UNIVERSIDAD DE COSTA RICA

ESCUELA DE ADMINISTRACIÓN DE NEGOCIOS

PROGRAMA DEL CURSO

Laboratorio Auditoría Informática I
PC-0424

Prof.: Gino Ramírez

II SEMESTRE 2005

INTRODUCCIÓN

Debido al desarrollo de la aplicación de la tecnología en los quehaceres de todas las organizaciones, principalmente en la preparación de datos para que la administración rinda informes a terceros interesados sobre la situación de las empresas; el papel del auditor ha tomado un giro importante tendente a examinar los controles de los ambientes de tecnologías de información. Tanto es así que ya diferentes marcos normativos de aceptación general (veánse normas como las NIA's, COBIT y COSO), consideran dentro de sus disposiciones la obligatoriedad de que el auditor se aboque al examen de los controles relacionados con la gestión de las tecnologías de Información.

En razón de lo anterior, dentro del curriculo de la carrera de Administración de Negocios con énfasis en contaduría pública se consideran dos cursos sobre Auditoría de Tecnologías de Información los cuales se complementan con cursos paralelos de laboratorio en los cuales se adquieren conocimientos sobre la aplicación de procedimientos de auditoría con y sobre el computador.

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

Este 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 tecnolgías 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, la materia estará relacionada con la gestión de las tecnologías de información..

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 compresión de la materia se realizarán exámenes basados totalmente prácticos con base en la materia brindada en clase.
La estructura de calificación es como sigue:

I Parcial	25%
II Parcial	25%
III Parcial	25%
Exámenes cortos	25%

	100%

De los exámenes parciales
Estos son exámenes totalmente prácticos, se realizan de manera individual en el laboratorio correspondiente. Dichas pruebas consisten en uno o varios ejercicios para lo cual, al estudiante le son suministrados los archivos de datos y programas necesarios para su ejecución.

De los exámenes cortos
Estos exámenes serán efetuados sobre cualquier tema que haya sido cubierto y se realizarán en cualquier momento de la clase. Se podrán realizar una o más pruebas durante una misma clase. El porcentaje final de la nota será distribuido, de manera uniforme, entre la cantidad de pruebas efectuadas.

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

OTROS

- En caso de ausencia a un exámen parcial, el estudiante deberá prepararse para aplicarlo en la clase inmediata siguiente.
- Los exámenes cortos no se reponen.
- 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)**. 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.

BIBLIOGRAFÍA Y OTROS

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

Cronograma del curso

CLASE	FECHA	TEMAS	OTROS
1	10/08/05	Conceptos Generales sobre: - Funciones y organización de las unidades de TI. - Estructuras de control de TI - Estándars internacionales sobre TI. - Metodología de la Auditoría de TI	- Resumen sobre la gestión de las TI. - Resumen ejecutivo COBIT - Resumen Metodología Aud. TI. - Referencias sobre Documentos Electrónicos - Resumen BS17799 - Resumen Modelo CMMI - Resumen NIAS relacionadas.
2	17/08/05	Repaso conceptos sobre: - Proceso de la auditoría. - Elaboración de programas de trabajo de auditoría. - Revisión caso práctico “Préstamos Seguros” y diseño preliminar de pruebas de auditoría.	- Resumen Admón. Datos - Presentación Admón. Datos - Caso “Prestamos Seguros” (texto y aplicaciones) - Ley de Derechos de autor y derechos conexos. - Directriz sobre pornografía. - Directriz sobre licenciamiento. - Criterios jurídicos sobre acceso a información en microcomputadores. - Criterios jurídicos sobre uso de recursos tecnológicos.
3	24/08/05	Aplicación de TAAC’s Controles de aplicación - Controles de entrada (Lote Datos) - Controles de proceso (ODBC – Excel)	- Resumen de TAAC’s - Técnicas y prácticas de auditoría - Resumen uso ACL - Resumen Base datos - Caso No1.
4	31/08/05	Controles de aplicación - Controles de salida - Integridad de datos (ODBC – Excel)	- Caso No. 2
5	07/09/05	Controles de aplicación - Integridad de datos (ODBC – Query)	- Caso No. 3
6	14/09/05	I Parcial	
7	21/09/05	Controles de aplicación - Integridad de datos ACL Introducción	- Caso No. 4
8	28/09/05	Controles de aplicación - Integridad de datos ACL Comandos básicos: Verificación, conteo, estadística, duplicados y saldos.	- Caso No. 5
9	05/10/05	Controles de aplicación - Integridad de datos ACL Comandos intermedios: Extracción, exportación, ordenamiento e indexación, estratificación,	- Caso No. 6

