



Universidad Autónoma del Estado de Hidalgo



Escuela Superior de Tlahuelilpan

Área Académica: Sistemas
Computacionales

Tema: Auditoría Informática

Profesor(a): Academia de Administración
y Sociales

Periodo: Julio – Diciembre 2011





Tema:

Abstract

The opening every time bigger that Mexico is giving to material enterprises even international enterprises, the growing use of informatics technologies as tool for achieve competitive advantage and trying to control trough computational systems the growing volume of generated transactions by commercial and financial activities of Mexican institutions, they have make the surveillance and evaluation as constants of this systems.

Knowing the antecedents and concepts as fundamental of the audit matter as classifications and type definition of audits. The purpose is showing the elements that cement the existence of discipline of audit in general for the understanding the basic aspects of computational systems audits.

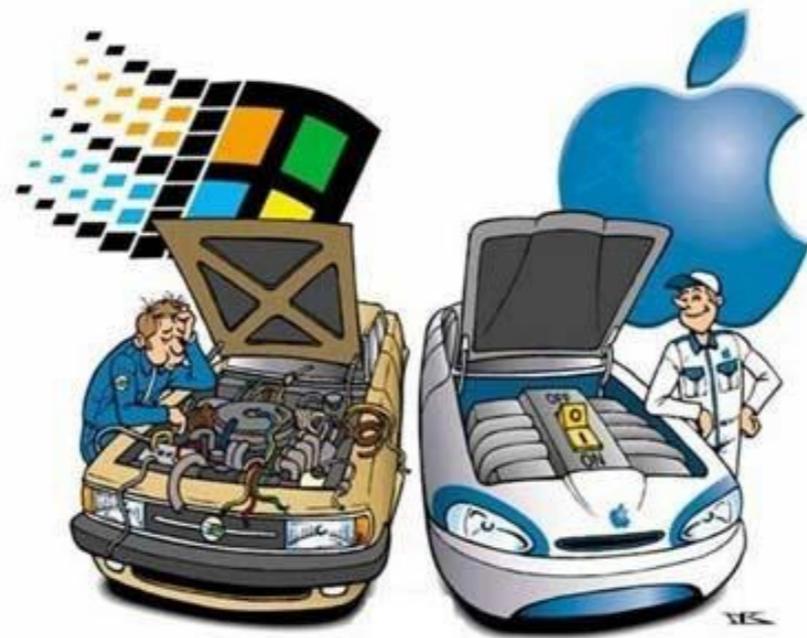
Keywords: audit, informatics, company, risk, threat, vulnerability, report, opinion.



Desarrollo del tema

1. INTRODUCCION
2. RIESGOS DE LA INFORMACIÓN Y EL CENTRO DE CÓMPUTO.
3. CONTROL INTERNO





1. Introducción

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.

Las organizaciones informáticas forman parte de lo que se ha denominado el "management" o gestión de la empresa. debido a su importancia en el funcionamiento de una empresa, existe la Auditoria Informática.

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.



Conceptos de Auditoría Informática

Es un examen que se realiza con carácter objetivo, crítico, sistemático y selectivo con el fin de evaluar la eficacia y eficiencia del uso adecuado de los recursos informáticos, de la gestión informática y si estas han brindado el soporte adecuado a los objetivos y metas del negocio.

Conceptos de Auditoria Informática

- La Auditoria de Tecnología de Información (T.I.) como se le conoce actualmente, (Auditoria informática o Auditoria de sistemas en nuestro medio), se ha consolidado en el mundo entero como cuerpo de conocimientos cierto y consistente, respondiendo a la acelerada evolución de la tecnología informática de los últimos 10 años.
- La INFORMACIÓN es considerada un activo tan o más importante que cualquier otro en una organización.

