentes de información para pruebas o revisión y lugares físicos o instalaciones donde se va auditar.

Procedimientos de auditoría para:

- **Recopilación de datos.**
- **Identificación de lista de personas a entrevistar.**
- **Identificación y selección del enfoque del trabajo**
- **Identificación y obtención de políticas, normas y directivas.**
- **Desarrollo de herramientas y metodología para verificar controles existentes.**
- **Procedimientos para evaluar los resultados de las pruebas revisiones.**
- **Procedimientos de comunicación con la gerencia.**
- **Procedimientos de seguimiento**.

El programa de auditoría se convierte también en una guía para documentar los diversos pasos de auditoría y para señalar la ubicación del material de evidencia.

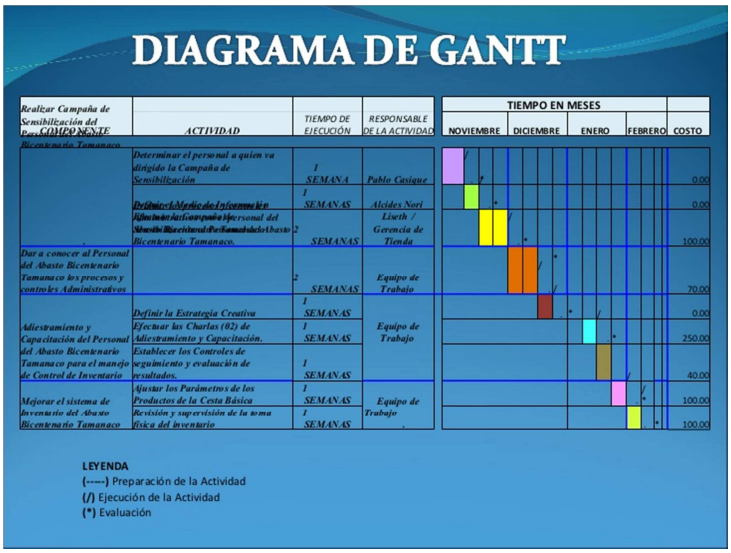
Los procedimientos involucran pruebas de cumplimiento o pruebas sustantivas, las de cumplimiento se hacen para verificar que los controles funcionan de acuerdo a las políticas y procedimientos establecidos y las pruebas sustantivas verifican si los controles establecidos por las políticas o procedimientos son eficaces.

Asignación de Recursos de auditoría.

[Recopilado de http://www.gestiopolis.com/recursos6/Docs/Fin/auditoria-concepto-funciones-1.htm]

La asignación de recursos para el trabajo de auditoría debe considerar las técnicas de administración de proyectos las cuales tienen los siguientes pasos básicos: Desarrollar un plan detallado: El plan debe precisar los pasos a seguir para cada tarea y estimar de manera realista, el tiempo teniendo en cuenta el personal disponible.

Contrastar la actividad actual con la actividad planificada en el proyecto: debe existir algún mecanismo que permita comparar el progreso real con lo planificado. Generalmente se utilizan las hojas de control de tiempo. Ajustar el plan y tomar las acciones correctivas: si al comparar el avance con lo proyectado se determina avances o retrasos, se debe reasignar tareas. El control se puede llevar en un diagrama de Gantt



Los recursos deben comprender también las habilidades con las que cuenta el grupo de trabajo de auditoría y el entrenamiento y experiencia que estos tengan. Tener en cuenta la disponibilidad del personal para la realización del trabajo de auditoría, como los períodos de vacaciones que estos tengan, otros trabajos que estén realizando, etc.

Técnicas de recopilación de evidencias.

[basado en prezi.com/la3uxwx6sdn7/auditoria/]

La recopilación de material de evidencia es un paso clave en el proceso de la auditoría, el

auditor de sistemas debe tener conocimiento de cómo puede recopilar la evidencia examinada. Algunas formas son las siguientes:

- Revisión de las estructuras organizacionales de sistemas de información.

- Revisión de documentos que inician el desarrollo del sistema, especificaciones de diseño funcional, historia de cambios a programas, manuales de usuario, especificaciones de bases de datos, arquitectura de archivos de datos, listados de programas, etc.; estos no necesariamente se encontrarán en documentos, sino en medios magnéticos para lo cual el auditor deberá conocer las formas de recopilarlos mediante el uso del computador.

