SYLLABUS

Curso	:	**AUDITORÍA Y SEGURIDAD INFORMÁTICA**
Horas de Teoría	:	02
Horas de Laboratorio	:	03
Semestre	:	2003-II
Responsable	:	Silverio Bustos
Profesor Teoría	:	Fernando Gallarday
Profesores Laboratorio	:	Fernando Gallarday Oscar Cabanillas

I. OBJETIVO:

Capacitar al alumno en los conceptos, métodos, técnicas y herramientas utilizadas en la auditoría y seguridad informática, de modo que pueda comprender el rol y alcance de estas actividades, así como le permita perfilar el desarrollo de habilidades para la realización de auditorías de los sistemas informáticos, así como la administración de la seguridad informática en la empresa. Se hace énfasis en la discusión de casos con los que se puede encontrar el auditor o administrador de Seguridad y se complementa con una revisión de técnicas y herramientas de análisis como apoyo a la seguridad y auditoría de sistemas.

II. SUMILLA:

El curso consta de dos partes: teoría y práctica. En la parte teórica se presentan los conceptos, técnicas y métodos que permitan planificar y ejecutar evaluaciones de los sistemas informáticos y su gestión, así como la administración de la seguridad informática. Se complementa, en la parte práctica, con la discusión de casos que se presentan en la realidad empresarial, en donde también se presentarán o discutirán modelos de evaluación realizados con técnicas y herramientas de software para análisis de datos o el desarrollo de mecanismos / herramientas alternativas y/o complementarias de apoyo a las evaluaciones. Las herramientas presentadas o equivalentes serán usadas en el desarrollo del proyecto asignado.

III. CONTENIDO DE LA PARTE TEÓRICA:

3.1 Introducción: Conceptos (2 horas):

La Auditoría vs Seguridad Informática: Objetivos - ¿Qué es? ¿Qué hace y en qué se basa? ¿Es necesaria?. Tendencias organizativas. Implicancias del uso de las Tecnologías de Información. Ambientes Virtuales. Retos por el avance en TI. Riesgo de Negocio. Riesgo de Auditoría. Control Interno. Objetivos del Control Interno. Ejemplos de riesgos y controles. El proceso de la Auditoría de Sistemas. Control Self Assesment. Auditoría continua. El modelo COBIT: Misión y Visión, Alcance, Estándares y Normas. Definición de Control en COBIT. Objetivos de Control en TI.

Bibliografía:

"Information Systems Control & Audit", Weber, 1999, Capítulo 1 y 2
"Handbook of IT Auditing", Parker, 1995 /1998 Supplement Capítulo A2 y A
"CISA Technical Review Manual", ISACA, 1998 – 2003, Capítulo 1

3.2 El Modelo COBIT (2 horas):

COBIT: Audiencia? . Elementos. El marco de referencia: principios. Definiciones y relaciones. El cubo del COBIT. Requerimientos de negocio: Calidad, Financiero y Seguridad. Los recursos de TI para COBIT. Dominios y procesos de TI – Ejemplos. Los dominios de COBIT: Planeamiento y Organización, Adquisición e Implantación, Servicio y Soporte y Monitoreo. Los Objetivos de Control. Relación de los procesos a los objetivos de control. Ejemplo PO1. Guía de Auditoría: Objetivos, estructura general. Ejemplo PO1. PREGUNTAS Y RESPUESTAS.
TRABAJO PRACTICO 1.

Bibliografía:

"Control Objectives for Information and related Technologies - COBIT" (2da. Edición), ISACA.

3.3 Planeamiento y ejecución de la evaluación (2 horas):

Elaboración de un Plan: Por qué preparar un plan? Qué es lo que se debe planear? Cómo puedo elaborar el plan? Métodos de análisis e identificación de riesgos y controles. Selección y ponderación de factores. Planes generales y programas de auditoría: estructura y fases. Pruebas de cumplimiento vs. Pruebas sustantivas. Controles principales. Auditorías Financieras, Operativas e Integrales y su relación con la Auditoría de Sistemas. Valoración de la evidencia. . PREGUNTAS Y RESPUESTAS.

Bibliografía:

"Information Systems Control & Audit", Weber, 1999, Part IV
"Handbook of IT Auditing", Parker, 1995 /1998 Supplement, Capítulos A3, A5, D1
"Standard for Auditing Computer Applications", Martin A. Krist, 1999, Part II

3.4 Gerencia de Sistemas de Información (2 horas):

Estrategias. Políticas, procedimientos y prácticas. Capacitación. Organización. : estructura, y funciones típicas. La Segregación de funciones y las técnicas para facilitarlas. Controles compensatorios: Pistas de auditoría, Logs de transacciones, Totales de control de lotes. Métodos para evaluar la efectividad y eficiencia de las operaciones. Técnicas de auditoría. PREGUNTAS Y RESPUESTAS.
TRABAJO PRACTICO 2.