Conceptos de Auditoria Informática

Existe pues, un cuerpo de conocimientos, normas, técnicas y buenas practicas dedicadas a la evaluación y aseguramiento de la calidad, seguridad, razonabilidad, y disponibilidad de la INFORMACION tratada y almacenada a través del computador y equipos afines, así como de la eficiencia, eficacia y economía con que la administración de un ente están manejando dicha INFORMACION y todos los recursos físicos y humanos asociados para su adquisición, captura, procesamiento, transmisión, distribución, uso y almacenamiento. Todo lo anterior con el objetivo de emitir una opinión o juicio, para lo cual se aplican técnicas de auditoria de general aceptación y conocimiento técnico específico

OBJETIVOS DE LA AUDITORIA INFORMATICA

La Auditoría Informática deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

Objetivos De La Auditoría Informática

Esta es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo: informática, organización de centros de información, hardware y software.

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.

Alcance de la Auditoria Informática

- 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 definición de los alcances de la auditoria compromete el éxito de la misma.

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 auditoría 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.

Tipos y clases de Auditorías

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*.

Tipos y clases de Auditorías

- Estas tres auditorías, mas la auditoría de Seguridad, son las cuatro Áreas 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 Áreas Especificas de la Auditoría Informática más importantes

Auditoria 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.

Auditoría Informática de Desarrollo de Proyectos o Aplicaciones

Revisión del proceso completo de desarrollo de proyectos por parte de la empresa auditada.

El análisis se basa en cuatro aspectos fundamentales:

- *Revisión de las metodologías utilizadas:*

Se analizarán éstas, de modo que se asegure la modularidad de las posibles futuras ampliaciones de la Aplicación y el fácil mantenimiento de las mismas

- *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
- Definición Lógica de la Aplicación.
- Desarrollo Técnico de la Aplicación.
- Diseño de Programas.
- Métodos de Pruebas.
- Documentación.
- Equipo de Programación

- *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.

- *Control de Procesos y Ejecuciones de Programas Críticos:*

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 podría provocar graves y altos costos de mantenimiento, hasta fraudes, pasando por acciones de sabotaje, espionaje industrial informativo, etc.

Auditoría Informática de Sistemas

Se ocupa de analizar la actividad que se conoce como Técnica de Sistemas en todas sus facetas.

- 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.

- Software Básico:

Es fundamental para el auditor conocer los productos de software básico que han sido facturados aparte de la propia computadora. En cuanto al Software desarrollado por el personal informático de la empresa, el auditor debe verificar que éste no agreda ni condiciona al Sistema.

Software de Teleproceso (Tiempo Real)

No se incluye en Software Básico por su especialidad e importancia.

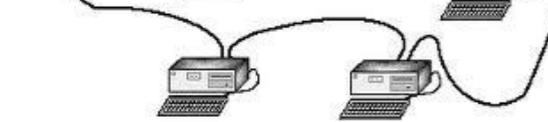
Tunning:

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.

Administración de Base de Datos:

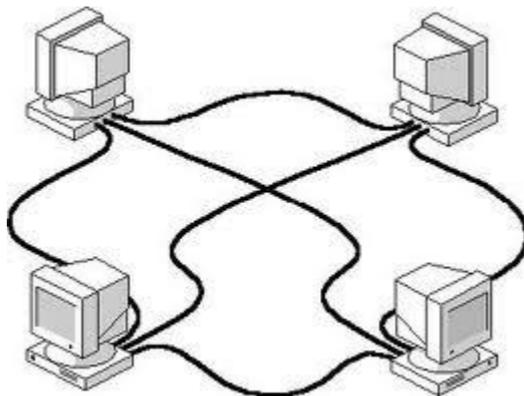
El diseño de las Bases de Datos, sean relaciones o jerárquicas, se ha convertido en una actividad muy compleja y sofisticada. La administración tendría que estar a cargo de Explotación.

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.



Auditoría Informática de Comunicaciones y Redes:

Revisión de la topología de Red y determinación de posibles mejoras, análisis de caudales y grados de utilización



Herramientas y Técnicas para la Auditoría Informática

- ***Cuestionarios***

Conjunto de preguntas a las que el sujeto puede responder oralmente o por escrito, cuyo fin es poner en evidencia determinados aspectos.

Características:

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.

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.

Entrevistas

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.

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

- ***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.



- ***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.

Las trazas se utilizan para comprobar la ejecución de las validaciones de datos previstas. Las mencionadas trazas no deben modificar en absoluto el Sistema.

