

**UNIVERSIDAD DE COSTA RICA**  
**ESCUELA DE ADMINISTRACIÓN DE NEGOCIOS**

**PROGRAMA DEL CURSO**

**Laboratorio Auditoría Informática I**  
**PC-0424**

**Prof.: Gino Ramírez**

**II SEMESTRE 2007**

## INTRODUCCIÓN

Debido al incremento en la aplicación de la tecnología en los quehaceres de todas las organizaciones, principalmente en la preparación de datos tanto para la toma de decisiones como para la rendición de informes a terceros interesados en relación con la gestión empresarial; la actividad de auditoría, en general, ha dado un giro tendente a examinar los controles de los ambientes de tecnologías de información para determinar el grado de confianza que puede depositar en la información en la que basa su examen.

Tanto es así que diferentes marcos normativos de aceptación general (véanse normas como las NIA's, COBIT y COSO), tienen implícito que tanto la administración como la auditoría se aboquen a la implementación y examen de controles relacionados con la gestión de las tecnologías de Información (TI).

En razón de lo anterior, dentro del currículo de la carrera de Administración de Negocios con énfasis en contaduría pública se consideran distintos cursos relacionados tanto con la gestión como con la auditoría de TI, los cuales se complementan con cursos paralelos de laboratorio en los que se adquieren conocimientos y se desarrollan algunas destrezas sobre la aplicación de procedimientos de auditoría con y sobre el computador.

En este caso particular se presentan los contenidos del programa correspondientes al curso de Laboratorio de Auditoría Informática I.

Dicho programa incluye los aspectos relativos al contenido, estructura y evaluación del curso. De ahí la importancia de que los estudiantes lo conozcan con detalle y cuenten con él durante todo el curso pues es la guía para conocer sobre las actividades que serán desarrolladas.

## OBJETIVO GENERAL

De conformidad con lo anterior se establece como **objetivo del curso**: lograr que el estudiante obtenga un conocimiento razonable sobre la aplicación de procedimientos de auditoría con y sobre el computador durante un proceso de evaluación de controles relacionados con la gestión de tecnologías de información.

Cabe aclarar que existen distintas técnicas de auditoría asistidas por el computador (CAAT's) que pueden ser aplicadas en las diferentes etapas de los distintos tipos de auditoría; sin embargo, por el alcance que compete a este curso, su alcance se enfoca al examen de los controles relacionados con la "administración de datos" – entrada, proceso, salida e integridad de datos.

## OBJETIVOS ESPECÍFICOS

Que al finalizar el curso el estudiante esté en capacidad de:

1. Conocer o identificar las actividades del proceso de auditoría de TI que pueden ser apoyadas con el uso del computador
2. Identificar, planificar, desarrollar y documentar pruebas de auditoría apoyadas con el computador.
3. Utilizar de manera razonable aplicaciones, paquetes o programas que apoyan la ejecución de pruebas de auditoría con ayuda del computador.
4. Procurar un conocimiento crítico por parte de los estudiantes sobre diferentes proveedores de herramientas informáticas que contribuyen con la función de auditoría de sistemas.
5. Considerando el nivel académico de los estudiantes y que la **redacción y ortografía** son requisitos indispensables en su desempeño profesional, dichos aspectos serán considerados y reforzados durante todo el curso y formarán parte de los aspectos a evaluar.

## METODOLOGÍA

Se impartirán clases magistrales de la materia principal por parte del profesor, apoyadas con prácticas intensivas que se deberán efectuar tanto en los microcomputadores del laboratorio como en forma extraclase.

## EVALUACIÓN

Para evaluar la comprensión de la materia se realizarán pruebas principalmente prácticas. La estructura de calificación es como sigue:

I Parcial	25%
II Parcial	25%
Exámenes cortos	30%
Laboratorios	20%
	-----
	<b>100%</b>

### De los exámenes parciales

Estas pruebas pueden incluir tanto aspectos prácticos sobre la teoría estudiada en clase como ejercicios prácticos. Se realizan de manera individual en el laboratorio correspondiente. Para la resolución de los ejercicios prácticos, al estudiante le son suministrados los archivos de datos y programas necesarios.

