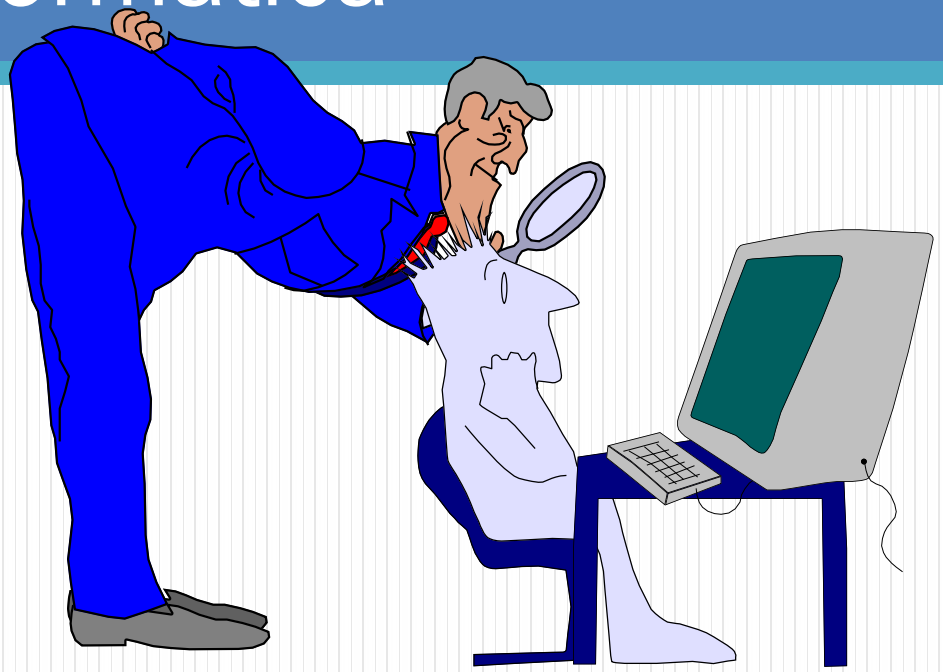
UNIVERSIDAD NACIONAL DE INGENIERÍA

Conceptos Básicos de Auditoría Informática



MSc. Julio Rito Vargas Avilés

Sábado 21 marzo de 2009

AUDITORÍA INFORMÁTICA	
Tema	**Objetivos**
1. Conceptos básicos	❑Conocer qué es la Auditoría
	❑Conocer la evolución de la Auditoría y su situación en Nicaragua
	❑Comprender las diferencias entre la auditoría externa e interna
	❑Comprender qué son los controles internos y la necesidad de los mismos en una organización.
2. Necesidad de la Auditoría Informática	❑Conocer la importancia que tiene la información para las organizaciones y las dificultades que presenta la gestión y el control de los SI/TI en las organizaciones
	❑Explicar los principios que rigen el establecimiento de un marco de gobierno en una organización y como implantarlo para los SI/TI
	❑Conocer las formas de actuación del auditor informático, ya sea auditando la función informática, los sistemas de información o como apoyo a la auditoría general en el uso de la informática
	❑Comprender cuáles son las diferencias esenciales entre información, sistemas de información y tecnología de información, tanto en sus aspectos cuantitativos como cualitativos, así como la necesidad de medir la gestión que se realiza en cada uno de ellos
	❑Comprender la necesidad de la existencia de la Auditoría de Sistemas de Información en las organizaciones y los distintos roles que la Auditoría de Sistemas de Información juega en las mismas
	❑Aprender a redactar los instrumentos más importantes de comunicación del gobierno de la información, especialmente procedimientos

AUDITORÍA INFORMÁTICA	
Temas	**Objetivos**
3. Controles internos	❑Explicar los fundamentos de un sistema de control interno en una organización así como los conceptos y técnicas de análisis y control de riesgos relacionados con los SI/TI.
	❑Explicar COBIT como marco de referencia para la implantación de dichos controles.
	❑Comprender la necesidad de implantar controles en los procesos TI en una organización
	❑Ser capaz de identificar qué objetivos de control son aplicables en casos simples
	❑Ser capaz de redactar una aplicación de objetivos de control en casos simples
	❑Evaluar la factibilidad y el riesgo