2. Riesgos para la información

- Existen dos palabras muy importantes que son riesgo y seguridad:
- **Riesgo:** Es todo tipo de vulnerabilidades, amenazas que pueden ocurrir sin previo aviso y producir numerosas pérdidas para las empresas.
- **Seguridad:** Es una forma de protección contra lo
- Los riesgos mas perjudiciales son a las tecnologías información y comunicaciones.



Riesgos para la información

- Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la *confidencialidad*, la *autenticidad* y *Integridad* de la misma.
- El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas.

Riesgos para la información

- Para el hombre como individuo, la seguridad de la información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo.
- El campo de la seguridad de la información ha crecido y evolucionado considerablemente a partir de la Segunda Guerra Mundial, convirtiéndose en una carrera acreditada a nivel mundial.

Riesgos para la información

- **Importancia de la Información**

Se suele pasar por alto **la base** que hace posible la existencia de los anteriores elementos. Esta base es la *información* .

- La información:

- Esta almacenada y procesada en computadoras.
- Puede ser confidencial para algunas personas o a escala institucional.
- Puede ser mal utilizada o divulgada.
- Puede estar sujeta a robos, sabotaje o fraudes.



Riesgos para la información

En la actualidad gracias a la infinidad de posibilidades que se tiene para tener acceso a los recursos de manera remota y al gran incremento en las conexiones a la internet los delitos en el ámbito de TI se han visto incrementado, bajo estas circunstancias los riesgos informáticos son más latentes.

- Fraudes.
- Falsificación.
- Venta de información.
- Destrucción de la información.



Riesgos para la información

Principales atacantes

- **HACKER**
- **CRACKER**
- **LAMMER**
- **COPYHACKER**

Riesgos para la información

- **BUCANEROS**
- **PHREAKER**
- **NEWBIE**
- **SCRIPT KIDDIE** (“Skid kiddie”)

El manejo de riesgos dentro de la seguridad en la información

- **Evitar.**

No se permite ningún tipo de exposición. Esto se logra simplemente con no comprometerse a realizar la acción que origine el riesgo. Esta técnica tiene más desventajas que ventajas, ya que la empresa podría abstenerse de aprovechar muchas oportunidades.

- **Reducir.**

Cuando el riesgo no puede evitarse por tener varias dificultades de tipo operacional, la alternativa puede ser su reducción hasta el nivel más bajo posible. Esta opción es la más económica y sencilla. Se consigue optimizando los procedimientos, la implementación controles y su monitoreo constante.



El manejo de riesgos dentro de la seguridad en la información

- **Retener, Asumir o Aceptar el riesgo.**
 - Aceptar las consecuencias de la ocurrencia del evento.
 - Puede ser voluntaria o involuntaria, la voluntaria se caracteriza por el reconocimiento de la existencia del riesgo y el acuerdo de asumir las pérdidas involucradas, esta decisión se da por falta de alternativas.
 - La retención involuntaria se da cuando el riesgo es retenido inconscientemente.
- **Transferir.**
 - Es buscar un respaldo y compartir el riesgo con otros controles o entidades. Esta técnica se usa ya sea para eliminar un riesgo de un lugar y transferirlo a otro, ó para minimizar el mismo, compartiéndolo con otras entidades.

RIESGOS EN EL CENTRO DE CÓMPUTO

- Factores físicos.
- Factores ambientales
- Factores humanos

RIESGOS EN EL CENTRO DE CÓMPUTO

Factores físicos.

- Cableado.
- La iluminación
- El aire de renovación o ventilación
- Las fuentes de alimentación.