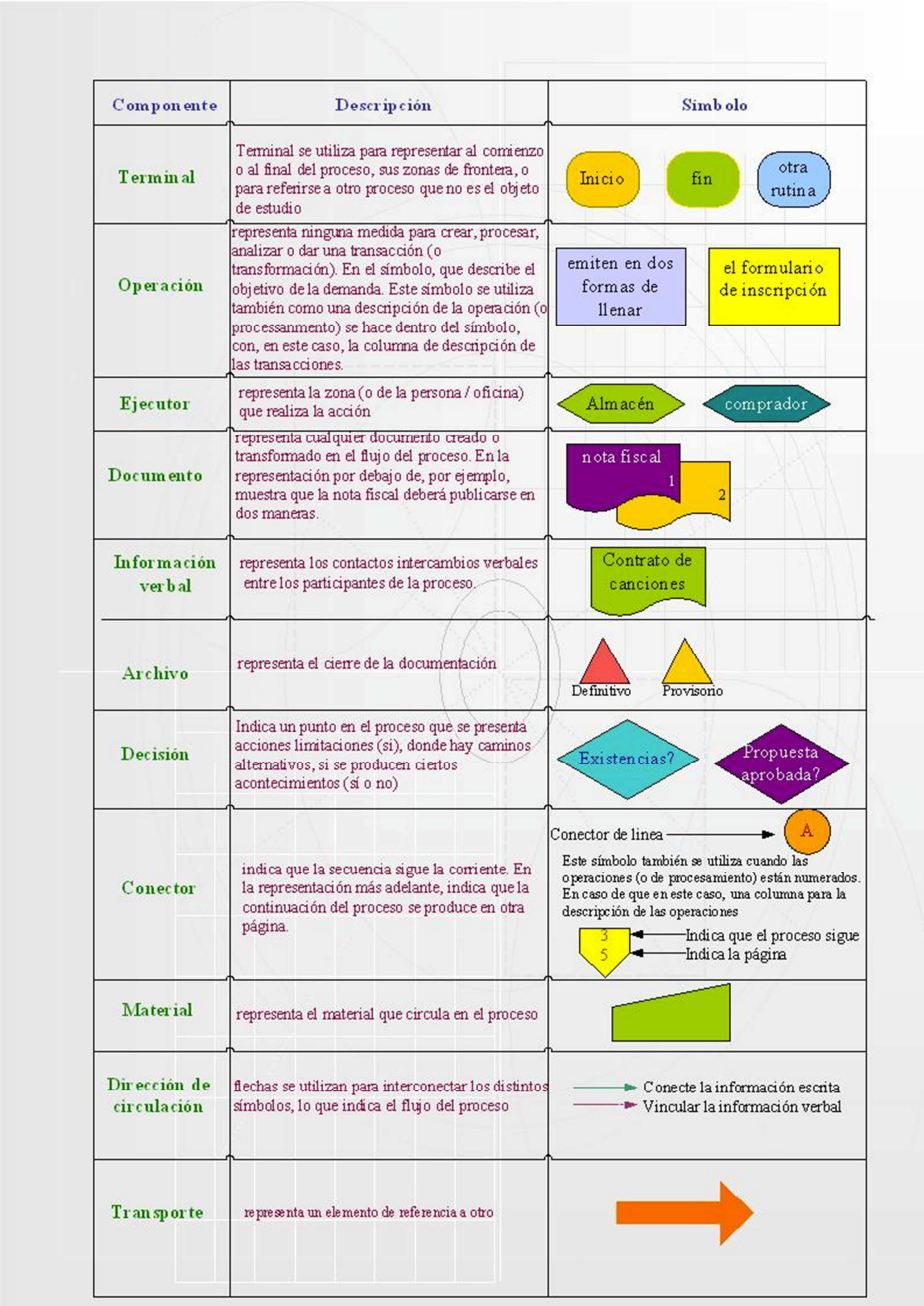
- Entrevistas con el personal apropiado, las cuales deben tener una naturaleza de descubrimiento no de acusatoria.

