Universidad Ricardo Palma

FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA INFORMÁTICA

DEPARTAMENTO ACADÉMICO DE INGENIERÍA

PLAN DE ESTUDIOS 2006-II

SÍLABO

1. DATOS ADMINISTRATIVOS

1.1.	Nombre del curso	:	AUDITORÍA Y SEGURIDAD
1.2.	Código	:	IF 1002
1.3.	Tipo del curso	:	Teórico-Práctico-Laboratorio
1.4.	Área Académica	:	Laboratorio
1.5.	Condición	:	Obligatorio
1.6.	Nivel	:	X (Décimo)
1.7.	Créditos	:	03
1.8.	Horas semanales	:	6hrs
1.9.	Requisito	:	IF 0902 Administración de Proyectos Informáticos IF0903 Gerencia Informática
1.10.	Profesor	:	Yopla Mercado, Yolanda

2. SUMILLA.

El curso se divide en dos partes, donde en la primera se prepara al estudiante en dar los conocimientos de auditoria, técnicas, métodos entre otros para integrar equipos de auditoria y poder realizar labores de auditoria de sistemas principalmente, desde la planificación de auditoria hasta la formulación y presentación del informe de auditoria. En la segunda parte se prepara al estudiante en todos los fundamentos para que este en la capacidad de implementar sistemas de gestión de la seguridad de la información alineado a las normas ISO referente a seguridad de la información y buenas practicas.

3. COMPETENCIAS DE LA CARRERA

3.1 Evalúa la gestión y operatividad de las áreas de tecnologías de información buscando causas que han puesto en riesgos la operatividad del soporte de las tecnologías de información al negocio.

3.2 Permite a los alumnos estar preparado para integrar equipos de control para labores de auditoria de sistemas, así como para equipos que van ha evaluar riesgos e implementación de labores de seguridad de información a través de la implementación de las normas ISO de la serie 27000.

3.3 Propone la integración de soluciones tecnológicas de información y procesos del negocio para encontrar las necesidades del negocio y otras empresas permitiendo alcanzar sus objetivos en una efectiva y eficiente forma.

4. COMPETENCIAS DEL CURSO

4.1. Planificación.- Para una labor de auditoria y/o seguridad se debe realizar un adecuado levantamiento de información de acuerdo a los objetivos trazados que permita realizar labores e planificación, tanto de auditoria como de seguridad de la información..

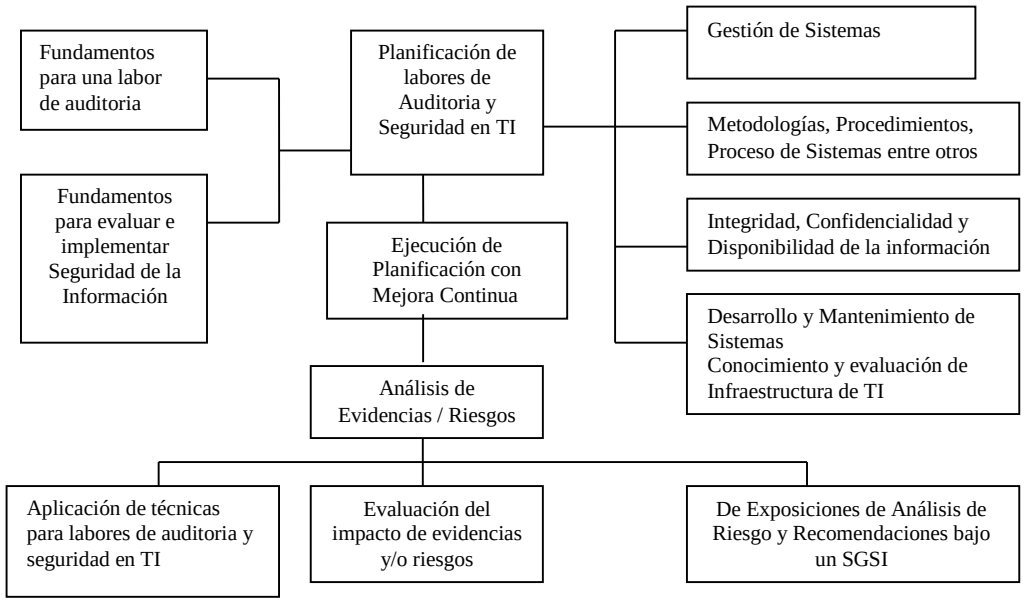
4.2. Análisis.- Permite aplicar todos los conocimientos que a la fecha el alumno tiene, para una adecuada labor de auditoria de sistemas o labores de seguridad de la información.