La tecnología de información (IT), según lo definido por la asociación de la tecnología de información de América (ITAA) **es "el estudio, diseño, desarrollo, implementación, soporte o dirección de los sistemas de información computarizados, en particular de software de aplicación y hardware de computadoras." Se ocupa del uso de las computadoras y su software para convertir, almacenar, proteger, procesar, transmitir y recuperar la información.** Hoy en día, el término "tecnología de información" se suele mezclar con muchos aspectos de la computación y la tecnología y el término es más reconocible que antes. La tecnología de la información puede ser bastante amplio, cubriendo muchos campos. Los profesionales TI realizan una variedad de tareas que van desde instalar aplicaciones a diseñar complejas redes de computación y bases de datos. Algunas de las tareas de los profesionales TI incluyen, administración de datos, redes, ingeniería de hardware, diseño de programas y bases de datos, así como la administración y dirección de los sistemas completos. Cuando las tecnologías de computación y comunicación se combinan, el resultado es la tecnología de la información o "infotech". La Tecnología de la Información (IT) es un término general que describe cualquier tecnología que ayuda a producir, manipular, almacenar, comunicar, y/o esparcir información.

Las *tecnologías de la información y la comunicación* (TIC**)** son un conjunto de servicios, redes, software y dispositivos que tienen como fin la mejora de la calidad de vida de las organizaciones y personas dentro de un entorno, y que se integran a un sistema de información interconectado y complementario.

Las Tecnologías de la información y la comunicación, son un solo concepto en dos vertientes diferentes como principal premisa de estudio en la ciencias sociales donde tales tecnologías afectan la forma de vivir de las sociedades.

¿Qué es la información?

- **la información puede ser definida como los datos que han sido recogidos, procesados, almacenados y recuperados con el propósito de tomar decisiones financieras y económicas o para el soporte de una producción y distribución eficientes de bienes y servicios.**
- La información tiene que ser considerada como **un recurso básico en una organización, junto a los talentos humanos, el capital, las materias primas y demás equipos.**
- Es **clave para la organización tanto para su supervivencia como para mejorar su posicionamiento en los negocios.**

¿Qué es la información?

- La información puede ser clasificada en cuatro clases: Información estratégica, Información para el control de gestión, Información financiera o contable e Información operativa o técnica.
  - **Información estratégica** permite a la alta gerencia **definir los objetivos de la organización, la cantidad y clase de recursos necesarias para alcanzar los objetivos y las políticas que gobiernan su uso.** La alta gerencia tiene que tomar decisiones económicas importantes basadas en las condiciones de los cambiantes mercados e innovación tecnológica. Parte de esta información es externa.

¿Qué es la información?

- **Información para el control de gestión** ayuda a los mandos medios especialmente para tomar decisiones en el período actual, **normalmente un año, para que sean consistentes con los objetivos estratégicos organizativos. Incluye comparaciones entre los resultados actuales y objetivos, presupuestos y medidas de rendimiento.**

- **Información técnica u operacional se produce por rutina, día a día e incluye datos de contabilidad, control de inventario, programación de la producción, planificación de necesidades de materiales, normas y gestión del personal, control del flujo de caja, logística, ingeniería, fabricación, recepción, distribución, ventas y todo el conjunto de operaciones que son necesarias para mantener la empresa en funcionamiento.**

¿Qué es la información?

- **Información contable y financiera** es **la información que se genera con el propósito de control e información financieros. Este tipo de información se recoge de acuerdo con Principios Contables Generalmente Aceptados y son aplicados por los profesionales contables.**

¿Por qué es valiosa la información para la toma de decisiones?

- La calidad de las decisiones tomadas depende directamente de la calidad de la información que las soporta.

La toma de decisiones requiere:

- Un profundo conocimiento de las circunstancias que rodean un problema.
- Conocimiento de las alternativas disponibles y
- Estrategias competitivas.

Atributos de la información que la hacen valiosa para la toma de decisiones

Completa: Si la información se pierde u oculta al que toma la decisión, el resultado de la decisión será pobre.

Exacta: Errores en la entrada, conversión o procesos puede dar como resultado conclusiones invalidas que darán lugar a decisiones erróneas.

Autorizada: La información puede ser semánticamente correcta, pero representar transacciones invalidas o no autorizadas.

Auditable: La información debe ser seguible a través de los documentos fuente o su ejecución seguida mediante sistemas de control monitorizados y preverificados.

Económica: El coste de producir la información debería no exceder su valor cuando se utiliza

Atributos de la información que la hacen valiosa para la toma de decisiones

Adecuada: Información específica debe estar disponible solamente para aquellos que la necesitan para asegurar una gestión eficiente. Demasiada información irrelevante a disposición de quién debe tomar la decisión puede ocultar el proceso.

Oportuna o Puntual: La información pierde su valor cuando a quién tiene que tomar la decisión, se le entrega después de que la necesita.