- Observación de operaciones y actuación de empleados, esta es una técnica importante para varios tipos de revisiones, para esto se debe documentar con el suficiente grado de detalle como para presentarlo como evidencia de auditoría.

- Auto documentación, es decir el auditor puede preparar narrativas en base a su observación, flujogramas, cuestionarios de entrevistas realizados.

- Aplicación de técnicas de muestreo para saber cuándo aplicar un tipo adecuado de pruebas (de cumplimiento o sustantivas) por muestras.

- Utilización de técnicas de auditoría asistida por computador CAAT, consiste en el uso de software genérico, especializado o utilitario.



Evaluación de fortalezas y debilidades de auditoría.

Luego de desarrollar el programa de auditoría y recopilar evidencia de auditoría, el siguiente paso es evaluar la información recopilada con la finalidad de desarrollar una opinión. Para esto generalmente se utiliza una matriz de control con la que se evaluará el

nivel de los controles identificados, esta matriz tiene sobre el eje vertical los tipos de errores que pueden presentarse en el área y un eje horizontal los controles conocidos para detectar o corregir los errores, luego se establece un puntaje (puede ser de 1 a 10 ó 0 a 20, la idea es que cuantifique calidad) para cada correspondencia, una vez completada, la matriz muestra las áreas en que los controles no existen o son débiles, obviamente el auditor debe tener el suficiente criterio para juzgar cuando no lo hay si es necesario el control.

En esta parte de evaluación de debilidades y fortalezas también se debe elegir o determinar la materialidad de las observaciones o hallazgos de auditoría. El auditor de sistemas debe juzgar cuales observaciones son materiales a diversos niveles de la gerencia y se debe informar de acuerdo a ello.

Informe de auditoría.

Los informes de auditoría son el producto final del trabajo del auditor de sistemas, este informe es utilizado para indicar las observaciones y recomendaciones a la gerencia, aquí también se expone la opinión sobre lo adecuado o lo inadecuado de los controles o procedimientos revisados durante la auditoría, no existe un formato específico para exponer un informe de auditoría de sistemas de información, pero generalmente tiene la siguiente estructura o contenido:

- Introducción al informe, donde se expresara los objetivos de la auditoría, el período o alcance cubierto por la misma, y una expresión general sobre la naturaleza o extensión de los procedimientos de auditoría realizados.
- Observaciones detalladas y recomendaciones de auditoría.
- Respuestas de la gerencia a las observaciones con respecto a las acciones correctivas.
- Conclusión global del auditor expresando una opinión sobre los controles y procedimientos revisados.

Seguimiento de las observaciones de auditoría.

El trabajo de auditoría es un proceso continuo, se debe entender que no serviría de nada el trabajo de auditoría si no se comprueba que las acciones correctivas tomadas por la gerencia, se están realizando, para esto se debe tener un programa de seguimiento, la oportunidad de seguimiento dependerá del carácter crítico de las observaciones de auditoría.

El nivel de revisión de seguimiento del auditor de sistemas dependerá de diversos factores, en algunos casos el auditor de sistemas tal vez solo necesite inquirir sobre la

situación actual, en otros casos tendrá que hacer una revisión más técnica del sistema.

PLANEACIÓN DE LA AUDITORÍA EN INFORMÁTICA

Para hacer una adecuada planeación de la auditoría en informática, hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características de área dentro del organismo a auditar, sus sistemas, organización y equipo.

En el caso de la auditoría en informática, la planeación es fundamental, pues habrá que hacerla desde el punto de vista de los dos objetivos:

- Evaluación de los sistemas y procedimientos.
- Evaluación de los equipos de cómputo.

Para hacer una planeación eficaz, lo primero que se requiere es obtener información general sobre la organización y sobre la función de informática a evaluar. Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas, con base en esto planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

INVESTIGACIÓN PRELIMINAR

Se deberá observar el estado general del área, su situación dentro de la organización, si existe la información solicitada, si es o no necesaria y la fecha de su última actualización.