RIESGOS EN EL CENTRO DE CÓMPUTO

Factores ambientales

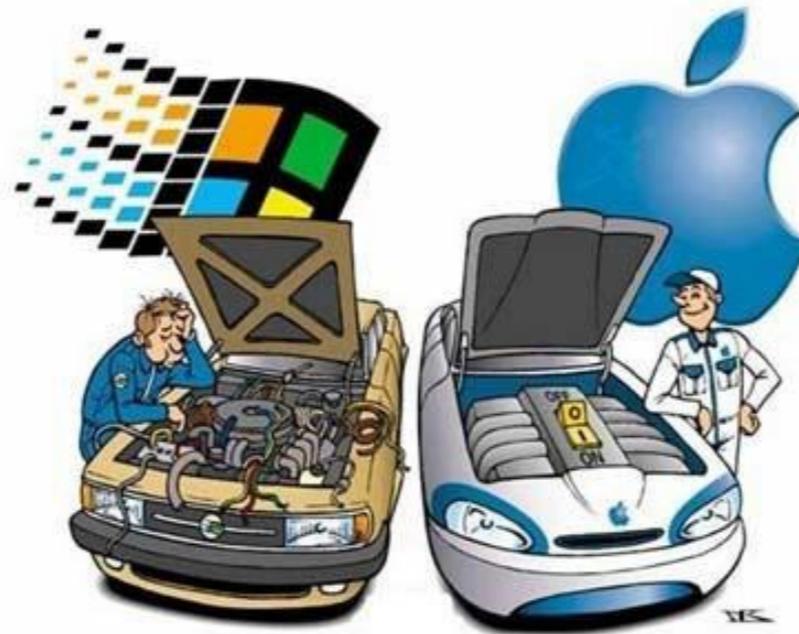
- Incendios.
- Inundaciones.
- Sismos.
- Humedad.

RIESGOS EN EL CENTRO DE CÓMPUTO

Factores humanos

- Robos.
- Actos vandálicos.
- Actos vandálicos contra el sistema de red
- Fraude.
- Sabotaje.
- Terrorismo.

RIESGO, EVIDENCIA Y PRUEBAS SUSTANTIVAS



Riesgo.

Es la probabilidad de que suceda un evento, impacto o consecuencia adversos. Se entiende también como la medida de la posibilidad y magnitud de los impactos adversos, siendo la consecuencia del peligro, y está en relación con la frecuencia con que se presente el evento.



Evidencia.

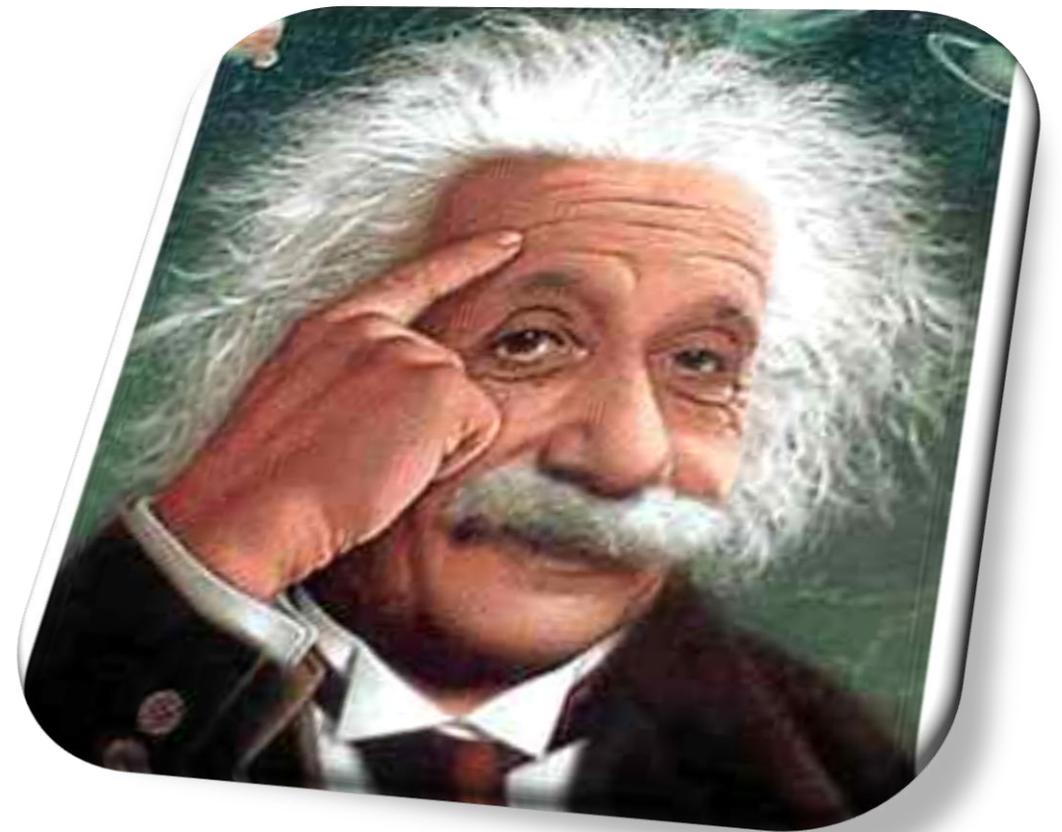
El auditor obtendrá la certeza suficiente y apropiada a través de la ejecución de sus comprobaciones de procedimientos para permitirle emitir las conclusiones sobre las que fundamentar su opinión acerca del estado del sistema de Informático.