**En caso de ausencia a un examen parcial, el estudiante deberá prepararse para aplicarlo en la clase inmediata siguiente.**

### De los exámenes cortos

Durante el curso se efectuarán 4 exámenes cortos con un valor de 7.5% cada uno. Serán efectuados de conformidad con el calendario establecido. Se establecen de previo sus fechas de realización para que el estudiante tome las provisiones del caso ya que estas pruebas no se reponen. MUCHA ATENCIÓN: LOS EXÁMENES CORTOS NO SE REPONEN; SIN EXCEPCIÓN.

### De los Laboratorios

Con el fin de beneficiar a aquellos estudiantes que se ausentan de un examen corto, se considerará la participación en las prácticas de laboratorio para lo cual se utilizará una hoja de calificación incluida en el anexo. El profesor hará consultas sobre cualquier tema que haya sido cubierto y se realizarán en cualquier momento de cualquier clase. Se podrán realizar una o más consultas durante una misma clase. A cada estudiante se le deberá aplicar 4 consultas durante el curso y podrán ser orales, escritas, constituidas en tareas extractase o bien en la resolución de un ejercicio durante la clase.

**MUY IMPORTANTE:** Como parte de cualquier proceso de evaluación será calificado con toda rigurosidad la **redacción y la ortografía**.

En virtud de que se realizarán únicamente 2 parciales NO EXISTE POSIBILIDAD DE OPTAR POR EXIMIRSE.

## OTROS

- El curso tiene como política minimizar el uso de papel por esa razón, en la medida de las posibilidades, todo el material relativo al curso será tramitado vía correo electrónico y si eso no es posible será entregado en algún medio de almacenamiento alterno. (Dirección: [ginor@ucr.ac.cr](mailto:ginor@ucr.ac.cr)). En virtud de lo anterior, cada estudiante deberá suministrar al profesor su dirección electrónica a más tardar en la segunda clase del curso.
- Se debe tener presente que el programa está ajustado a un laboratorio de dos horas únicamente, por lo que se deberá aprovechar al máximo ese tiempo disponible, POR ELLO ES REQUERIDO PUNTUALIDAD.

**BIBLIOGRAFÍA Y OTROS**

- Lecturas varias suministradas por el profesor
- Copia de software freeware o shareware suministrado por el profesor