Se debe hacer la investigación preliminar solicitando y revisando la información de cada una de las áreas basándose en los siguientes puntos:

ADMINISTRACIÓN

Se recopila la información para obtener una visión general del departamento por medio de observaciones, entrevistas preliminares y solicitud de documentos para poder definir el objetivo y alcances del departamento.

Para analizar y dimensionar la estructura por auditar se debe solicitar:

A NIVEL DEL ÁREA DE INFORMÁTICA.- Objetivos a corto y largo plazo.

RECURSOS MATERIALES Y TÉCNICOS.- Solicitar documentos sobre los equipos, número de ellos, localización y características.

- Estudios de viabilidad.
- Número de equipos, localización y las características (de los equipos instalados y por instalar y programados)
- Fechas de instalación de los equipos y planes de instalación.
- Contratos vigentes de compra, renta y servicio de mantenimiento.
- Contratos de seguros.

□□Convenios que se tienen con otras instalaciones.
□□Configuración de los equipos y capacidades actuales y máximas.
□□Planes de expansión.
□□Ubicación general de los equipos.
□□Políticas de operación.
□□Políticas de uso de los equipos.

SISTEMAS

Descripción general de los sistemas instalados y de los que estén por instalarse que contengan volúmenes de información.

□□Manual de formas.
□□Manual de procedimientos de los sistemas. □□Descripción genérica.
□□Diagramas de entrada, archivos, salida.
□□Salidas.
□□Fecha de instalación de los sistemas.
□□Proyecto de instalación de nuevos sistemas.

En el momento de hacer la planeación de la auditoría o bien su realización, debemos evaluar que pueden presentarse las siguientes situaciones.

Se solicita la información y se ve que:

□□No tiene pero es necesaria.
□□No se tiene y no se necesita.

Se tiene la información pero:

□□No se usa.
□□Es incompleta.
□□No esta actualizada.
□□No es la adecuada.
□□Se usa, está actualizada, es la adecuada y está completa.

En el caso de *No se tiene y no se necesita*, se debe evaluar la causa por la que no es necesaria. En el caso de *No se tiene pero es necesaria*, se debe recomendar que se elabore de acuerdo con las necesidades y con el uso que se le va a dar.

En el caso de que se tenga la información pero no se utilice, se debe analizar por que no se usa. En caso de que se tenga la información, se debe analizar si se usa, si está actualizada, si es la adecuada y si está completa.

El éxito del análisis crítico depende de las consideraciones siguientes:

- Estudiar hechos y no opiniones (no se toman en cuenta los rumores ni la información sin fundamento)
- Investigar las causas, no los efectos.
- Atender razones, no excusas.
- No confiar en la memoria, preguntar constantemente.
- Criticar objetivamente y a fondo todos los informes y los datos recabados.

PERSONAL PARTICIPANTE

Una de las partes más importantes dentro de la planeación de la auditoría en informática es el personal que deberá participar y sus características.

Uno de los esquemas generalmente aceptados para tener un adecuado control es que el personal que intervenga esté debidamente capacitado, con alto sentido de moralidad, al cual se le exija la optimización de recursos (eficiencia) y se le retribuya o compense justamente por su trabajo.

Con estas bases se debe considerar las características de conocimientos, práctica profesional y capacitación que debe tener el personal que intervendrá en la auditoría. En primer lugar se debe pensar que hay personal asignado por la organización, con el suficiente nivel para poder coordinar el desarrollo de la auditoría, proporcionar toda la información que se solicite y programar las reuniones y entrevistas requeridas.

Éste es un punto muy importante ya que, de no tener el apoyo de la alta dirección, ni contar con un grupo multidisciplinario en el cual estén presentes una o varias personas del área a auditar, sería casi imposible obtener información en el momento y con las características deseadas.

También se debe contar con personas asignadas por los usuarios para que en el momento que se solicite información o bien se efectúe alguna entrevista de comprobación de hipótesis, nos proporcionen aquello que se esta solicitando, y complementen el grupo multidisciplinario, ya que se debe analizar no sólo el punto de vista de la dirección de informática, sino también el del usuario del sistema.

Para completar el grupo, como colaboradores directos en la realización de la auditoría se deben tener personas con las siguientes características:

- Técnico en informática.
- Experiencia en el área de informática.