Segura: La información debe ser protegida de su difusión a personas no autorizadas, sin ello puede dar lugar a pérdidas económicas en la organización. Debe estar protegida contra destrucciones accidentales o voluntarias

¿Qué hace que la información sea un recurso crítico para la organización?

- Los estudios realizados en diversas organizaciones y universidades revelan que en **los sectores financieros, productivos y de servicios, una caída total de las redes y equipos informáticos de tres o cuatro días puede dar lugar a la pérdida del negocio.**

- **la pérdida de confidencialidad en las bases de datos puede proporcionar a los competidores una ventaja definitiva**

¿ Se reconoce a la información como un recurso crítico?

- **Con relación a la protección de las instalaciones físicas y el control de acceso a los sistemas de información**, hay pocas estadísticas disponibles sobre el **uso del software de control de acceso en cuanto a sus políticas de utilización y calidad de su administración.**

  Una vez que se es consciente de que tal software puede ser instalado y utilizado de distintas maneras, es más evidente que **poseer este software, por si mismo, no garantiza la seguridad sino que la administración es la clave del éxito.**

- **Aun cuando el software de control de acceso esté instalado y bien administrado, hay numerosas vías por las cuales, los programadores de sistemas desde dentro y los "hackers" desde fuera de la organización pueden burlar los mecanismos de seguridad**.

¿Cómo mejorar la gestión y el control de las T.I.?

- Para ello es necesario que las organizaciones puedan disponer de:
- **Una función de auditoría informática independiente** .
- **Una utilización correcta de la informática en la práctica de los distintos tipos de auditoría**,
- **La definición de unos objetivos de control de T.I.**

Necesidad de la Auditoría Informática

Por tanto la auditoría informática debe analizar:

- **La función informática, que engloba el análisis de la organización, seguridad, segregación de funciones y gestión de las actividades de proceso de datos.**

  Los sistemas informáticos, buscando asegurar la adecuación de los mismos a los fines para los que fueron diseñados.

Objetivos de la Auditoría Informática

Los objetivos de la auditoría informática son:

- **Verificar el control interno de la función informática.**
- **Asegurar a la alta dirección y al resto de las áreas de la empresa que la información que les llega es la necesaria en el momento oportuno, y es fiable, ya que les sirve de base para tomar decisiones importantes.**
- **Eliminar o reducir al máximo la posibilidad de pérdida de la información por fallos en los equipos, en los procesos o por una gestión inadecuada de los archivos de datos.**
- **Detectar y prevenir fraudes por manipulación de la información o por acceso de personas no autorizadas a transacciones que exigen trasvases de fondos.**