La fiabilidad de la evidencia está en relación con la fuente de la que se obtenga interna y externa, y con su naturaleza, es decir, visual, documental y oral.



La Evidencia es la base razonable de la opinión del auditor informático, es decir el informe de Auditoria Informática.



Puntos para evaluar la fiabilidad de la evidencia

1. La evidencia externa es más fiable que la interna.
2. La evidencia interna es más fiable cuando los controles internos relacionados con ellos son satisfactorios.
3. La evidencia obtenida por el propio auditor es más fiable que la obtenida por la empresa.
4. La evidencia en forma de documentos y manifestaciones escritas es más fiable que la procedente de declaraciones orales.
5. El auditor puede ver aumentada su seguridad como la evidencia obtenida de diferentes fuentes.
6. Debe existir una razonable relación entre el costo de obtener una evidencia y la utilidad de la información que suministra.

La Evidencia tiene una serie de calificativos a saber:

La Evidencia Relevante, que tiene una relación lógica con los objetivos de la auditoria.

La Evidencia Fiable, que es valida y objetiva aunque, con nivel de confianza.

La Evidencia Suficiente, que es de tipo cuantitativo para soportar la opinión profesional del auditor.

La Evidencia Adecuada, que es de tipo cualitativo para afectar las conclusiones del auditor.

Métodos para la evidencia de auditoría:

Inspección: consiste en la revisión de la coherencia y concordancia de los registros, así como en el examen de los documentos y activos tangibles.

La observación: consiste en ver la ejecución de un proceso o procedimiento efectuado por otros.

Las preguntas: obtienen información apropiada de las personas de dentro y fuera de la entidad.

Las confirmaciones: mediante ellas se obtiene corroboración, normalmente por escrito, de una información contenida en los registros

Los cálculos: comprueban la exactitud aritmética de los registros y de los cálculos y análisis realizados por la entidad o en la realización de cálculos independientes.

En principio, las pruebas son de cumplimiento o sustantivas.