Bibliografía:

"Information Systems Control & Audit", Weber, 1999, Capítulo 3
COBIT – P01 Defining a Strategic IT Plan
"Handbook of IT Auditing", Parker, 1995 /1998 Supplement, Capítulos 3 y 6

3.5 Proceso de Sistemas (2 horas):

Plataforma de hardware: Arquitectura, planificación de capacidad, monitoreo, mantenimiento preventivo, adquisiciones. Plataforma de Software: arquitectura, adquisiciones, control de cambios, configuración. Redes y Telecomunicaciones. Monitoreo de performance. Control de redes de comunicación. Encripción. Prácticas operativas: Administración de operaciones. Sala de Cómputo. Programación de procesos. Administración de problemas. Control de cambios. Aseguramiento de calidad. Soporte Técnico. Seguridad física. Técnicas de auditoría. . PREGUNTAS Y RESPUESTAS.

Bibliografía:

"Handbook of IT Auditing", Parker, 1995 /1998 Supplement, Capítulos A1 y B1
COBIT – PO2 Defining the information Architecture
COBIT – DS3 Managing Performance and Capacity.

COBIT – DS9 Managing the configuration.
COBIT – M1 Monitoring the Process.

3.6 Integridad, Confidencialidad y Disponibilidad de los Sistemas (2 horas):

Control de acceso lógico: políticas, vías de acceso, exposiciones, técnicas de auditoría. Control de acceso físico: exposiciones y controles. Controles ambientales. La validación de datos, su procesamiento y totales de control. Controles de entrada. Controles de procesamiento. Control sobre archivos. Control de las salidas. Técnicas de Auditoría. Plan de contingencias: Evaluación de riesgos. Instalaciones externas. Infraestructura de cómputo alternativo. Prueba del plan de continuidad del negocio. Mantenimiento del plan. Técnicas de auditoría. PREGUNTAS Y RESPUESTAS.

Bibliografía:

"Information Systems Control & Audit", Weber, 1999, Capítulo 9
"Handbook of IT Auditing", Parker, 1995 /1998 Supplement, Capítulo B1, B6, D5 y E4.
COBIT – DS5 Ensuring System Security
"CISA Technical Review Manual", ISACA, 1998 – 2003, Capítulo 4

3.7 Desarrollo, Adquisición y Mantenimiento de Sistemas (2 horas):

Rol del auditor en la administración de proyectos. Ciclo de vida del desarrollo de sistemas (SDLC). Riesgos de un inadecuado SDLC. Controles: PERT/CPM, presupuestos. Definición de Requerimientos. Estudio de factibilidad. Adquisición de Software. Diseño. Programación. Pruebas. Implantación. Herramientas de desarrollo y ayudas de productividad. Documentación. Procedimientos de Prueba. Procedimientos de autorización y aprobación. Migración de programas. Cambios de emergencia. Integridad de fuentes y ejecutables. Técnicas de Auditoría. PREGUNTAS Y RESPUESTAS.

Bibliografía:

"Information Systems Control & Audit", Weber, 1999, Capítulo 4
COBIT – PO11 Managing Quality.
"Handbook of IT Auditing", Parker, 1995 /1998 Supplement, Capítulo A4, B3, B4.
"CISA Technical Review Manual", ISACA, 1998 – 2003, Capítulo 6

EXAMEN PARCIAL

3.8 Clasificación de los Datos, Funciones y Roles en la Seguridad (2 horas):

Clasificación de la Información. Políticas, roles y actores. Estructura organizativa de Seguridad informática. Categorización de activos. Funciones de Seguridad vs Funciones de Auditoria. PREGUNTAS Y RESPUESTAS.

Bibliografía:

"Handbook of Information Security Management",Harold Tipton & Micki Krause. 1999
"CISSP Prep Guide: Mastering the Ten Domains of Computer Security", Ronald L. Krutz, Russell Dean Vines, 2001, Cap. 1

3.9 Métodologia de análisis de riesgos – Método de escenarios (2 horas):

Metodología para análisis de riesgos. Método de escenarios. Categoria de Activo, Activo, amenaza, origen, fuente, naturaleza, controles existentes, debilidades de control, escenario, probabilidad de ocurrencia, probabilidad que los controles no impidan el riesgo, pérdida a ocurrir, evaluación.

Bibliografía:

"Handbook of Information Security Management",Harold Tipton & Micki Krause. 1999
"CISSP Prep Guide: Mastering the Ten Domains of Computer Security", Ronald L. Krutz, Russell Dean Vines, 2001, Cap. 1

3.10 Negocios Electrónicos - Confidencialidad (4 horas):

Antecedentes y conceptos. Costos de la inseguridad. Hacker, software, shareware, freeware, el uso de puertos para servicios y seguridad en Internet. Requerimientos de Seguridad para hacer Negocios Electrónicos. Encripción – Desencripción. Claves Simétricas. Claves Asimétricas - Infraestructura de llaves públicas (PKI). Firmas Digitales. Certificados Digitales. PREGUNTAS Y RESPUESTAS.