CLASE	FECHA	TEMAS	OTROS
		sumarización, clasificación.	
10	12/10/05	Controles de aplicación - Integridad de datos ACL Comandos avanzados: Unión y Merge	- Caso No. 7
11	19/10/05	Controles de aplicación Integridad de datos ACL Graficación, bitácoras y generación de informes en Word.	
12	26/10/05	II Parcial	
13	02/11/05	Muestreo	- Caso No. 8
14	09/11/05	Ejecución de pruebas relacionadas con inventario de recursos, licenciamiento y uso de recursos	- Caso No. 9 - SW. Sandra y Belarc
15	16/11/05	Controles de acceso y Seguridad (spyware, firewall, sniffer, keylogger)	- Caso No. 10
16	23/11/05	Cambio de nombre de archivos ejecutables Uso de direcciones WEB en archivos de Office para evadir inhabilitación de navegadores Encriptamiento, certificado electrónico y llaves públicas Alteración de correos electrónicos y suplantación de remitentes Seguridad Inalámbrica: infrarrojos, bluetooth	
17	30/11/05	III Parcial	

CLASE 1	**PREGUNTAS DE REPASO**
Funciones y organización de las unidades de tecnologías de información	Describa brevemente una estructura organizacional típica de una unidad de informática y las funciones propias de cada puesto.
- Jefatura	
- Asistente administrativo (inventarios, licenciamiento y contratos)	Cuáles son algunas de las funciones que se encuentran en una unidad de informática que se pueden calificar como incompatibles y por qué?
- Analistas y programadores	
- Soporte técnico (micros)	
- Administración del Centro Cómputo	Cuáles son algunos de los controles que típicamente deberían implementarse con respecto a las funciones o procesos que se desempeñan en una unidad de informática típica.
o Operadores	
o Medioteca	
- Redes y Telecomunicaciones	
- Bases de datos	
- Seguridad	
Estructura de control en la gestión de las TI	
- Estructura Objetivos de Control	Indique qué significa COBIT, quién lo emite, cómo está estructura y para qué sirve.
- Estructura COBIT	
- Estructura local	Describa la estructura de control sobre TI vista en clase.
Estándares internacionales	
- Boletín 5080	Describa en términos generales en qué consisten los estándares, normativa o modelos de control y gestión relacionados con TI vistos en clase.
- NIA's 400, 401, 1001, 1002, 1003, 1009	
- NIAS's actualizadas	
- ITIL	
- ASNZ-4360	
- NIST	
- ISO1799 y BS17799	
- PMI – PMBOK	
- CMMI	
Metodología de auditoría	
- Planificación (asignación de recursos, comunicación y definición del alcance)	Describa el proceso de auditoría de TI visto en clase; indique cuál es el objetivo de cada una de las etapas, y describa al menos tres procedimientos típicos relacionados con pruebas sobre las TI.
- Revisión Preliminar	
- Examen (evaluación de control interno y pruebas específicas)	
- Comunicación de resultados	
Elaboración de programas de auditoría	Describa cada una de las partes de un programa de auditoría. Pruebe confeccionar un programa de auditoría sobre un aspecto particular para cada una de las fases del proceso de auditoría.
- Objetivo	
- Alcance (asunto, periodo, normativa)	
- Procedimientos (qué y cómo)	
- Recursos	
Papeles de trabajo (papeles de trabajo electrónicos)	Cuáles son las características de los P/T?
Hallazgos de auditoría (condición, criterio, causa y efecto) y recomendaciones, advertencias y disposiciones.	Cuáles son los componentes de los hallazgos?
Redacción de informes	Cuáles son las condiciones a tener en cuenta para la redacción de informes.
Controles de Administración de Datos	Cuáles son los controles relacionados con admón.. de Datos, qués es CRM, ERP y Minería de Datos?
CRM, ERP, Minería de datos	

CLASE 2

Repaso CLASE 1

- Organización CC
- Estructuras de Control
- Proceso de Auditoría
    - Programa de Auditoría (Objetivo, alcance y procedimientos)
    - Elaboración de informes (Hallazgos: condición – causa – efecto – criterio) Conclusión y disposiciones (factibles).

