UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN
ESCUELA INGENIERIA DE SISTEMAS Y TELEMATICA

1. Datos generales

Materia: AUDITORÍA Y SEGURIDAD DE SISTEMAS

Código: FAD0216

Paralelo:

Periodo : Septiembre-2017 a Febrero-2018

Profesor: CRESPO MARTINEZ PAUL ESTEBAN

Correo electrónico ecrespo@uazuay.edu.ec

Docencia	Práctico	Autónomo: 0		Total horas
		Sistemas de tutorías	Autónomo	
4				4

Prerrequisitos:

Código: FAD0200 Materia: TELECOMUNICACIONES III

2. Descripción y objetivos de la materia

Las nuevas de Tecnologías de Información promueven a las empresas a utilizar estas tecnologías. Esto crea una dependencia del uso de TI, así como la vulnerabilidad a posibles riesgos en la gestión de la información. Esta materia da a conocer los cimientos teóricos-prácticos que fundamentan la aplicación de los métodos, técnicas y herramientas de la Auditoría y Seguridad de Sistemas, que permite al estudiante realizar la evaluación profesional de la gestión de los modernos sistemas computacionales en las empresas. Para este fin el estudiante se enriquecerá de conocimiento de Gobierno TI, Cobit, Seguridad de la información, Administración de Riesgos de la Empresa, y Herramientas de auditaría y seguridad de la información para estar preparados para gestionar auditorías de sistemas.

Auditoría y Seguridad de Sistemas permite al estudiante enriquecer su conocimiento de técnicas de Gobierno TI, Cobit, Seguridad de la información, Administración de Riesgos de la Empresa, y Herramientas automatizadas para auditar. Basado en las buenas prácticas internacionales y a esto le sumamos la aplicación de casos prácticos reforzará la permanencia del conocimiento y estarán preparados para gestionar auditorías de sistemas

Auditoría y Seguridad de Sistemas se relaciona con varias de las materias de la malla curricular de la carrera de Ingeniería de Sistemas entre ellas tenemos: Telecomunicaciones, Base de Datos, Emprendedores, Ingeniería de Software, Calidad de Software y Sistemas de Información Gerencial. Todas estas son insumos y unidos al contenido que se suministra en esta materia hace que el estudiante esté preparado para poder gestionar auditorías de sistemas en las empresas.

3. Contenidos

1	**GOBIERNO EN TECNOLOGÍA DE LA INFORMACIÓN**
1.1	Que es IT Governance?, responsabilidades del Gobierno TI (1 horas)
1.2	Evolución, Cambio e Innovación en la Organización de TI (1 horas)
1.3	Estrategias, Estándares y lineamientos de TI (1 horas)
1.4	Marco de Gobernabilidad de las TI (2 horas)
1.5	Herramientas, Procesos e Indicadores de TI (1 horas)
1.6	Estructura de la organización, roles y responsabilidades, relacionadas con el uso y la administración de TI (1 horas)
1.7	La arquitectura de TI de la empresa, y sus implicaciones en el establecimiento de direcciones estratégicas de largo plazo. (2 horas)
2	**ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS**
2.1	Antecedentes de la Auditoría (,5 horas)
2.2	Definición general de la Auditoría (,5 horas)
2.3	Conceptos básicos sobre la Auditoría (,5 horas)
2.4	Clasificación de los tipos de Auditoría (,5 horas)
2.5	Auditoría Forense (1 horas)
2.6	Perfiles, Responsabilidades y Principios de Auditoria de Sistemas (,5 horas)
2.7	Funciones de Auditoria de Sistemas (2 horas)
2.8	Objetivos generales de la Auditoría de Sistemas (2 horas)

