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: A
Periodo : Septiembre-2019 a Febrero-2020
Profesor: PINTADO ZUMBA PABLO FERNANDO
Correo electrónico: ppintado@uazuay.edu.ec

Nivel: 9

Distribución de horas.

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

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

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 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. Objetivos de Desarrollo Sostenible

4. Contenidos

1.1	Que es IT Governance?, responsabilidades del Gobierno TI
1.2	Evolución, Cambio e Innovación en la Organización de TI
1.3	Estrategias, Estándares y lineamientos de TI
1.4	Marco de Gobernabilidad de las TI
1.5	Herramientas, Procesos e Indicadores de TI
1.6	Estructura de la organización, roles y responsabilidades, relacionadas con el uso y la administración de TI
1.7	La arquitectura de TI de la empresa, y sus implicaciones en el establecimiento de direcciones estratégicas de largo plazo.
2.1	Antecedentes de la Auditoría

2.2	Definición general de la Auditoría
2.3	Conceptos básicos sobre la Auditoría
2.4	Clasificación de los tipos de Auditoría
2.5	Auditoría Forense
2.6	Perfiles, Responsabilidades y Principios de Auditoria de Sistemas
2.7	Funciones de Auditoria de Sistemas
2.8	Objetivos generales de la Auditoría de Sistemas
2.9	Normas generales de Auditoría
3.1	Introducción de Seguridad de la Información
3.2	Infraestructura de seguridad de la información
3.3	Monitoreo y Planificación de rendimiento de TI
3.4	Procesos de eCommerce y eBusiness
3.5	Seguridad en eCommerce
4.1	Introducción - Gobierno TI - Gobierno Empresarial TI
4.2	Características COBIT5
4.3	Principios COBIT 5
4.4	Catalizadores
4.5	Implementación
4.6	Modelo de evaluación de capacidad de procesos
5.1	Introducción y Necesidades de Auditoría Informática
5.2	Dimensiones del Auditor Informático
5.3	Entorno de la Auditoría Informática
5.4	Ejecución de una auditoria de SI
5.5	Resumen Fases de Auditoría Informática
5.6	Papeles de trabajo
5.7	Técnicas de Auditoría
5.8	Trabajo Práctico:
5.9	Taller de uso de la herramienta IDEA ó ACL
6.1	Introducción a la administración de la seguridad de Información
6.2	Normas estándares internacionales de seguridad
6.3	ISO 27000 - SASI
6.4	Análisis comparativo de ISO17799 e ISO27000
6.5	ERM (Enterprise Risk Management)
6.6	COSO-II - ERM

5. 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 -Prácticas de campo

Resultado de aprendizaje de la carrera relacionados con la materia

Resultado de aprendizaje de la materia	Evidencias
	(externas)
-Conocer y utilizar software especializado para Auditoría de Sistemas.	-Evaluación escrita -Evaluación oral -Prácticas de campo (externas)
-Conocer y utilizar software especializado para aumentar la seguridad en las aplicaciones.	-Evaluación escrita -Evaluación oral -Prácticas de campo (externas)

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

Desglose de evaluación

Evidencia	Descripción	Contenidos sílabo a evaluar	Aporte	Calificación	Semana
Evaluación escrita	prueba escrita	ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS, GOBIERNO EN TECNOLOGÍA DE LA INFORMACIÓN	APORTE	4	Semana: 5 (07-OCT-19 al 10-OCT-19)
Evaluación oral	lección oral	ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS, GOBIERNO EN TECNOLOGÍA DE LA INFORMACIÓN	APORTE	1	Semana: 5 (07-OCT-19 al 10-OCT-19)
Prácticas de campo (externas)	trabajo practico	ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS, GOBIERNO EN TECNOLOGÍA DE LA INFORMACIÓN	APORTE	5	Semana: 5 (07-OCT-19 al 10-OCT-19)
Evaluación escrita	prueba escrita	EL CONTROL INTERNO INFORMATICO - COBIT, INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION	APORTE	4	Semana: 10 (11-NOV-19 al 13-NOV-19)
Evaluación oral	lección escrita	EL CONTROL INTERNO INFORMATICO - COBIT, INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION	APORTE	1	Semana: 10 (11-NOV-19 al 13-NOV-19)
Prácticas de campo (externas)	trabajo practico	EL CONTROL INTERNO INFORMATICO - COBIT, INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION	APORTE	5	Semana: 10 (11-NOV-19 al 13-NOV-19)
Evaluación escrita	prueba escrita	METODOLOGÍA PARA REALIZAR LA AUDITORÍA DE SISTEMAS, SEGURIDAD DE INFORMACIÓN Y ERM (ENTERPRISE RISK MANAGEMENT)	APORTE	4	Semana: 15 (16-DIC-19 al 21-DIC-19)
Evaluación oral	lección oral	METODOLOGÍA PARA REALIZAR LA AUDITORÍA DE SISTEMAS, SEGURIDAD DE INFORMACIÓN Y ERM (ENTERPRISE RISK MANAGEMENT)	APORTE	1	Semana: 15 (16-DIC-19 al 21-DIC-19)
Prácticas de campo (externas)	trabajo practico	METODOLOGÍA PARA REALIZAR LA AUDITORÍA DE SISTEMAS, SEGURIDAD DE INFORMACIÓN Y ERM (ENTERPRISE RISK MANAGEMENT)	APORTE	5	Semana: 15 (16-DIC-19 al 21-DIC-19)
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 (13-ENE-20 al 18-ENE-20)
Evaluación escrita	examen 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	SUPLETORIO	20	Semana: 21 (al)

Evidencia	Descripción	Contenidos sílabo a evaluar	Aporte	Calificación	Semana
		MANAGEMENT)			

Metodología

Criterios de evaluación

6. 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
ISO		ISO/IEC 27002	2013	
ISACA	ISACA	COBIT 5	2013	9781604202823
Pablo Pintado		Material de apoyo del curso	2018	

Web

Autor	Título	Url
Rattan Vikas - Biblioteca Digital Ebsco	E-Commerce Security Using Pki Approach	http://web.ebscohost.com/ehost/detail?vid=7&hid=12&sid=83bc99a6-b175-4870-9ab0-9a9bb232a099%40sessio
Shahibi, Mohd. Sazili1 Fakeh, Shamsul Kamal Wan1 - Biblioteca Digital Ebsco	Security Factor And Trust In E-Commerce Transactions.	http://web.ebscohost.com/ehost/detail?vid=4&hid=12&sid=83bc99a6-b175-4870-9ab0-9a9bb232a099%40sessio

Software

Autor	Título	Url	Versión
ACL	ACL		

Revista

Bibliografía de apoyo

Libros

Autor	Editorial	Título	Año	ISBN
ISACA.ORG	ISACA.ORG	COBIT 2019 - MARCO DE REFERENCIA Objetivos de gobierno y gestión	2019	

Web

Software

Revista

Docente

Director/Junta

Fecha aprobación: 28/08/2019

Estado: Aprobado