□□Experiencia en operación y análisis de sistemas. □□Conocimientos de los sistemas más importantes.
En caso de sistemas complejos se deberá contar con personal con conocimientos y experiencia en áreas específicas como base de datos, redes, etc. Lo anterior no significa que una sola persona tenga los conocimientos y experiencias señaladas, pero si deben intervenir una o varias personas con las características apuntadas.

El hecho de contar con la información del avance nos permite revisar el trabajo elaborado por cualquiera de los asistentes. Como ejemplo de propuesta de auditoría en informática.

1.4 Tecnologías

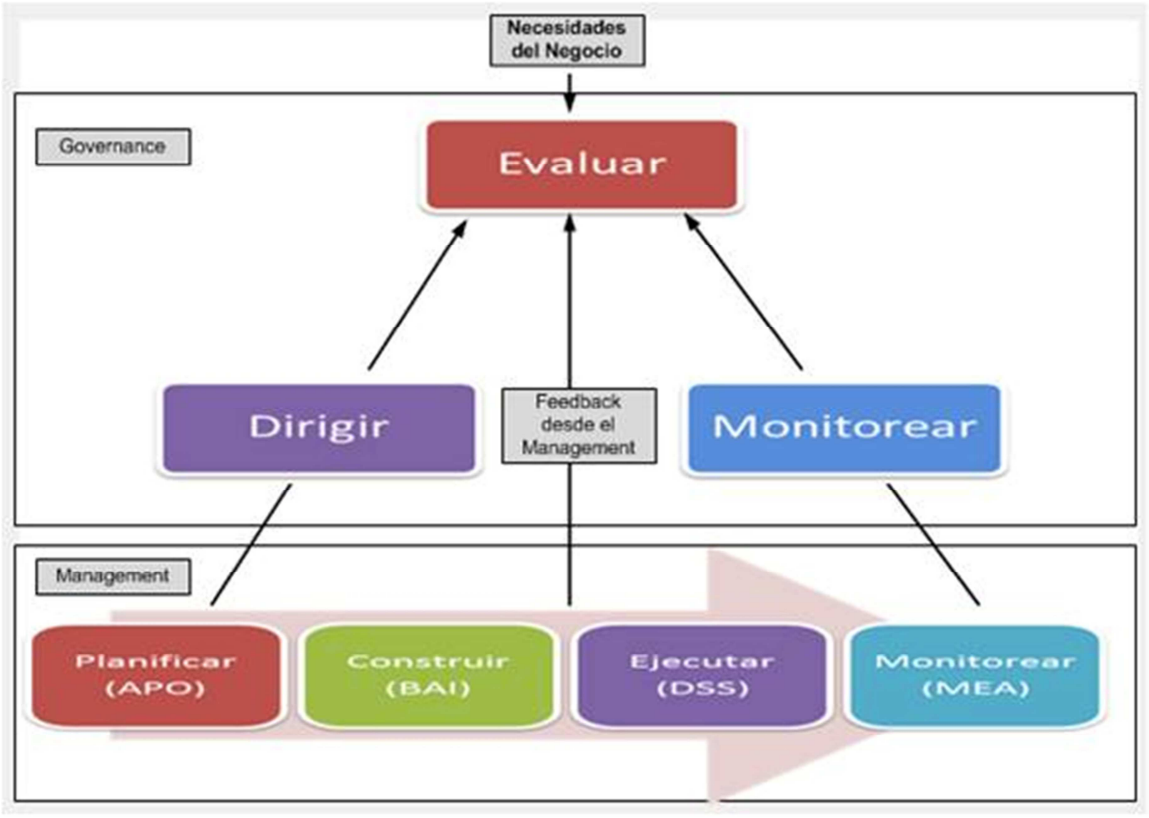
La necesidad de contar con lineamientos y herramientas estándar para el ejercicio de la auditoría informática ha promovido la creación y desarrollo de mejores prácticas como COBIT, COSO e ITIL.

Actualmente la certificación de ISACA para ser CISA *Certified Information Systems Auditor* es una de las más reconocidas y avaladas por los

estándares internacionales ya que el proceso de selección consta de un examen inicial bastante extenso y la necesidad de mantenerse actualizado acumulando horas (puntos) para no perder la certificación.

