UNIVERSIDAD DEL AZUAY

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

1. Datos

Materia: AUDITORÍA Y SEGURIDAD DE SISTEMAS
Código: FAD0216
Paralelo: A
Periodo : Septiembre-2021 a Febrero-2022
Profesor: PINTADO ZUMBA PABLO FERNANDO
Correo electrónico: ppintado@uazuay.edu.ec
Prerrequisitos:

Código: FAD0200 Materia: TELECOMUNICACIONES III

Nivel: 9

Distribución de horas.

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

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

01	GOBIERNO EN TECNOLOGÍA DE LA INFORMACIÓN
01.1	Que es IT Governance?, responsabilidades del Gobierno TI (1 horas)
01.2	Evolución, Cambio e Innovación en la Organización de TI (1 horas)
01.3	Estrategias, Estándares y lineamientos de TI (1 horas)

01.4	Marco de Gobernabilidad de las TI (2 horas)
01.5	Herramientas, Procesos e Indicadores de TI (1 horas)
01.6	Estructura de la organización, roles y responsabilidades, relacionadas con el uso y la administración de TI (1 horas)
01.7	La arquitectura de TI de la empresa, y sus implicaciones en el establecimiento de direcciones estratégicas de largo plazo. (2 horas)
02	ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS
02.1	Antecedentes de la Auditoría (1 horas)
02.2	Definición general de la Auditoría (1 horas)
02.3	Conceptos básicos sobre la Auditoría (1 horas)
02.4	Clasificación de los tipos de Auditoría (1 horas)
02.5	Auditoría Forense (1 horas)
02.6	Perfiles, Responsabilidades y Principios de Auditoria de Sistemas (1 horas)
02.7	Funciones de Auditoria de Sistemas (2 horas)
02.8	Objetivos generales de la Auditoría de Sistemas (2 horas)
02.9	Normas generales de Auditoría (1 horas)
03	INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION
03.1	Introducción de Seguridad de la Información (1 horas)
03.2	Infraestructura de seguridad de la información (2 horas)
03.3	Monitoreo y Planificación de rendimiento de TI (2 horas)
03.4	Procesos de eCommerce y eBusiness (2 horas)
03.5	Seguridad en eCommerce (2 horas)
04	EL CONTROL INTERNO INFORMATICO - COBIT
04.1	Introducción - Gobierno TI - Gobierno Empresarial TI (1 horas)
04.2	Características COBIT5 (3 horas)
04.3	Principios COBIT 5 (3 horas)
04.4	Catalizadores (3 horas)
04.5	Implementación (2 horas)
04.6	Modelo de evaluación de capacidad de procesos (3 horas)
05	METODOLOGÍA PARA REALIZAR LA AUDITORÍA DE SISTEMAS
05.1	Introducción y Necesidades de Auditoría Informática (1 horas)
05.2	Dimensiones del Auditor Informático (1 horas)
05.3	Entorno de la Auditoría Informática (1 horas)
05.4	Ejecución de una auditoria de SI (1 horas)
05.5	Resumen Fases de Auditoría Informática (1 horas)
05.6	Papeles de trabajo (2 horas)
05.7	Técnicas de Auditoría (1 horas)
05.8	Trabajo Práctico: (2 horas)
05.9	Taller de uso de la herramienta IDEA ó ACL (1 horas)
06	SEGURIDAD DE INFORMACIÓN Y ERM (ENTERPRISE RISK MANAGEMENT)
06.1	Introducción a la administración de la seguridad de Información (1 horas)
06.2	Normas estándares internacionales de seguridad (2 horas)
06.3	ISO 27000 - SASI (1 horas)
06.4	Análisis comparativo de ISO17799 e ISO27000 (1 horas)
06.5	ERM (Enterprise Risk Management) (3 horas)
06.6	COSO-II - ERM (1 horas)

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 -Trabajos prácticos - productos
-Conocer y utilizar software especializado para Auditoría de Sistemas.	-Evaluación escrita -Evaluación oral -Trabajos prácticos - productos
-Conocer y utilizar software especializado para aumentar la seguridad en las aplicaciones.	-Evaluación escrita -Evaluación oral -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 -Trabajos prácticos - productos
-Aplica métodos y tecnologías aceptadas internacionalmente para realizar una auditoría exitosa.	-Evaluación escrita -Evaluación oral -Trabajos prácticos - productos
-Conocer y aplicar Gobierno TI.	-Evaluación escrita -Evaluación oral -Trabajos prácticos - productos
-Reconoce, instala, administra y documenta los mecanismos y herramientas de seguridad de la información aprendida.	-Evaluación escrita -Evaluación oral -Trabajos prácticos - productos
-Usar prácticas de auditoría a nivel gerencial para la toma de decisiones.	-Evaluación escrita -Evaluación oral -Trabajos prácticos - productos