4.3. Aplica los criterios del Control Interno a todo proceso / actividad en su carrera profesional. Así como la aplicación de las buenas practicas de ITIL, Cobit.

4.4. Administra los principales riesgos a la integridad, confidencialidad y disponibilidad de la información de la empresa, sobre la base del análisis de riesgos.

4.5. Presenta alternativas basada en casos de cómo diseñar e implementa mecanismos de protección contra las principales técnicas de delitos informáticos

5. RED DE APRENDIZAJE:



6. PROGRAMACIÓN SEMANAL DE LOS CONTENIDOS

UNIDAD TEMÁTICA N° 1: CONCEPTOS BASICOS Y DEFINICIONES PREVIAS

Logro de la Unidad: Reformar los conocimientos de los alumnos en los conocimientos necesarios que se debe tener para el desarrollo de una labor de auditoria y seguridad en tecnologías de información.

Nº de horas: 03

SEMANA	CONTENIDOS	ACTIVIDADES DE APRENDIZAJE
1	Introducción al curso Conceptos básicos para el desarrollo del curso Derecho informático	Introducción al curso /Objetivo del curso / Marco conceptual / Metodología para la labor de auditoria de sistemas / Tipos y niveles según sistemas de información / Metodología de desarrollo de sistemas de información / La organización y el área de informática / Certificaciones y especializaciones en el Área de TI / Derecho Informático / Pirámide del Kelsen / Entidades emisoras de normas sobre Tecnología de Información

UNIDAD TEMÁTICA N° 2: DEFINICIONES DE AUDITORIA GUBERNAMENTAL y AUDITORIA DE SISTEMAS. HERRAMIENTAS PARA LABORES DE AUDITORIA

Logro de la Unidad: Dar los conceptos de auditoria y porque se realiza labores de auditoria, así como el perfil y rol del auditor de sistemas, así como el conocimiento de herramientas automatizadas para labores de auditoria de sistemas.

Nº de horas: 03

SEMANA	CONTENIDOS	ACTIVIDADES DE APRENDIZAJE
2	Auditoria Gubernamental Definición de Auditoria de Sistemas Técnicas de Auditoria Asistido por Computadora – TAAC y Técnicas en General	Porque se realiza una labor de auditoria gubernamental / Conocer la estructura del Sistema Nacional de Control del Perú / Tipos de Auditoria Gubernamental / Definición Características / Riesgos / Tipos y clasificación / Justificación / Objetivos /Perfil / Rol / TAAC

UNIDAD TEMÁTICA N° 3: FUNDAMENTOS PARA UNA PLANIFICACIÓN DE AUDITORÍA DE SISTEMAS

Logro de la Unidad: Que los alumnos conozcan una metodología para una labor integral de auditoria, asimismo, que conozcan sobre certificaciones para labores de auditoria de sistemas, así como conocimiento de buenas practicas a través de la aplicación de COBIT.
Nº de horas: 06

SEMANA	CONTENIDOS	ACTIVIDADES DE APRENDIZAJE
3	Isaca y Cobit Sistema de Control Interno	Organizaciones de Auditoria de Sistemas /Que es ISACA ? / Certificaciones de ISACA /Que es Cobit? / Metodología COBIT /Gobierno IT / Sistema de Control Interno
4	Cuestionario de Control Interno Metodología para una labor de auditoria de sistemas Formulación de un plan de auditoria Casos propuesto y resueltos	Definición de Cuestionario / Características / Supuestos en un cuestionarios / preguntas claves en la formulación de un cuestionario / Tipos de preguntas de aplicación en cuestionarios /Ejemplos / Metodología para labor de auditoria

UNIDAD TEMÁTICA N° 4: PLANIFICACIÓN Y EJECUCÓON DE UNA LABOR DE AUDITORÍA DE SISTEMAS
Logro de la Unidad: Dar los conceptos básicos para que puedan realizar labores de planificación de labores de auditoria enfocada al desarrollo de un objetivo definido, que les permita encontrar evidencias y/o riesgos para realizar de ser el caso la formulación de observaciones, conclusiones y/o recomendaciones.
Nº de horas: 06