3. Control Interno

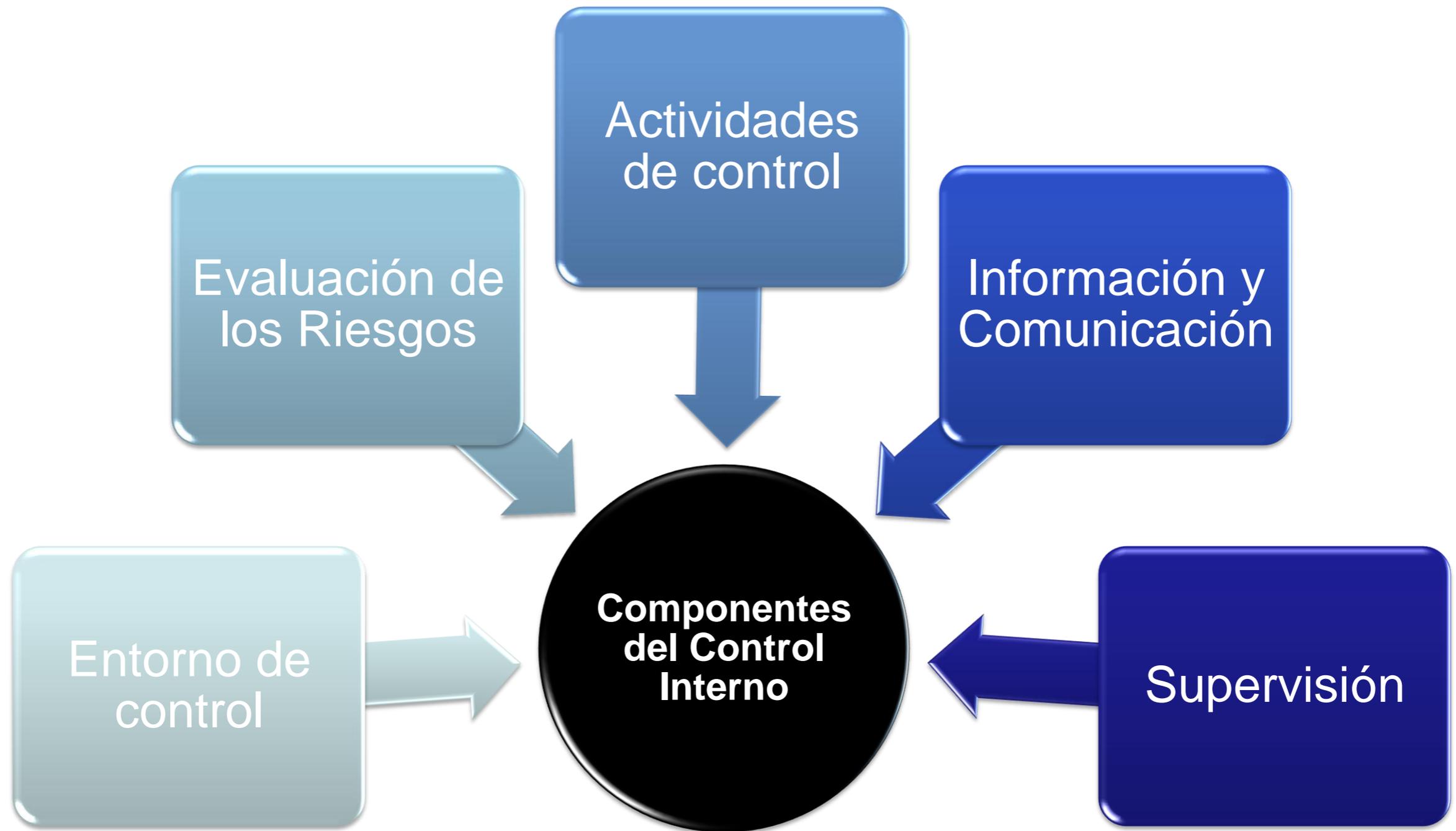
Control Interno como cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos. (Auditoría Informática - Un Enfoque Práctico - Mario G. Plattini)

El Informe COSO define el Control Interno como “Las normas, los procedimientos, las prácticas y las estructuras organizativas diseñadas para proporcionar seguridad razonable de que los objetivos de la empresa se alcanzarán y que los eventos no deseados se preverán, se detectarán y se corregirán.

En el ambiente informático, el control interno se materializa fundamentalmente en controles de dos tipos:

- Controles manuales: aquellos que son ejecutados por el personal del área usuaria o de informática sin la utilización de herramientas computacionales.
- Controles Automáticos: son generalmente los incorporados en el software, llámense estos de operación, de comunicación, de gestión de base de datos, programas de aplicación, etc.

Componentes del Control Interno



Actividades de Control

Son las políticas y procedimientos que ayudan a asegurar que se toman las medidas para limitar los riesgos que pueden afectar que se alcancen los objetivos organizacionales.

Información y Comunicación

Se debe identificar, ordenar y comunicar en forma oportuna la información necesaria para que los empleados puedan cumplir con sus obligaciones.

La información puede ser operativa o financiera, de origen interno o externo.

Deben existir adecuados canales de comunicación.

El personal debe ser informado de la importancia de que participe en el esfuerzo de aplicar el control interno.

Supervisión

Debe existir un proceso que compruebe que el sistema de control interno se mantiene en funcionamiento a través del tiempo.

La misma tiene tareas permanentes y revisiones periódicas. Estas últimas dependerán en cuanto a su frecuencia de la evaluación de la importancia de los riesgos en juego.