Tipos de Auditoría informática

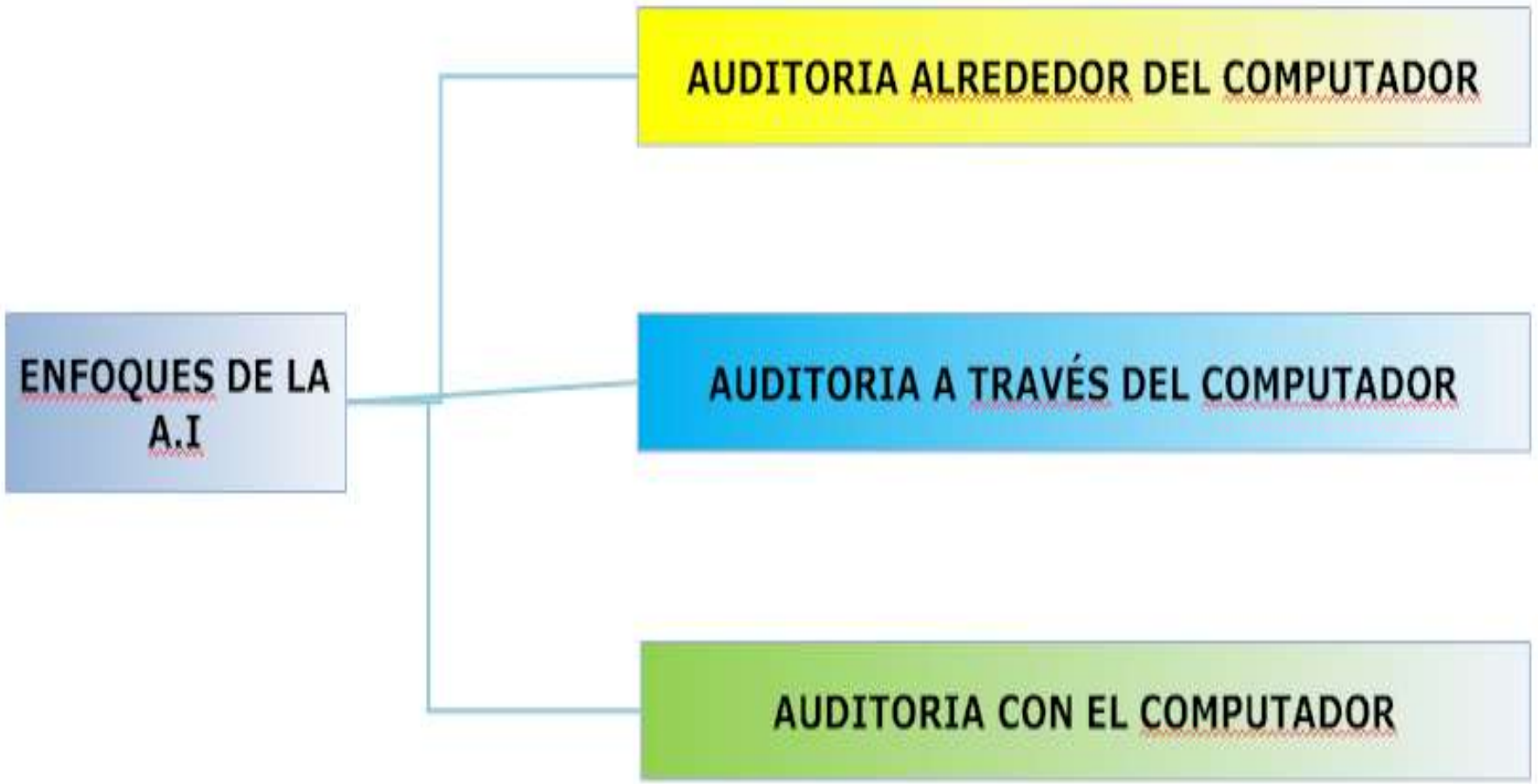
- Dentro de la auditoría informática destacan los siguientes tipos (entre otros):
- **Auditoría de la gestión:** Referido a la contratación de bienes y servicios, documentación de los programas, etc.
- **Auditoría legal del Reglamento de Protección de Datos**: Cumplimiento legal de las medidas de seguridad exigidas por el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos.
- **Auditoría de los datos**: Clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas.
- **Auditoría de las bases de datos**: Controles de acceso, de actualización, de integridad y calidad de los datos.
- **Auditoría de la seguridad**: Referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.
- **Auditoría de la seguridad física**: Referido a la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de esta. También está referida a las protecciones externas (arcos de seguridad, CCTV, vigilantes, etc.) y protecciones del entorno.
- **Auditoría de la seguridad lógica**: Comprende los métodos de autenticación de los sistemas de información.
- **Auditoría de las comunicaciones**. Se refiere a la auditoria de los procesos de autenticación en los sistemas de comunicación.
- **Auditoría de la seguridad en producción**: Frente a errores, accidentes y fraudes.

¿Qué hace la Auditoría Informática?

- Detectar evidencias de riesgos y/o problemas en el apoyo informático a los procesos de negocios originados por un mal uso informático y/o del control.

- Sugerir mejoras

ENFOQUES DE LA AUDITORIA INFORMATICA



Auditoría alrededor del computador

- **En este enfoque de auditoría, los programas y los archivos de datos no se auditan.**

  La auditoría alrededor del computador concentra sus esfuerzos en la entrada de datos y en la salida de información. Es el más cómodo para los auditores de sistemas, por cuanto únicamente se verifica la efectividad del sistema de control interno en el ambiente externo de la máquina. Naturalmente que se examinan los controles desde el origen de los datos para protegerlos de cualquier tipo de riesgo que atente contra la integridad, completitud, exactitud y legalidad.

  La auditoría alrededor del computador no es tan simple como aparentemente puede presentarse, pues tiene objetivos muy importantes como:

  1. Verificar la existencia de una adecuada segregación funcional.
  2. Comprobar la eficiencia de los controles sobre seguridades físicas y lógicas de los datos.
  3. Asegurarse de la existencia de controles dirigidos a que todos los datos enviados a proceso estén autorizados.
  4. Comprobar la existencia de controles para asegurar que todos los datos enviados sean procesados.
  5. Cerciorarse que los procesos se hacen con exactitud.
  6. Comprobar que los datos sean sometidos a validación antes de ordenar su proceso.
  7. Verificar la validez del procedimiento utilizado para corregir inconsistencias y la posterior realimentación de los datos corregidos al proceso.
  8. Examinar los controles de salida de la información para asegurar que se eviten los riesgos entre sistemas y el usuario.
  9. Verificar la satisfacción del usuario. En materia de los informes recibidos.
  10. Comprobar la existencia y efectividad de un plan de contingencias, para asegurar la continuidad de los procesos y la recuperación de los datos en caso de desastres.