Bibliografía:

"Handbook of Information Security Management",Harold Tipton & Micki Krause. 1999
"CISSP Prep Guide: Mastering the Ten Domains of Computer Security", Ronald L. Krutz, Russell Dean Vines, 2001, Cap. 1 y 4

3.11 Exposiciones en los medios de pago a través de Internet (2 horas):

Sistemas de Encripción. Medios de Pago Electrónico a través de Internet. Clasificación de Medios de Pago (anónimos, privados e identificados). Sistema de pago con tarjeta de crédito, SET, Smartcard. Riesgos asociados al uso de medios de pago electrónicos. PREGUNTAS Y RESPUESTAS.

Bibliografía:

"Handbook of Information Security Management",Harold Tipton & Micki Krause. 1999
"Web Security & Commerce", Simson Garfinkle, Gene Spafford, 1997, Cap. 11
"CISSP Prep Guide: Mastering the Ten Domains of Computer Security", Ronald L. Krutz, Russell Dean Vines, 2001, Cap. 4

3.12 Técnicas de Fraude y Niveles de Protección de activos (2 horas):

Niveles de protección sobre activos. Técnicas de fraude: Eavesdropping, impersonation, data didling, piggybacking, trojan horse, salami, social engineering, backdoors, logic bombs, piracy, denial of service, statistical attack, analitical attack, factoring attack, algorithmic attack, sniffing, spoofing.

Bibliografía:

"Handbook of Information Security Management",Harold Tipton & Micki Krause. 1999
www.google.com – computer crime. Información sobre cada técnica.

3.13 Revisión de la Auditoria a la Seguridad Informática (2 horas):

Fases. Planeamiento, Relevamiento, Identificación de riesgos y controles, Evaluación del cumplimiento, Comprobación del Riesgo, Informe y Seguimiento.

Bibliografía:

"Handbook of Information Security Management",Harold Tipton & Micki Krause. 1999

IV. CONTENIDO DE LA PARTE PRÁCTICA: 42 HORAS EN LABORATORIO.

1. Discusión de conceptos y estándares para presentación de trabajos y casos; exposiciones resolución de preguntas de selección múltiple y trabajos. Casuística (3 horas)

2. Desarrollo de ejercicios y casuística de temas tratados (3 horas).

3. Desarrollo de ejercicios y casuística de temas tratados. ACL 1 (3 horas).

4. Revisión y Coordinación de Proyectos (3 horas).

5. Práctica calificada (3 horas).

6. Revisión de Coordinación de Proyectos (3 horas).

7. Desarrollo de ejercicios y casuística de temas tratados. ACL 2 (3 horas).

8. Revisión de la herramienta de software ACL y aplicación de casos (3 horas).

9. Práctica calificada (3 horas).

10. Soporte en el desarrollo del proyecto (15 horas).

V. METODOLOGÍA:

Las clases de la parte teórica se desarrollaran en aula; se presentaran conceptos, métodos y técnicas que permitan planificar, y evaluar aplicaciones informáticas y su gestión, haciendo énfasis en aplicaciones concretas, y donde, el Profesor compartirá sus experiencias profesionales. La primera parte del curso está orientada a la Auditoría Informática, mientras que en la segunda parte se enfoca la seguridad informática. Los estudiantes desarrollarán **"Trabajos Prácticos de investigación bibliográfica"** o de realidades empresariales que deben ser **entregados en las oportunidades en que lo establezca el profesor del curso**; además, se combinarán con lecturas obligatorias compuestas por artículos o capítulos de libros o revistas o páginas WEB que se discutirán en clase, por lo que deben ser leídos antes de clase.

Las clases de la parte práctica se desarrollaran en Laboratorio; en donde se discutirán casos de la realidad empresarial y, en donde, se presentarán las principales características de los productos de software de auditoría, realizándose pruebas calificadas**. Los estudiantes deberán completar y exponer sus "Trabajos Prácticos" de "Investigación Aplicada", estos deberán ser expuestos en el Aula de Laboratorio**.

Debe precisarse que los Profesores de Teoría y de Laboratorio, periodicamente harán evaluaciones rápidas acerca de las lecturas y temas desarrollados. Ver el Programa Calendarizado.