SEMANA	CONTENIDOS	ACTIVIDADES DE APRENDIZAJE
5	Formulación de un programa de auditoria Formulación de hallazgos de auditoria Casos propuesto y resueltos	Estructura de un programa de auditoria / normas a aplicar según el caso / formulación de programas de auditoria / atributos del hallazgos / ejemplos y casos resueltos y propuestos
6	Desarrollo de casos de auditoria Formulación de observaciones, conclusiones y recomendaciones Casos propuesto y resueltos	Definición de observaciones, conclusiones y recomendaciones / ejemplos de formulación y casos resueltos y propuestos

UNIDAD TEMÁTICA N° 5: INFORMES DE AUDITORÍA
Logro de la Unidad: Que los alumnos sepan formular informes de auditoria, así como saber documentar toda la evidencia que respalde el informe de auditoria a través de los papeles de trabajo.
Nº de horas: 03

SEMANA	CONTENIDOS	ACTIVIDADES DE APRENDIZAJE
7	Formulación de un informe técnico de auditoria Formulación de un informe de auditoria Papeles de trabajo de una labor de auditoria Casos propuesto y resueltos	Estructura de informes de auditoria, informes técnicos que sustenta y respalda los informes de auditoria / ejemplos de informes/ desarrollo de informes a través de las observaciones

UNIDAD TEMÁTICA N° 6: LA SEGURIDAD DE LA INFORMACIÓN Y EVALUACIÓN DE RIESGOS EN TI
Logro de la Unidad: Dar los conocer la importancia de la seguridad de la información que se viene dando hoy en día en las organizaciones y las acciones que vienen tomando, sobre un análisis de riesgo.
Nº de horas: 06

SEMANA	CONTENIDOS	ACTIVIDADES DE APRENDIZAJE
9	La seguridad de la información, principios básicos Gestión de Riesgos y Matriz de Riesgos	La importancia de la seguridad de la información / principios de confidencialidad, integridad y disponibilidad, enfoque de análisis de riegos y gestión de riesgos / alternativas de solución / video
10	Certificaciones CISO y Fundamentos para implementar un modelo de Sistema de Gestión de la Seguridad de la Información – SGSI	La importancia del oficial de seguridad de la información -CSO/ certificaciones para CSO / Definiciones de Procedimientos / Proceso /

	Basado en la normas ISO de la serie 2700X	Acciones para implementar un modelo de SGSI

UNIDAD TEMÁTICA N° 7: IMPLEMENTACIÓN DE UN MODELO DE SGSI – PARTE I

Logro de la Unidad: Desarrollo de actividades y/o acciones que permita al negocio implementar como buenas prácticas: Política de Seguridad, Organización de la Seguridad de la Información, Gestión de Activos, Seguridad de los Recursos Humanos, Seguridad Física y Ambiental, Gestión de las Comunicaciones, Operaciones y Control de Accesos en aras de incrementar la seguridad y disminuir los riesgos de la información del negocio.

Nº de horas: 09

SEMANA	CONTENIDOS	ACTIVIDADES DE APRENDIZAJE
11	Dominio 01: Política de Seguridad Dominio 02: Organización de Seguridad/Organización de la Seguridad de la Información Dominio 03: Administración de Activos/Gestión de Activos	Política de seguridad de la información / Documento de política de seguridad de la información /. Revisión de la política de seguridad de la información / Organización de la Seguridad de la Información / Responsabilidad de los Activos / Clasificación de la Información
12	Dominio 04: Seguridad de los Recursos Humanos Dominio 05: Seguridad Física y Ambiental	Seguridad en la definición del trabajo y los recursos / Seguridad en el desempeño de las funciones del empleo / Finalización o cambio del puesto de trabajo / Áreas seguras / Seguridad de los equipos.
13	Dominio 06: Gestión de las Comunicaciones y Operaciones Dominio 07: Sistema de Control de Accesos/Control de Accesos	Procedimientos y responsabilidades de operación / Supervisión de los servicios contratados a terceros. / Planificación y aceptación del sistema. / Protección contra software malicioso y código móvil. / Gestión interna de soportes y recuperación / Gestión de redes. / Utilización y seguridad de los soportes de información. / Intercambio de información y software. / Servicios de comercio electrónico / Monitorización / Requisitos de negocio para el control de accesos. / Gestión de acceso de usuario / Responsabilidades del usuario / Control de acceso en red / Control de acceso al sistema operativo / Control de acceso a las aplicaciones / Informática móvil y tele trabajo / Ejemplos y trabajos en grupo

UNIDAD TEMÁTICA N° 8: IMPLEMENTACIÓN DE UN MODELO DE SGSI – PARTE II

Logro de la Unidad: Desarrollo de actividades y/o acciones que permita al negocio implementar como buenas prácticas: Adquisición, Desarrollo y Mantenimiento de Sistemas de Información, Gestión de Incidentes de Seguridad de la Información, Plan de Continuidad del Negocio y Cumplimiento en aras de incrementar la seguridad y disminuir los riesgos de la información del negocio.

