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-2018 a Febrero-2019

Profesor: PINTADO ZUMBA PABLO FERNANDO

Correo electrónico ppintado@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.	-Evaluación escrita -Evaluación oral -Investigaciones -Prácticas de campo (externas) -Prácticas de laboratorio -Trabajos prácticos - productos
-Conocer y utilizar software especializado para Auditoría de Sistemas.	-Evaluación escrita -Evaluación oral -Investigaciones -Prácticas de campo (externas) -Prácticas de laboratorio -Trabajos prácticos - productos
-Conocer y utilizar software especializado para aumentar la seguridad en las aplicaciones.	-Evaluación escrita -Evaluación oral -Investigaciones -Prácticas de campo

Resultado de aprendizaje de la carrera relacionados con la materia

Resultado de aprendizaje de la materia	Evidencias
	(externas) -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 -Evaluación oral -Investigaciones -Prácticas de campo (externas) -Trabajos prácticos - productos
-Aplica métodos y tecnologías aceptadas internacionalmente para realizar una auditoría exitosa.	-Evaluación escrita -Evaluación oral -Investigaciones -Prácticas de campo (externas) -Trabajos prácticos - productos
-Conocer y aplicar Gobierno TI.	-Evaluación escrita -Evaluación oral -Investigaciones -Prácticas de campo (externas) -Trabajos prácticos - productos
-Reconoce, instala, administra y documenta los mecanismos y herramientas de seguridad de la información aprendida.	-Evaluación escrita -Evaluación oral -Investigaciones -Prácticas de campo (externas) -Trabajos prácticos - productos
-Usar prácticas de auditoría a nivel gerencial para la toma de decisiones.	-Evaluación escrita -Evaluación oral -Investigaciones -Trabajos prácticos - productos

Desglose de evaluación

Evidencia	Descripción	Contenidos sílabo a evaluar	Aporte	Calificación	Semana
Evaluación oral	evaluación oral	ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS, GOBIERNO EN TECNOLOGÍA DE LA INFORMACIÓN	APORTE 1	1	Semana: 5 (15/10/18 al 20/10/18)
Trabajos prácticos - productos	trabajos prácticos en campo	ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS, GOBIERNO EN TECNOLOGÍA DE LA INFORMACIÓN	APORTE 1	5	Semana: 5 (15/10/18 al 20/10/18)
Evaluación escrita	prueba	ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS, GOBIERNO EN TECNOLOGÍA DE LA INFORMACIÓN	APORTE 1	4	Semana: 5 (15/10/18 al 20/10/18)
Evaluación oral	lección	EL CONTROL INTERNO INFORMATICO - COBIT, INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION	APORTE 2	1	Semana: 10 (19/11/18 al 24/11/18)
Trabajos prácticos - productos	trabajos prácticos y en campo	EL CONTROL INTERNO INFORMATICO - COBIT, INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION	APORTE 2	5	Semana: 10 (19/11/18 al 24/11/18)
Evaluación escrita	prueba	EL CONTROL INTERNO INFORMATICO - COBIT, INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION	APORTE 2	4	Semana: 10 (19/11/18 al 24/11/18)
Trabajos prácticos - productos	trabajo práctico y en campo	METODOLOGÍA PARA REALIZAR LA AUDITORÍA DE SISTEMAS, SEGURIDAD DE INFORMACIÓN Y ERM (ENTERPRISE RISK	APORTE 3	5	Semana: 15 (al)

Evidencia	Descripción	Contenidos sílabo a evaluar	Aporte	Calificación	Semana
		MANAGEMENT)			
Evaluación oral	lección	METODOLOGÍA PARA REALIZAR LA AUDITORÍA DE SISTEMAS, SEGURIDAD DE INFORMACIÓN Y ERM (ENTERPRISE RISK MANAGEMENT)	APORTE 3	1	Semana: 15 (al)
Evaluación escrita	prueba	METODOLOGÍA PARA REALIZAR LA AUDITORÍA DE SISTEMAS, SEGURIDAD DE INFORMACIÓN Y ERM (ENTERPRISE RISK MANAGEMENT)	APORTE 3	4	Semana: 15 (al)
Evaluación escrita	examen final	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: 19-20 (20-01-2019 al 26-01-2019)
Evaluación escrita	Supletorio	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	20	Semana: 21 (al)

Metodología

Se tomaran 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 en cada aporte 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.
El resultado de las evaluaciones serán entregadas a los estudiantes como máximo hasta la segunda clase después de la fecha de la evaluación y antes de la entrega de notas en la Universidad (fechas prefijadas por la Universidad).
Para las lecciones 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 lección no tendrá nota de esta lección y podrá recuperar luego de haber sido evaluados ese aporte al resto de estudiantes y antes de haber sido entregado las notas a la Universidad.
Se recomienda considerar los siguientes aspectos para el estudio de los casos y trabajos:

- Utilice las preguntas asignadas, como guías a tratarse, no como límites o máximos a considerar, es decir, puede ampliar su alcance de investigación o aplicación para fortalecer su exposición
- Identifique los hechos más relevantes
- Defina el problema
- Formule alternativas de solución
- Analice la mayor cantidad de alternativas posibles
- Emita conclusiones y recomendaciones
- Para los trabajos prepare una presentación con apoyo de toda herramienta multimedia que apoye la exposición, en cuyas laminas cumpla la buena práctica de 7x7 (no más de 7 palabras por línea y nos mas de 7 líneas por página). El Profesor tendrá en cuenta los siguientes aspectos:

- Conocimiento y dominio del tema
- Análisis y sustento de ideas
- Aplicación de conceptos técnicos relacionados con la materia
- Imagen del expositor
- Entusiasmo
- Claridad de expresión
- &nbs

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.
Se tomarán evaluaciones escritas en cada aporte, así como el examen final y de ser el caso examen supletorio.
Los resultados de las evaluaciones serán entregados a los estudiantes como máximo hasta la siguiente clase luego de la evaluación y antes
de la entrega de notas en la Universidad (fechas prefijadas por la Universidad).
En todos los trabajos se tomará en cuenta la redacción y ortografía, por lo que se pide especial atención en estos dos aspectos ya que
existen muy buenos trabajos con buen contenido técnico y pobres en redacción y ortografía lo que dará como resultado una mala calificación
Para las investigaciones se evaluará:
Nivel de detalle, redacción, profundidad de la investigación, estructura del documento, el cual debe contener al menos:
1. Resumen
2. Introducción
3. Cuerpo de la investigación
4. Conclusiones y recomendaciones
5. Referencias bibliográficas.
Nota: Se usará la plataforma URKUND para el análisis de coincidencia.

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
ISO		ISO/IEC 27002	2013	
ISACA	ISACA	COBIT 5	2013	9781604202823
Pablo Pintado		Material de apoyo del curso	2018	

Web

Software

Autor	Título	URL	Versión
ACL	ACL		

Docente

Director/Junta

Fecha aprobación: **07/09/2018**

Estado: **Aprobado**