Desglose de evaluación

Evidencia	Descripción	Contenidos sílabo a evaluar	Aporte	Calificación	Semana
Evaluación escrita	Evaluación escrita	ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS, GOBIERNO EN TECNOLOGÍA DE LA INFORMACIÓN	APORTE	5	Semana: 5 (18/10/21 al 23/10/21)
Trabajos prácticos - productos	Trabajo practico - paritipación	ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS, GOBIERNO EN TECNOLOGÍA DE LA INFORMACIÓN	APORTE	5	Semana: 5 (18/10/21 al 23/10/21)
Evaluación escrita	Evaluación escrita	EL CONTROL INTERNO INFORMATICO - COBIT, INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION	APORTE	5	Semana: 10 (22/11/21 al 27/11/21)
Trabajos prácticos - productos	Trabajo practico	EL CONTROL INTERNO INFORMATICO - COBIT, INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION	APORTE	5	Semana: 10 (22/11/21 al 27/11/21)
Evaluación escrita	Evaluación escrita	METODOLOGÍA PARA REALIZAR LA AUDITORÍA DE SISTEMAS, SEGURIDAD DE INFORMACIÓN Y ERM (ENTERPRISE RISK MANAGEMENT)	APORTE	5	Semana: 15 (al)
Trabajos prácticos - productos	Trabajo practico	METODOLOGÍA PARA REALIZAR LA AUDITORÍA DE SISTEMAS, SEGURIDAD DE INFORMACIÓN Y ERM (ENTERPRISE RISK MANAGEMENT)	APORTE	5	Semana: 15 (al)
Evaluación escrita	Examen final	ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS, EL CONTROL INTERNO INFORMATICO - COBIT,	EXAMEN	20	Semana: 19-20 (23-01-2022 al 29-01-2022)

Evidencia	Descripción	Contenidos sílabo a evaluar	Aporte	Calificación	Semana
		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)			
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 MANAGEMENT)	SUPLETORIO	20	Semana: 21 (07/02/22 al 07/02/22)

Metodología

Por esta ocasión especial, se tomará en cuenta la participación de los estudiantes en clase con su respectiva puntuación (incluye leccones orales de la clase anterior). Así como tendremos trabajos prácticos que serán sustentados por los estudiantes en clase.
Adicionalmente, se tomará evaluaciones síncronas en cada aporte sobre el contenido de la materia, las mismas que serán notificadas al estudiante en clase con anticipación.
Se tomará un examen final al concluir el ciclo, cuyo contenido será sobre todas las unidades.
El resultado de las evaluaciones será entregado a los estudiantes en la siguiente clase después de la fecha de la evaluación y antes de la entrega de notas en la Universidad (fechas prefijadas por 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 u oportunidad
- Formule alternativas de solución u oportunidad
- 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
• Claridad de expresión
• Creatividad
• Control del tiempo asignado
• Equilibrio del grupo (Participación de todos)
• 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

- No se recibirán trabajos extemporáneos
- Debe cuidar tanto el contenido como la presentación de los trabajos tomando en cuenta que ambos son aspectos claves para el éxito.
- Serán entregados vía email (con confirmación de recepción) en la fecha pre-acordada, en formato A4, usando letra tipo Arial 10 para el texto normal, 12 con mayúsculas y negrita para títulos y 11 con negrita y cursiva para subtítulos.Debe llevar en la portada los siguientes datos centrados:

UNIVERSIDAD DEL AZUAY
FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN
ESCUELA DE INGENIERIA DE SISTEMAS y TELEMATICA
AUDITORIA Y SEGURIDAD DE SISTEMAS
TEMA O TRABAJO O CASO
NOMBRE DE LA PERSONA o GRUPO DE TRABAJO
CUENCA - ECUADOR
FECHA
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.

Criterios de Evaluación

Se tomará en cuenta la participación de los estudiantes en clase con su respectiva puntuación (incluye lecciones orales de la última clase).
Así como tendremos trabajos prácticos que serán sustentados por los estudiantes en clase.
Adicionalmente, se tomará evaluaciones síncronas en cada aporte sobre el contenido de la materia, las mismas que serán notificadas al estudiante en clase con anticipación.
Se tomará un examen final al concluir el ciclo, cuyo contenido será sobre todas las unidades.
Nota: Se usará la plataforma URKUND para el análisis de coincidencia.
El resultado de las evaluaciones será entregado a los estudiantes en la siguiente clase después de la fecha de la evaluación y antes de la entrega de notas en la Universidad (fechas prefijadas por la Universidad).
En los trabajos se tomará en cuenta la redacción y ortografía, por lo que se pide especial atención en estos dos aspectos porque existen muy buenos trabajos con buen contenido técnico y pobres en redacción y ortografía lo que dará como resultado una mala calificación

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%
Shahibi, Mohd. Sazili1 Fakeh, Shamsul Kamal	Security Factor And Trust In E-Commerce Transactions.	http://web.ebscohost.com/ehost/detail?vid=4&hid=12&sid=83bc99a6-b175-4870-9ab0-9a9bb232a099%

Software

Autor	Título	Url	Versión
ACL	ACL		

Bibliografía de apoyo

Libros

Autor	Editorial	Título	Año	ISBN
Pablo Pintado	N/A	Material de apoyo de Auditoría y Seguridad de Sitemas	2021	

Web

Software

Docente

Director/Junta

Fecha aprobación: 13/09/2021

Estado: Aprobado