2ª PARTE

Como parte de un proceso de auditoría de las tecnologías de información deben evaluarse distintos componentes o controles; entre ellos:

- Controles de carácter general
- La planeación y organización
- Lo relativo a la implementación y mantenimiento de aplicaciones
- La prestación y soporte de servicios
- El seguimiento

Distinto a la división antes detallada, existe otra menos evidente pero también muy clara que establece un grupo de controles generales y otro directamente relacionado con los programas o software de aplicación.

Normalmente un proceso de auditoría implica inicialmente una evaluación de los componentes generales que constituyen el entorno o lo que rodea a las aplicaciones. Dicha evaluación permite al auditor formase una opinión sobre la estructura del control interno general y con base en ello establecer un alcance y oportunidad de pruebas de auditoría determinado, para se aplicadas a los programas o software de aplicación.

Ahora, independientemente de la división de que se trate, o del proceso de auditoría que se siga, lo cierto es que uno de los controles que sin duda requerirán una razonable evaluación son los relacionados con las aplicaciones y que normalmente se conocen como "controles de aplicación" o, en un concepto ampliado, la "administración de datos".

TEMAS:

1. Conceptos básicos sobre administración de datos
   Para conocer un poco más sobre la "administración de datos" refiérase al **resumen** y a la presentación adjunta.

2. Para practicar lo relativo a la evaluación de estos controles resuelva el **caso** de la empresa "Préstamos Seguros". Se conoce el caso y se distribuye el software y se hace un recorrido por sus funcionalidades.

3. Se hacen ejercicios básicos e introductorios:
    a. Con base en la información del caso: identifique posibles pruebas de auditoría que podrían efectuarse sobre dicha situación
        i. Evaluación sobre los controles de acceso lógico
            1. claves en aplicación de intereses
            2. claves en sistema de seguridad central
            3. claves del sistema contable
            4. bitácoras del sistema central
            5. bitácoras de las aplicaciones
        ii. Evaluación sobre los controles de aplicación
            1. evaluación de controles de entrada en captura de información
            2. evaluación de controles de proceso utilizando Excel
            3. evaluación de integridad de datos utilizando Excel

CLASES 3, 4 Y 5

1. Repaso clase anterior

2. Como parte del caso visto en clase se deberá examinar los siguientes aspectos:

- Dado que la ejecución de pruebas de auditoría que se realizan sobre componentes de aplicaciones o bien utilizando la misma computadora, es necesario estudiar lo correspondiente a la aplicación de **TAAC's**. Para ello deberá estudiarse el **resumen** adjunto y la **normativa** respectiva.

- Controles de acceso (COMO UN ADICIONAL a los controles de aplicación ESTOS TEMAS NO SON CUBIERTOS EN ESTA CLASE)
    - Bitácoras - Prueba sobre información almacenada en bitácoras
        - Detalle de políticas de acceso de la empresa
        - Consideraciones de solicitud de información a la unidad de recursos humanos sobre contrataciones, despidos, renuncias, suspensiones, vacaciones y otros aspectos relativos al personal que puedan estar relacionados con el uso de las aplicaciones.
        - Personal con el perfil necesario para habilitar o deshabilitar las bitácoras.
        - Responsable del control o revisión de la información almacenada en las bitácoras.
        - Almacenamiento o respaldos de la información de las bitácoras.
    - Claves de acceso – Pruebas sobre la razonabilidad de las claves de acceso
        - Claves de acceso incrustadas en el "código del programa"
        - Claves de acceso encriptadas en archivos separados
        - Claves de acceso no encriptadas

- **Controles de aplicación**

Cuando se trata de controles de aplicación hay dos cosas claramente separadas que se deben examinar: la aplicación y la información que ésta maneja.