2.9	Normas generales de Auditoría (,5 horas)
3	**INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION**
3.1	Introducción de Seguridad de la Información (1 horas)
3.2	Infraestructura de seguridad de la información (2 horas)
3.3	Monitoreo y Planificación de rendimiento de TI (1 horas)
3.4	Procesos de eCommerce y eBusiness (2 horas)
3.5	Seguridad en eCommerce (2 horas)
4	**EL CONTROL INTERNO INFORMATICO - COBIT**
4.1	Introducción - Gobierno TI - Gobierno Empresarial TI (1 horas)
4.2	Características COBIT5 (3 horas)
4.3	Principios COBIT 5 (3 horas)
4.4	Catalizadores (3 horas)
4.5	Implementación (1 horas)
4.6	Modelo de evaluación de capacidad de procesos (3 horas)
5	**METODOLOGÍA PARA REALIZAR LA AUDITORÍA DE SISTEMAS**
5.1	Introducción y Necesidades de Auditoría Informática (,5 horas)
5.2	Dimensiones del Auditor Informático (,5 horas)
5.3	Entorno de la Auditoría Informática (,5 horas)
5.4	Ejecución de una auditoria de SI (1 horas)
5.5	Resumen Fases de Auditoría Informática (1 horas)
5.6	Papeles de trabajo (1 horas)
5.7	Técnicas de Auditoría (1 horas)
5.8	Trabajo Práctico: (2 horas)
5.9	Taller de uso de la herramienta IDEA ó ACL (1 horas)
6	**SEGURIDAD DE INFORMACIÓN Y ERM (ENTERPRISE RISK MANAGEMENT)**
6.1	Introducción a la administración de la seguridad de Información (,5 horas)
6.2	Normas estándares internacionales de seguridad (2 horas)
6.3	ISO 27000 - SASI (1 horas)
6.4	Análisis comparativo de ISO17799 e ISO27000 (,5 horas)
6.5	ERM (Enterprise Risk Management) (2,5 horas)
6.6	COSO-II - ERM (1 horas)

4. Sistema de Evaluación

Resultado de aprendizaje de la carrera relacionados con la materia

Resultado de aprendizaje de la materia	Evidencias
af. Diseña, implementa, analiza y gestiona sistemas de seguridad de la Información aplicando estandares internacionales.	
-Conoce las bases de seguridad informática.	-Prácticas de laboratorio -Trabajos prácticos - productos
-Conocer y utilizar software especializado para Auditoría de Sistemas.	-Prácticas de laboratorio -Trabajos prácticos - productos
-Conocer y utilizar software especializado para aumentar la seguridad en las aplicaciones.	-Prácticas de laboratorio -Trabajos prácticos - productos
ah. Planifica, evalua y ejecuta las estrategias, planes y programas de TI, en base a los requerimientos del negocio.	
-Aplica metodologías reconocidas para asegurar que la información no sea vulnerable.	-Evaluación escrita -Foros, debates, chats y otros -Trabajos prácticos - productos
-Aplica métodos y tecnologías aceptadas internacionalmente para realizar una auditoría exitosa.	-Evaluación escrita -Trabajos prácticos - productos
-Conocer y aplicar Gobierno TI.	-Evaluación escrita -Trabajos prácticos -

Resultado de aprendizaje de la carrera relacionados con la materia

Resultado de aprendizaje de la materia	Evidencias
	productos
-Reconoce, instala, administra y documenta los mecanismos y herramientas de seguridad de la información aprendida.	-Informes -Trabajos prácticos - productos
-Usar prácticas de auditoría a nivel gerencial para la toma de decisiones.	-Informes -Trabajos prácticos - productos