VI. PONDERACIÓN DE LAS EVALUACIONES:

El promedio final del curso será calculado como un promedio ponderado según muestra el siguiente cuadro

Concepto	Ponderación	Responsable
Examen Parcial Teoría	25 %	Profesor de Teoría
Examen Final Teoría	25 %	Profesor de Teoría
Promedio de Prácticas	13 %	Profesor de Teoría
Promedio de Laboratorio	38 %	Profesor de Laboratorio

Nota Final = (2*Examen Parcial + 2*Examen Final + Promedio de Prácticas + 3*Promedio de Laboratorio)/8

Observación: Las notas de Quiz incluyen: Evaluaciones rápidas, control de lecturas, participación en clase, ejercicios, etc.

VII. BIBLIOGRAFÍA:

Páginas Web:

http://www.isaca.org
http://www.theiia.org
http://www.sans.org
http://www.acl.com
http://packetstormsecurity.org
http://www.astalavista.com

Lecturas Básicas:

"Information Systems Control & Audit", *Ron Weber, 1999*
"CISA Technical Review Manual", *ISACA, 1998 - 2003*
"Handbook of IT Auditing", *Parker, 1995 /1998 Supplement*
"Standard for Auditing Computer Applications", *Martin A. Krist, 1999*
"Handbook of Information Security Management",*Harold Tipton & Micki Krause. 1999*
"CISSP Prep Guide: Mastering the Ten Domains of Computer Security", *Ronald L. Krutz, Russell Dean Vines, 2001*
"Web Security & Commerce", *Simson Garfinkle, Gene Spafford, 1997*

Lecturas Complementarias:

"CAATTs and other BEASTs for Auditors" (2 nd. Edition)
David G. Coderre, Global Audit Publications (GAP)

"Business and Information Systems"
Robert C. Nickerson, Addison Wesley, 1998

"Information Systems: A Management Perspective (2nd. Edition)
Steven Alter, The Benjamin/Cummings Publishing Company, 1996

"Overview of the Capability Maturity Model" (CMM) Version 1.1
M.C. Paulk, C.B. Weber, S.M. García, M.B. Chrissis & M. Bush, SEI – CMU, 1993

"Fraud Detection: Using Data Analysis Techniques to Defect Fraud"
David G. Coderre, Global Audit Publications (GAP)

"101 ACL Applications: A Toolkit for Today´s Auditor" (2nd. Edition)
Richard B. Lanza, Global Audit Publications (GAP)

"ACL for Windows – Reference Manual" (Online Version 7.2.1)
ACL Services Ltd.

"ACL for Windows – User Guide" (Online Version 7.2.1)
ACL Services Ltd.

Libros Texto:

"COBIT" (2nd. Edition)
ISACA, 1998

Effective Project Management (2nd.Edition)
Robert Wysocki, Robert Beck, David Crane, Wiley Computer Publishing, 2000 Cap. 13 Monitor and Control progress

"ACL for Windows – Workbook" (Version 7.2.1)
ACL Services Ltd.,

Programa Calendarizado

Auditoría y Seguridad Informática

Ciclo 2003 - I

Semana	Teoría (2 horas)	Laboratorio (3 horas)
1	Cap. 1: Introducción – Conceptos.	Discusión de conceptos y estándares para presentación de trabajos y casos; exposiciones resolución de preguntas de selección múltiple y trabajos. **Presentación del Proyecto.**
2	Cap. 2: El Modelo COBIT	Desarrollo de ejercicios y casuística de temas tratados
3	Cap. 3: Planeamiento y ejecución de la evaluación **Quiz 1**	Desarrollo de ejercicios y casuística de temas tratados. **ACL 1**
4	Cap. 4: Gerencia de Sistemas de Información.	**Revisión y Coordinación de Proyectos**
5	Cap. 5: Proceso de Sistemas.	**Calificada 1 (Laboratorio)**
6	Cap. 6: Integridad, Confidencialidad y Disponibilidad de los Sistemas. **Quiz 2**	**Revisión y Coordinación de Proyectos**
7	Cap. 7: Desarrollo, Adquisición y Mantenimiento de Sistemas	Desarrollo de ejercicios y casuística de temas tratados. **ACL 2**
8	**EXAMEN PARCIAL**	
9	Cap. 8: Clasificación de los Datos, Funciones y Roles en la Seguridad	Revisión de la herramienta de software ACL y aplicación de casos
10	Cap. 9: Métodologia de análisis de riesgos – Método de escenarios.	**Calificada 2 (Laboratorio)**
11	Cap. 10: Negocios Electrónicos - Confidencialidad.	Revisión y Soporte al Proyecto
12	Cap. 10: Negocios Electrónicos - Confidencialidad	Revisión y Soporte al Proyecto
13	Cap. 11: Exposiciones en los medios de pago a través de Internet	Revisión y Soporte al Proyecto
14	Cap. 12: Técnicas de Fraude y Niveles de Protección de activos.	Revisión y Soporte al Proyecto
15	Cap. 13: Revisión de la Auditoria a la Seguridad Informática.	Revisión y Soporte al Proyecto **Exposición del Proyecto**
16	**EXAMEN FINAL**	