Objetivos de Control para la información y Tecnologías relacionadas (**COBIT**, en inglés: **Control Objectives for Information and related Technology**)

es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información,(ISACA, en inglés: Information Systems Audit and Control Association), y el Instituto de Administración de las Tecnologías de la Información (ITGI
, en inglés: IT Governance Institute) en 1992.

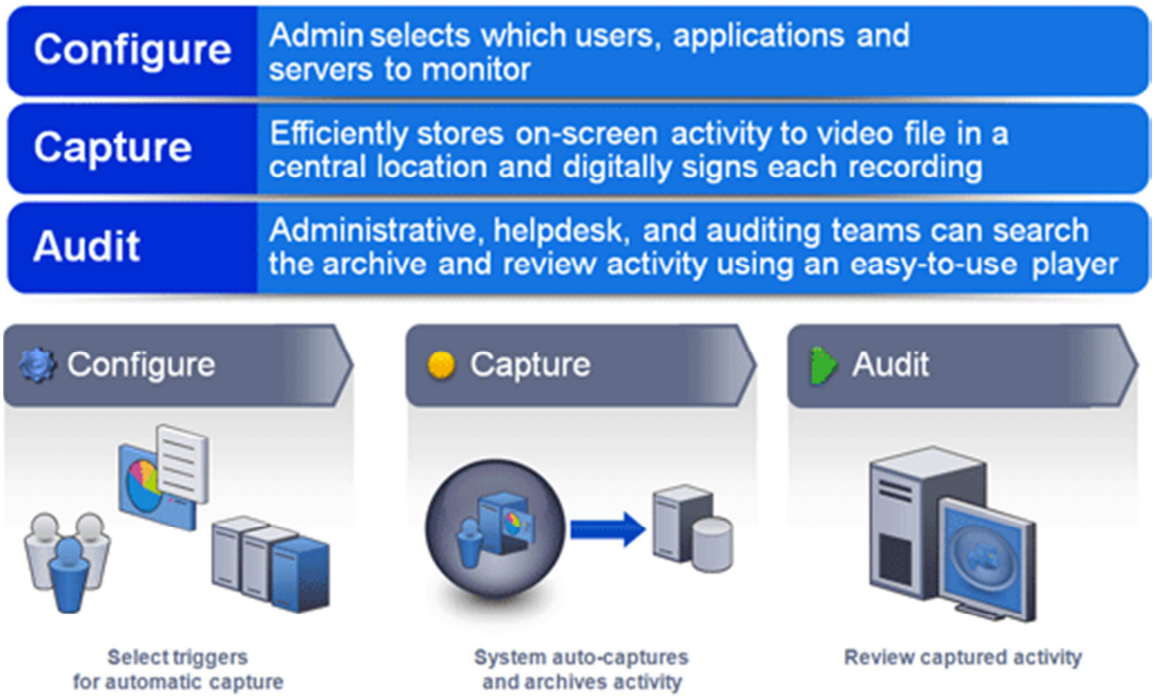


Partiendo de la realidad de que toda empresa usa recursos informáticos como computadoras, programas, etc. En la actualidad tiene mucha importancia la aplicación del concepto de auditoria informática como un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de la infraestructura informática de una empresa y si la inversión que se ha hecho en la misma cumple con los propósitos para lo cual fue desarrollada.

La auditoria informática es por lo tanto el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos, pues el progreso de la tecnología de la computación y la informática, está mejorando día a día, esto a la vez está
causando los problemas de las oportunidades a cometer errores, el revisar e inspeccionar es el trabajo de la auditoria para poder brindar un mejor trabajo de control a la sociedad y para un mejor control de la auditoria informática no nos podemos olvidar del control interno y la veracidad que debe tener, como cuando el sistema está en funcionamiento su evaluación y control se tienen que hacerse siempre.

Teniendo en cuenta que usando la computadora para auditar se necesita que el personal esté capacitado y conozca las herramientas y métodos aplicables para la Auditoria Informática, por ello la importancia del seminario en auditoria informática que ofrece HM Consulting y del cual damos más detalles en lo adelante.