Nº de horas: 06

SEMANA	CONTENIDOS	ACTIVIDADES DE APRENDIZAJE
14	Dominio 08: Adquisición, Desarrollo y Mantenimiento de Sistemas de Información Dominio 09: Administración/Gestión de Incidentes de Seguridad de la Información	Requisitos de seguridad de los sistemas. / Seguridad de las aplicaciones del sistema / Controles criptográficos / Seguridad de los ficheros del sistema / Seguridad en los procesos de desarrollo y soporte / Gestión de las vulnerabilidades técnicas / Comunicación de eventos y debilidades en la seguridad de la información / Gestión de incidentes y mejoras en la seguridad de la información.
15	Dominio 10: Plan de Continuidad del Negocio/Gestión de la Continuidad Comercial Dominio 11: Cumplimiento	Aspectos de la gestión de continuidad del negocio / Proceso de la gestión de continuidad del negocio / Continuidad del negocio y análisis de impactos /

		Conformidad con los requisitos legales / Revisiones de la política de seguridad y de la conformidad técnica. / Consideraciones sobre la auditoria de sistemas.

7. LABORATORIOS Y EXPERIENCIAS PRÁCTICAS

Laboratorio 1: Formulación de la Planificación de Auditoria en base a un objetivo determinado
Laboratorio 2: Formulación de Hallazgos de Auditoria
Trabajo 1 : Presentación de un Informe de Auditoria
Laboratorio 3: Funciones del Área de Seguridad de la Información, Políticas de Seguridad de la Información
Laboratorio 4: Desarrollo de Acciones, Procedimientos y/o Procesos para implementar dominios del SGSI
Trabajo 2 : Presentación del Sistema de Gestión de Seguridad de la Información en forma integral

8. TÉCNICAS DIDÁCTICAS

7.1. Dialogo simultaneo
7.2. Tormenta de ideas
7.3. Técnica expositiva
7.4. Videos
7.5. Formulación de Casos y Soluciones con participación de los alumnos
7.6. Pizarrón

9. EQUIPOS, INSTRUMENTOS Y MATERIALES

8.1 Equipos e Instrumentos:

Salón de clase con equipo multimedia

Laboratorio equipado con equipos de cómputo que permita descargar software libre como herramientas TAAC para auditoria. Así como equipos con proyector multimedia

9.2 Materiales:

Que los equipos de laboratorio tengan instalados software de desarrollo y software de base de datos

10. EVALUACIÓN

9.1. Criterios:

- La asistencia a clases es del 70 % como mínimo.
- Conocimientos
- Desarrollar los casos dejados en forma grupales
- Orden y claridad de ideas en las exposiciones, debates y diálogos.
- Presentación de trabajos en forma ordenada y concordante

9.2. Fórmula:

El Promedio Final PF se calcula tal como se muestra a continuación:

$$PF = [2EA + 2EB + 3((LB1 + LB2 + TF1 + LB3 + LB4 + TF2)/6) + (PC1 + PC2)/2] / 8$$

EA: Examen Parcial EB: Examen Final
PC: Prácticas Calificadas LB: Laboratorios Calificados
TF: Trabajo Final

10. REFERENCIAS BIBLIOGRÁFICAS Y OTRAS FUENTES

a. AUDITORÍA INFORMÁTICA
Un Enfoque Práctico, 2ª Ed. Ampliada y Revisada

PIATTINI, Mario y Del PESO, Emilio (coordinadores)
Editorial Alfaomega-Rama, 2005

b. TÉCNICAS DE LA AUDITORÍA INFORMÁTICA
DERRIEN, Yann
Editorial Alfaomega-Rama, 2005

c. Auditoria Informática.
José Antonio Echenique.
Ed. Mc-Graw Hill.

Referencias en la Web

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