CLASE	FECHA	TEMAS	MATERIALES	COMENTARIOS
1	15/08/05	<b>Conceptos Generales</b> sobre: <ul style="list-style-type: none"> <li>- Funciones y organización de las unidades de TI.</li> <li>- Estructuras de control de TI</li> <li>- Estándares internacionales sobre TI.</li> <li>- Metodología de la Auditoría de TI.</li> <li>- Aspectos básicos de auditoría: programa, evidencia, pruebas, papeles de trabajo y comunicación de resultados.</li> </ul>	<ul style="list-style-type: none"> <li>- <b>00_Resumen</b> sobre la gestión de las TI.</li> <li>- <b>01_Resumen</b> ejecutivo COBIT 4</li> <li>- <b>02_Resumen</b> Metodología Aud. TI.</li> <li>- <b>03_Referencias</b> sobre Documentos Electrónicos</li> <li>- <b>04_Resumen</b> BS17799</li> <li>- <b>05_Resumen</b> Modelo CMMI</li> <li>- <b>06_Resumen</b> 5080 y NIAS relacionadas.</li> <li>- <b>08_Técnicas y prácticas</b> de auditoría.</li> <li>- <b>09_Temario clase 1</b></li> <li>- <b>07_Diagrama conceptos</b> básicos.</li> </ul>	<p>Es importante que los estudiantes tengan completa claridad del contexto dentro del cual se desarrolla la materia que se imparte en este curso. En ese sentido es necesario que se conozca que el curso constituye, principalmente un complemento del curso Auditoría Informática I; y que la materia está relacionada con la gestión de las tecnologías de información.</p> <p>Por lo anterior, esta primera clase es teórica y tiene como propósito ubicar al estudiante dentro de ese contexto y de cómo se relacionan las distintas pruebas con él.</p> <p>Indirectamente se analizarían otras metodologías o procedimientos de auditoría relacionados con tecnologías de información que podrían estar vinculados a otros contextos, como el de toma de decisiones y análisis financiero.</p>
2	22/08/05	<b>Metodología de Auditoría</b> <ul style="list-style-type: none"> <li>- <b>Desarrollo del caso “Préstamos Seguros”.</b></li> <li>- <b>Revisión práctica de las etapas de PP y PD y elaboración de Pgrs de Auditoría.</b></li> <li>- <b>Estudio de una aplicación informática en un entorno empresarial.</b></li> <li>- <b>Práctica de selección y priorización utilizando el modelo DELPHY</b></li> </ul>	<ul style="list-style-type: none"> <li>- 00_Temario_clase2</li> <li>- Caso0_PrestamosSeguros.doc</li> <li>- Carpeta MAIN</li> <li>- Ejercicio_Calidad DELPHY.xls</li> </ul>	<p>Una vez estudiado el contexto en el que se desarrolla la auditoría de TI, se estudia lo siguiente:</p> <ol style="list-style-type: none"> <li>1. Conociendo que un paso inicial es determinar cuáles son los controles o aspectos relacionados con la gestión de las TI qué serán sujetos de evaluación y que para ello es necesario ejecutar una adecuada Planificación, se estudia lo relativo a esta etapa de la auditoría utilizando como base el documento de práctica denominado “Caso0_Préstamos Seguros” y se práctica, de manera preliminar la elaboración de programas de auditoría en el cual se detallen los procedimientos a aplicar en el entorno de “Préstamos Seguros”.</li> <li>2. Como complemento se estudia el proceso de selección y priorización mediante modelo DELPHY.</li> </ol>
3	29/08/05	<b>Solicitud de acceso a recursos tecnológicos.</b> <ul style="list-style-type: none"> <li>- <b>Solicitud de copia de archivos de datos y aplicaciones.</b></li> <li>- <b>Solicitud de acceso a archivos de datos o aplicaciones.</b></li> <li>- <b>Conexión ODBC</b></li> <li>- <b>Totales Hash</b></li> <li>- <b>Proceso importación de</b></li> </ul>	<ul style="list-style-type: none"> <li>- 00_Temario_clase3_Solicitud</li> <li>- Caso1_Solicitud</li> <li>- Caso1_Solicitud Resolución</li> </ul>	<p>Para la realización de pruebas relacionadas con TI generalmente es requerido obtener acceso e incluso copia de algunos recursos tecnológicos (archivos de datos o aplicaciones).</p> <p>Dicha solicitud merece un tratamiento serio y riguroso a fin de minimizar eventuales riesgos asociados. De ahí que es necesario repasar los requisitos necesarios para elaborar este tipo de solicitudes así como los procedimientos a seguir en la recepción de lo solicitado.</p>