Auditoría a través del computador

- Este enfoque está orientado a examinar y evaluar los recursos del software, y surge como complemento del enfoque de auditoría alrededor del computador, en el sentido de que su acción va dirigida a evaluar el sistema de controles diseñados para minimizar los fraudes y los errores que normalmente tienen origen en los programas.

  Este enfoque es más exigente que el anterior, por cuanto es necesario saber con cierto rigor, lenguajes de programación o desarrollo de sistemas en general, con el objeto de facilitar el proceso de auditaje.

  Objetivos de esta auditoría
  1. Asegurar que los programas procesan los datos, de acuerdo con las necesidades del usuario o dentro de los parámetros de precisión previstos.
  2. Cerciorarse de la no-existencia de rutinas fraudulentas al interior de los programas.
  3. Verificar que los programadores modifiquen los programas solamente en los aspectos autorizados.
  4. Comprobar que los programas utilizados en producción son los debidamente autorizados por el administrador.
  5. Verificar la existencia de controles eficientes para evitar que los programas sean modificados con fines ilícitos o que se utilicen programas no autorizados para los procesos corrientes.
  6. Cerciorarse que todos los datos son sometidos a validación antes de ordenar su proceso correspondiente.

  Informe de Auditoría: deberá orientarse a opinar sobre la validez de los controles, en este caso de software, para proteger los datos en su proceso de conversión en información.

Auditoría con el computador

- Este enfoque va dirigido especialmente, al examen y evaluación de los archivos de datos en medios magnéticos, con el auxilio del computador y de software de auditoría generalizado y /o a la medida. Este enfoque es relativamente completo para verificar la existencia, la integridad y la exactitud de los datos, en grandes volúmenes de transacciones.

  La auditoría con el computador es relativamente fácil de desarrollar porque los programas de auditoría vienen documentados de tal manera que se convierten en instrumentos de sencilla aplicación. Normalmente son paquetes que se aprenden a manejar en cursos cortos y sin avanzados conocimientos de informática. Los paquetes de auditoría permiten desarrollar operaciones y prueba, tales como:
  1- recálculos y verificación de información, como por ejemplo, relaciones sobre nómina, montos de depreciación y acumulación de intereses, entre otros.
  2- Demostración gráfica de datos seleccionados.
  3- Selección de muestras estadísticas.
  4- Preparación de análisis de cartera por antigüedad.

  Informe de Auditoría: Este informe deberá versar sobre la confiabilidad del sistema de control interno para proteger los datos sometidos a proceso y la información contenida en los archivos maestros.

  Los tres (3) enfoque de auditoría vistos, son complementarios, pues ninguno de los tres, es suficiente para auditar aplicaciones en funcionamiento.

Auditoría Interna informática

Hoy la auditoría interna es:

- Una unidad con atribuciones y facultades para auditar todas las operaciones TIC de las organizaciones.
- **Se define como una función de valoración independiente establecida dentro de una organización para examinar y evaluar sus actividades como un servicio a la organización.**

- **Su objetivo es asistir a los miembros de la organización en el cumplimiento efectivo de sus responsabilidades**

Auditoría Interna informática

- proporciona análisis, valoraciones, recomendaciones, consejo e información sobre las actividades revisadas.

- El alcance de la auditoría interna debe abarcar el examen y evaluación de la adecuación y efectividad del sistema de control interno y la calidad de la de ejecución en la realización de las responsabilidades asignadas.

Auditoría Externa

- **La auditoría externa se puede definir como un servicio público o privado prestado por profesionales calificados en Auditoría Informática, que consiste en la realización, según normas y técnicas específicas, de una revisión de las TIC, a fin de expresar su opinión independiente sobre si lo auditado presentan violaciones, irregularidades, fraudes u errores en un momento dado, sus resultados y hallazgos durante un periodo determinado, de acuerdo con las normas de control interno, normas ISO, de la Contraloría General de la República y otras que sea de competencias.**

TAREA

- Principios éticos y funciones de un auditor informático (exposición 20 minutos)
- Normas de control interno Informático (exposición 20 min.)
- Caso de estudio 2(para el grupo)
- Caso de estudio 3(para el grupo)
- Resumen de la conferencia anterior (5 min)