El Control Interno Informático

Sistema integrado al proceso administrativo, en la planeación, organización, dirección y control de las operaciones con el objeto de asegurar la protección de todos los recursos informáticos y mejorar los índices de economía, eficiencia y efectividad de los procesos operativos automatizados. (Auditoría Informática - Aplicaciones

en Producción - José Dagoberto Pinilla)

El control interno informático controla diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijados por la dirección de la organización y/o dirección de informática, así como los requerimientos legales

La misión del Control Interno Informático es asegurarse de que las medidas que se obtienen de los mecanismos implantados por cada responsable sean correctas y validas

Principales Objetivos

- Controlar que todas las actividades se realizan cumpliendo los procedimientos y normas fijados, evaluar su bondad y asegurarse del cumplimiento de las normas legales.
- Asesorar sobre el conocimiento de las normas
- Colaborar y apoyar el trabajo de Auditoría Informática interna/externa
- Definir, implantar y ejecutar mecanismos y controles para comprobar el logro de los grados adecuados del servicio informático

FUNCIONES ESPECIFICAS:

- Difundir y controlar el cumplimiento de las normas, estándares y procedimientos al personal de programadores, técnicos y operadores.
- Diseñar la estructura del Sistema de Control Interno de la Dirección de Informática en los siguientes aspectos:
 - Desarrollo y mantenimiento del software de aplicación.
 - Explotación de servidores principales
 - Software de Base
 - Redes de Computación
 - Seguridad Informática
 - Licencias de software
 - Cultura de riesgo informático en la organización
 - Control interno informático (áreas de aplicación)

CLASIFICACIÓN DE LOS CONTROLES INTERNOS INFORMÁTICOS

Controles Preventivos: Sirve para tratar de evitar un evento no deseado de todas las áreas de departamento como son: Equipo de cómputo, sistemas, telecomunicaciones.

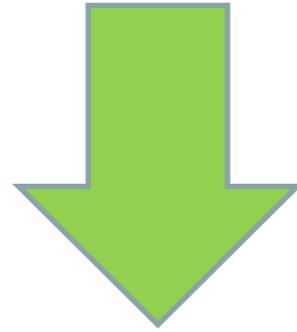
Ejemplo: contar con un software de seguridad que impida los accesos no autorizados al sistema.

Controles Detectivos: trata de descubrir a posteriori errores o fraudes que no haya sido posible evitarlos con controles preventivos. Ejemplo (registros de intentos de acceso no autorizados, el registro de la actividad diaria para detectar errores u omisiones).

Controles Correctivos: Tratan de asegurar que se subsanen todos los errores identificados, mediante los controles preventivos; es decir facilitan la vuelta a la normalidad ante una incidencia. Es un plan de contingencia.

Ejemplo: Back up supondría un control correctivo.

Sistema de control interno:



Es el conjunto de todos los elementos en donde lo principal son las personas, los sistemas de información, la supervisión y los procedimientos.

- Este es de vital importancia, ya que promueve la eficiencia, asegura la efectividad, previene
- que se violen las normas y los principios de general aceptación.
- Los directivos de las organizaciones deben crear un ambiente de control, un conjunto de procedimientos de control directo y las limitaciones del control interno.

Los controles pueden implantarse a varios niveles diferentes. La evaluación de los controles de la Tecnología de la Información exige analizar diversos elementos interdependientes.

Por ello es importante llegar a conocer bien la configuración del sistema, con el objeto de identificar los elementos, productos y herramientas que existen para saber dónde pueden implantarse los controles. así como para identificar posibles riesgos.

***Auditor
interno/externo
informático:***

- Ha de revisar los diferentes controles internos definidos en cada una de las funciones informáticas y el cumplimiento de normativa interna y externa, de acuerdo al nivel de riesgo, conforme a los objetivos definidos por la Dirección de Negocio y la Dirección de Informática. Informará a la Alta Dirección de los hechos observados y al detectarse deficiencias o ausencias de controles recomendarán acciones que minimicen los riesgos que pueden originarse.

Bibliografía:

- Piattinni, G. M & Peso del E. *Auditoría Informática. Un enfoque práctico.* Alfaomega
- Echenique G. J.A. (2001). *Auditoría en Informática.* 2da. Ed. Mc Graw- Hill