		<b>datos</b>		Para ello se estudia la “solicitud de información”, siguiendo como guía el “Caso1_SolicitudInformación”.
4	05/09/05	<b>EXAMEN CORTO 1</b> Evaluación de seguridad: - Claves de acceso: tipo de claves, claves encriptadas, claves de SO, claves en aplicaciones, número de intentos de acceso, control de acceso por horas o días, suspensión de sesión por no uso. - Bitácoras: verificación empleados en vacaciones, incapacitados, suspendidos, cambios de puestos, separados de la organización, Perfiles de acceso.	- 00_temario_clase4y5_Seguridad - 01_Resumen ISO 17799 - Caso2_ControlAcceso - Caso2_1_Encripción	Ya para esta clase el estudiante está familiarizado con el contexto de la Auditoría de TI y su metodología y puede realizar un programa para examinar un aspecto específico. Considerando la estructura establecida para el curso se inicia con el examen del componente de “SEGURIDAD”.  Utilizando el contexto de “Préstamos Seguros”, se diseña un programa de auditoría para revisar los controles de acceso del sistema operativo y de las aplicaciones, distintos formatos de palabras clave, proceso de encriptación de PW, y uso de bitácoras a nivel de sistema operativo y de aplicación; practicando con ello el diseño de pruebas de auditoría y la elaboración de programas de trabajo. Para ello se utiliza como referencia el resumen sobre técnicas y prácticas de auditoría.  Como parte de este punto se practica lo siguiente:  - Tipo de claves utilizadas (cantidad de caracteres, de SO y de aplicación, encriptadas o expuestas) - Cantidad de intentos permitidos - Suspensión de sesión en tiempo definido - Restricción de acceso por horas o días. - Registro de acceso en bitácoras: cantidad de información - Prueba de empleados en vacaciones, suspendidos, separados del cargo, incapacitados, trasladados a otro puesto  Se diseñarán programas de auditoría y se ejecutarán pruebas con la debida documentación, observando el debido cuidado en la recopilación de evidencia, el archivo de los papeles de trabajo, su referenciación y custodia, incluyendo los datos de información recopilados.
5	12/09/05	<b>IDEM</b>	<b>IDEM</b>	<b>IDEM</b>
6	19/09/05	<b>Controles de aplicación</b> <b>Pruebas a los controles de entrada</b> (Lote Datos) <b>EXAMEN CORTO 2</b>	- 00_Temario_Clase6_Controles-Entrada - 01_Resumen Admón. de Datos. - 01_1 Presenta Admón. Datos. - 02_Resumen de TAAC-s - 02_1 Tipos TAAC's - Caso No. 3 Lote Datos	Una vez realizada la evaluación de la seguridad del entorno se inicia la evaluación de las aplicaciones.  Se estudia la teoría sobre los controles asociados con la “Administración de datos” o “Controles de Aplicación” y, utilizando el contexto del “Caso0 Préstamos Seguros” se realizan una serie de prácticas que abarcan desde la elaboración del programa de auditoría, en el cual se