Desglose de evaluación

Evidencia	Descripción	Contenidos sílabo a evaluar	Aporte	Calificación	Semana
Evaluación escrita	Evaluación escrita sobre fundamentos de gobierno, auditoria y riesgo.	ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS, GOBIERNO EN TECNOLOGÍA DE LA INFORMACIÓN	APORTE 1	5	Semana: 4 (16/10/17 al 21/10/17)
Trabajos prácticos - productos	Presentación de trabajos sobre marcos de referencia de Gobierno, Seguridad y Auditoria	ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS, GOBIERNO EN TECNOLOGÍA DE LA INFORMACIÓN	APORTE 1	5	Semana: 5 (23/10/17 al 28/10/17)
Informes	Informe sobre análisis forense	ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS	APORTE 2	3	Semana: 6 (30/10/17 al 01/11/17)
Prácticas de laboratorio	Prácticas de laboratorio: Uso de herramientas para el análisis de vulnerabilidades	INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION	APORTE 2	4	Semana: 7 (06/11/17 al 11/11/17)
Evaluación escrita	Evaluación escrita sobre principios y catalizadores de COBIT	INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION	APORTE 2	3	Semana: 8 (13/11/17 al 15/11/17)
Informes	Informe de auditoria	EL CONTROL INTERNO INFORMATICO - COBIT, METODOLOGÍA PARA REALIZAR LA AUDITORÍA DE SISTEMAS	APORTE 3	8	Semana: 13 (18/12/17 al 22/12/17)
Foros, debates, chats y otros	Discusión sobre el informe de auditoria realizado.	EL CONTROL INTERNO INFORMATICO - COBIT, METODOLOGÍA PARA REALIZAR LA AUDITORÍA DE SISTEMAS	APORTE 3	2	Semana: 14 (al)
Evaluación escrita	Resolución de un caso de auditoria informática, aplicando herramientas y técnicas de la auditoria, seguridad y gobierno.	ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS, EL CONTROL INTERNO INFORMATICO - COBIT, GOBIERNO EN TECNOLOGÍA DE LA INFORMACIÓN, INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION, METODOLOGÍA PARA REALIZAR LA AUDITORÍA DE SISTEMAS, SEGURIDAD DE INFORMACIÓN Y ERM (ENTERPRISE RISK MANAGEMENT)	EXAMEN	20	Semana: 17-18 (14-01-2018 al 27-01-2018)
Evaluación escrita	Evaluación sobre la teoría y conceptos aprendidos mediante el uso de reactivos.	ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS, EL CONTROL INTERNO INFORMATICO - COBIT, GOBIERNO EN TECNOLOGÍA DE LA INFORMACIÓN, INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION, METODOLOGÍA PARA REALIZAR LA AUDITORÍA DE SISTEMAS, SEGURIDAD DE INFORMACIÓN Y ERM (ENTERPRISE RISK MANAGEMENT)	SUPLETORIO	10	Semana: 19-20 (28-01-2018 al 03-02-2018)
Evaluación escrita	Resolución de un caso de auditoria informática, aplicando herramientas y técnicas de la auditoria, seguridad y gobierno.	ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS, EL CONTROL INTERNO INFORMATICO - COBIT, GOBIERNO EN TECNOLOGÍA DE LA INFORMACIÓN, INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION, METODOLOGÍA PARA REALIZAR LA AUDITORÍA	SUPLETORIO	10	Semana: 19-20 (28-01-2018 al 03-02-2018)

Evidencia	Descripción	Contenidos sílabo a evaluar	Aporte	Calificación	Semana
		DE SISTEMAS, SEGURIDAD DE INFORMACIÓN Y ERM (ENTERPRISE RISK MANAGEMENT)			

Metodología

Se tomarán lecciones orales al inicio de cada clase sobre el contenido de la clase anterior.
Se realizarán trabajos prácticos aplicando los conocimientos adquiridos en clase. Estos trabajos son explicados su alcance previamente. Los trabajos son sustentados por los estudiantes en clase, con el objetivo que el resto de estudiantes adquieran mayor conocimiento.
Se tomará una prueba escrita sobre el contenido de la materia, las mismas que serán notificadas a estudiante en clase con anticipación de una semana.
Se tomará un examen final al concluir el ciclo, cuyo contenido será sobre todas las unidades.
Para las pruebas se evaluará el conocimiento adquirido de los temas tratados en la última clase, por lo que el estudiante que no asistió está en la obligación de igualar su conocimiento previamente. Si el estudiante no está presente al momento de la prueba no tendrá nota de ese aporte y no podrá recuperarla posteriormente. Además, no se recibirán trabajos extemporáneos.