Así, inicialmente debe examinarse la aplicación en cuanto a sus tres grupos de control: entrada – proceso – salida. Posterior a esta etapa se procede con la evaluación de la integridad de la información que consta en las bases de datos de dicha aplicación. Sin embargo, algo que resulta fundamental para realizar estas pruebas es lograr el acceso adecuado tanto a la aplicación como a su información. Para ello es necesario estudiar inicialmente los siguientes conceptos:

a. Solicitud de información o de acceso a las aplicaciones (componentes, alcances y consecuencias de las notas de solicitud ya sea una conexión ODBC o de una copia de la información)
b. Proceso de importación de datos
c. Conexión ODBC
d. Repasar los conceptos de bases de datos relacionales

Una vez repasados esos conceptos se asume que se tiene copia de la aplicación y de sus bases de datos y se practica con la aplicación de las pruebas siguientes:

- Entrada de datos
    - Aplicación de lote de datos de prueba

Considerando la lectora del resumen de TAAC's los estudiantes estarían preparados para confeccionar o diseñar de manera formal y bien planificada la aplicación de una prueba de auditoría con ayuda del computador. El primer ejercicio sería preparar una prueba para la evaluación de los "controles de entrada de datos" En el resumen sobre "Administración de Datos" se detallan cuáles son esos controles: habría que seleccionar los que apliquen, aplicar la técnica de auditoría correcta, desarrollar el programa de auditoría junto con la prueba detallada y aplicarla, determinar los resultados y redactar los hallazgos. RESOLVER CASO NO.1_LOTEDATOS

- Proceso (la práctica de este punto está incluido en los casos 2 y 3)
- Salida (No se hará práctica sobre este punto)
- Integridad de Datos RESOLVER CASOS NO.2_IMPDATOS Y 3_RELACIONESYODBC

Posterior a los ejercicios anteriores deberá introducirse el uso de la herramienta o software de auditoría ACL o IDEA. Con ello se harán pruebas utilizando los siguientes componentes:

CLASE 7, 8, 9 , 10 Y 11

Estudio del software de auditoría ACL

CLASE 13 Y SIGUIENTES

Revisión de los componentes:

- **Inventario de recursos** (control de dispositivos, salida de dispositivos para mantenimiento, protección de la información en labores de mantenimiento)
- **Licenciamiento** (esquemas y costos de licenciamiento, Ley de Derechos de Autor, inventario y resguardo de licencias, jurisprudencia)
- **Uso de recursos tecnológicos** (Verificación existencia y debida comunicación de políticas institucionales, implementación de controles preventivos, medidas sancionatorias, criterios jurídicos sobre el acceso para revisar la información del computador, jurisprudencia sobre uso no autorizado de recursos tecnológicos)

Procedimientos

- Elaboración del programa de auditoría
- Ejecución de las pruebas
    - Verificación de inventario de recursos del computador Uso de software "**SANDRA" y "BELARC**" y opción "Información del sistema"
    - Revisión del uso del computador **Uso de explorador** para identificar archivos con información no autorizada
- Redacción de hallazgos y recomendaciones
- Comunicación de resultados (simulación de un caso)

Comprobación de trabajo y por valor de un quiz

- Remisión vía correo electrónico de los hallazgos redactados
- **CLASE 4**

Revisión de un sistema automatizado en sus componente de acceso y base de datos

Repaso conceptos clase anterior
Estructura del control en TI
Proceso de auditoría

Revisión de los componentes:
Controles de aplicación
Controles de **entrada**
Controles de **proceso**
Controles de **salida**

Procedimientos

- Elaboración del programa de auditoría
- Ejecución de las pruebas

- Redacción de hallazgos y recomendaciones
- Comunicación de resultados (simulación de un caso)

Comprobación de trabajo y por valor de un quiz

CLASE 5

Repaso conceptos clase anterior
Estructura del control en TI
Proceso de auditoría

Revisión de los componentes:
Controles de acceso lógico
Uso de información de **bitácoras**

Examen de uso de **palabras clave**

Procedimientos
Revisión y familiarización con sistema simulado de empresa "PRÉSTAMO SEGUROS"

- Elaboración del programa de auditoría
- Ejecución de las pruebas
    - Resolución caso Préstamos seguros
-
- Redacción de hallazgos y recomendaciones
- Comunicación de resultados (simulación de un caso)

Comprobación de trabajo y por valor de un quiz
- Remisión vía correo electrónico de los hallazgos redactados