				<p>plasman las pruebas diseñadas, hasta la ejecución y planteamiento de los resultados en forma de hallazgo para la comunicación de resultados.</p> <p>De los controles de aplicación se examina los controles de entrada y la integridad de datos. Para ello es necesario estudiar la teoría sobre TAAC's para conocer el procedimiento a seguir con respecto a la planificación, ejecución y documentación de resultados de este tipo de pruebas.</p> <p>Como práctica se resuelve el "Caso_3_LoteDatos".</p>
7	26/09/05	<p>Controles de aplicación</p> <p>Pruebas sobre Integridad de datos</p> <ul style="list-style-type: none"> <li>- Uso de ODBC</li> <li>- Uso de MS-SQL - Excel</li> </ul>	<ul style="list-style-type: none"> <li>- 00_Temario_Clase7_IntDatos-ODBC-MSQuery</li> <li>- ResumenBaseDatos</li> <li>- ResumenMSQuery</li> <li>- Caso4_InteDatos</li> </ul>	<p>Para introducir los conceptos de evaluación de integridad de datos se inicia con la ejecución de pruebas sobre archivos de una base de datos de una aplicación, en este caso de "Préstamos Seguros".</p> <p>Las pruebas sobre archivos pueden realizarse de múltiples formas y por múltiples canales.</p> <p>Por ejemplo: una opción es realizar las pruebas conectándose directamente a las bases de datos mediante ODBC o bien, obteniendo una copia de los archivos.</p> <p>En esta clase se inicia estudiando la conexión ODBC y realizando las pruebas directamente con Excel mediante la herramienta MSQuery.</p>
8	03/10/05	I Parcial		
9	10/10/05	<p>Controles de aplicación</p> <p>Pruebas sobre Integridad de datos - ACL</p> <ul style="list-style-type: none"> <li>- Componentes básicos <ul style="list-style-type: none"> <li>o Vista</li> <li>o Índice</li> <li>o Lotes</li> <li>o Espacios de Trabajo</li> <li>o Bitácora</li> </ul> </li> </ul>	<p>00_Temario Clase9a15_ACL</p> <p>Conceptos clave ACL</p> <p>Workbook</p> <p>CasoGeneralACL</p>	<p>La segunda etapa del curso abarca el estudio de una herramienta de auditoría, como una TAAC, en este caso para la "extracción y análisis de datos!". Por las condiciones académicas y la disponibilidad de SW se utilizará el SW ACL.</p> <p>Este instrumento permitirá practicar la aplicación de una herramienta automatizada en el examen de archivos de información de una organización. En el caso particular de la aplicación del caso en estudio "Préstamos Seguros".</p>
10	17/10/05	<p>Controles de aplicación</p> <p>Pruebas sobre Integridad de datos – ACL</p> <ul style="list-style-type: none"> <li>- Comandos básicos <ul style="list-style-type: none"> <li>o Estadística</li> </ul> </li> </ul>	<p>Una vez introducido el SW ACL se procede a explicar su conformación y sus comandos básicos. Para ello se utiliza los archivos que contiene la versión académica. Se incluye en esta explicación la aplicación de filtros y la</p>	

UNIVERSIDAD DE COSTA RICA – Escuela Administración de Negocios  
 Laboratorio Auditoría Informática I – 2º semestre 2005 – Prof. Gino Ramírez

		<ul style="list-style-type: none"> <li>○ Antigüedad</li> <li>○ Clasificación</li> <li>○ Conteo</li> <li>○ Extracción</li> <li>○ Histograma</li> <li>○ Ordenar</li> <li>○ Secuencia</li> <li>○ Estratificación</li> <li>○ Exportar</li> <li>○ Resumir</li> <li>○ Totalizar</li> <li>○ Verificar</li> </ul> <ul style="list-style-type: none"> <li>- Filtros</li> <li>- Importación de archivos</li> </ul>	<p>importación de archivos de datos.</p> <p>Este último tema de importación se explica utilizando dos herramientas: Excel y ACL. Se analiza además aspectos como:</p> <ul style="list-style-type: none"> <li>- La incidencia de los formatos de archivos en el proceso de importación</li> <li>- El uso de cifras de control.</li> <li>- El proceso de verificación en el proceso de importación.</li> </ul>	
11	24/10/05	<p>IDEM</p> <p><b>EXAMEN CORTO 1</b></p>	<p>IDEM</p> <p>Como complemento de la materia anterior se realizan algunos ejercicios similares con Excel para demostrar que algunas de las pruebas se pueden realizar con dicha herramienta haciendo la importante salvedad de la limitación que tiene Excel en cuanto al número de líneas (o registros) que puede manejar.</p>	IDEM
12	31/10/05	IDEM	IDEM	IDEM
13	07/11/05	<p>Controles de aplicación</p> <p>Pruebas sobre Integridad de datos – ACL</p> <ul style="list-style-type: none"> <li>- Relaciones</li> <li>- JOIN</li> <li>- Combinar</li> <li>- Muestreo</li> </ul>		
14	14/11/05	<p>IDEM</p> <p><b>EXAMEN CORTO 1</b></p>	IDEM	IDEM
15	21/11/05	IDEM	IDEM	IDEM
16	28/11/05	II Parcial		