Criterios de Evaluación

Se tomarán lecciones orales al inicio de cada clase sobre el contenido de la clase anterior.
Se realizarán trabajos prácticos aplicando los conocimientos adquiridos en clase. Estos trabajos son explicados su alcance previamente. Los trabajos son sustentados por los estudiantes en clase, con el objetivo que el resto de estudiantes adquieran mayor conocimiento.
Las pruebas escritas contemplan teoría (opción múltiple) y razonamiento.
El trabajo del tercer parcial consiste en la aplicación de uno de los principios de COBIT y sus catalizadores para hacer una evaluación a una empresa. El informe de auditoria será tratado con absoluta confidencialidad y los resultados obtenidos serán socializados en un foro o debate dentro del curso.
Se tomará un examen final al concluir el ciclo, cuyo contenido será sobre todas las unidades. Este examen consiste en la resolución de un caso empresarial, aplicando las herramientas y técnicas aprendidas en auditoria, seguridad y gobierno de TI.
No se aceptarán trabajos, tareas o lecciones fuera del plazo establecido.
Para las sustentaciones y trabajos, se considerará:
- Diapositivas con máximo 7 lineas de texto
- Documentos libres de faltas ortográficas
- Conocimiento y dominio del tema
- Creatividad en el análisis y sustento de ideas
- Aplicación de conceptos técnicos relacionados con la materia
- Imagen, postura y calidad de expresión del expositor
- Control del tiempo asignado
- Equilibrio del grupo (Participación de todos)
- Manejo de preguntas y respuestas
- Correcto uso del material audiovisual.

Al momento de la sustentación de los trabajos de los otros grupos guarde respeto escuchando con atención la exposición, porque inclusive puede recibir preguntas sobre el mismo y será evaluado
Durante y después de la exposición, los alumnos y el profesor podrán realizar preguntas a un miembro especifico del grupo expositor sobre el contenido del caso
Los trabajos serán entregados vía correo electrónico (con confirmación de recepción) en la fecha establecida, en formato A4, usando letra tipo Times New Roman 12 para el texto normal, 12 con mayúsculas y negrita para títulos y 12 con negrita y cursiva para subtítulos, márgenes superior e izquierdo de 3 cm. e inferior y derecho de 2 cm. y 1,5 de espacio entre líneas. Al final del trabajo se agregará la leyenda "Por mi honorabilidad y ética, declaro que el presente trabajo es fruto de mi propio esfuerzo".
En todos los trabajos se tomará en cuenta la redacción y ortografía. Trabajos copiados entre compañeros, bajados de Internet o tomados de otras fuentes serán calificados con cero puntos y reportados a las autoridades universitarias respectivas.

5. Referencias

Bibliografía base

Libros

Autor	Editorial	Título	Año	ISBN
DERRIEN, Y	Marcomb	TÉCNICAS DE LA AUDITORÍA INFORMÁTICA	2009	9781449209667
GÓMEZ VIEITES, A	Rama	ENCICLOPEDIA DE LA SEGURIDAD INFORMÁTICA	2011	9788499640365
VILCHES TRONCOSO, R	El Cid	APUNTES DEL ESTUDIANTE DE AUDITORÍA	2005	Apuntes del estudiante de

Web

Autor	Título	URL
Rattan Vikas - Biblioteca	E-Commerce Security Using Pki Approach	http://web.ebscohost.com/ehost/detail?
Shahibi, Mohd. Sazili1	Security Factor And Trust In E-Commerce	http://web.ebscohost.com/ehost/detail?

Software

Bibliografía de apoyo

Libros

Autor	Editorial	Título	Año	ISBN
ISACA	ISACA	COBIT 5	2013	
ISACA		Cobit 5 - Guía de autoevaluación	2013	
ISACA	ISACA	COBIT 5 EL MARCO	2013	9781604202823

Web

Autor	Título	URL
Chidi Henry Emeribe, CISA, COBIT 5 Foundation	Establishing a Governance and Management Structure for E-commerce Using COBIT 5	http://www.isaca.org/COBIT/focus/Pages/establishing-a-
Greet Volders, CGEIT, COBIT Certified Assessor and Kees de Jong, CIPM, CISSP, SIPP/E	Implementing COBIT 5 at ENTSO-E	http://www.isaca.org/COBIT/focus/Pages/implementing-
Greet Volders, CGEIT,	Implementing COBIT 5 at ENTSO-E	http://www.isaca.org/COBIT/focus/Pages/implementing-

Software

Autor	Título	URL	Versión
Autopsy - Sleuthkit	Autopsy		4
ACL	ACL		
Microsoft	Microsoft Power BI		
Kali	Kali Linux		

Docente

Director/Junta

Fecha aprobación: 13/09/2017

Estado: Aprobado