Citrix anuncia SmartAuditor



Citrix Systems anunció SmartAuditor, nueva característica de Citrix Presentation Server que ayuda a monitorear, grabar y reproducir sesiones específicas de aplicaciones como parte de sus medidas progresivas de administración de riesgos y cumplimiento de las regulaciones. Incorporando la auditoría de la actividad de los usuarios como propiedad central de la infraestructura de entrega de aplicaciones existente de una compañía, SmartAuditor facilita a los clientes demostrar que los empleados siguen lineamientos establecidos para el acceso a información, integridad de las transacciones y protección de la propiedad intelectual.

Programas para auditoría informática

En el mercado existen una gran variedad de software o programas para la realización de auditoria informática en las empresas, dentro de los cuales queremos destacar los que son gratuitos como las herramientas Centennial Discovery, Gasp, Novell ZENworks Asset

Management®, y EasyVista que han sido diseñadas para ayudarles a identificar y realizar un seguimiento del software instalado en sus computadoras y redes.

Partiendo de que las auditorías son un componente clave en cualquier plan completo para la gestión de bienes de software. BSA pone estas herramientas a su disposición de forma gratuita, gracias a la cooperación de Attest Systems Inc., Centennial Software, Novell Inc. y Staff&Line.

Sugerimos que lean los acuerdos de licencia y cualquier otra información relacionada con el uso permitido. Para cada una de las herramientas se pueden destacar sus atributos como la GASP: una herramienta para auditoria de software, hardware y archivos, las versiones de esta herramienta se encuentran disponibles para plataformas Windows y Mac. Además está Centennial DiscoveryTM: una herramienta completa para auditoría y descubrimiento de la red.

Esta herramienta se encuentra disponible para las plataformas Windows, Mac, Unix y Linux. También ZENworks Asset Management: para inventario integrado de bienes, empleo de software, y conciliación de licencias. Esta herramienta funciona en plataformas Windows, Unix, Mac y Linux. La Staff&Line propone EasyVista, una gama integrada y modular que cubre todos los aspectos de Gestión de TI en una solución integrada y modular, 100% web, 100% ITIL v3. y Download EasyVista Trial.

Anuncian Oracle Audit Vault Oracle anunció la disponibilidad de Oracle Audit Vault a fin de que las empresas puedan abordar las dificultades relacionadas con los requisitos reglamentarios y las amenazas internas. Creado sobre un software confiable y escalable de la infraestructura de base de datos de Oracle, Oracle Audit Vault es una solución de gestión y consolidación de auditoría que permite a las empresas simplificar los informes de cumplimiento, detectar preventivamente las amenazas,
reducir costos y garantizar los datos de auditoría. Frente a las reglamentaciones y al temor de un incremento en las amenazas internas, las empresas están utilizando la auditoría de base de datos como una medida importante de seguridad, aplicando el principio trust-but-verify.

El 14% de los computadores tienen malware Según los datos recogidos durante la última semana en la web Infected or Not por las soluciones online NanoScan y TotalScan, el 14% de las computadoras analizadas tenían malware activo, es decir, amenazas que en el momento del análisis estaban llevando a cabo acciones maliciosas. Por su parte, el 25% del total de ordenadores analizados tenía malware latente, o lo que es lo mismo, amenazas que, simplemente, se encuentran en el sistema sin llevar a cabo acciones maliciosas. Del total de ordenadores analizados, el 72% contaba con algún tipo de protección antivirus instalada.

73% de las empresas fue víctima de delito digital en 2008

La consultora Ernst & Young presentó el primer estudio que se realiza sobre el delito digital.

La encuesta se realizó en 115 empresas de diferentes industrias.

La mayoría de los empresarios señalaron que en el 2008 fueron víctimas de un delito digital, el 29% son accesos ilegítimos (virus, malware, datos personales, denegación de servicio), 24% sustracción de dispositivos móviles (Smartphones, PDA, Notebooks, dispositivos externos de almacenamiento), 19% defraudaciones (manipulación y/o acceso de datos), 10% delitos extorsivos o similares, 8% correo electrónico, 6% la propiedad intelectual.