



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

### 1. Datos

**Materia:** AUDITORÍA Y SEGURIDAD DE SISTEMAS  
**Código:** FAD0216  
**Paralelo:** B  
**Periodo :** Septiembre-2021 a Febrero-2022  
**Profesor:** CRESPO MARTINEZ PAUL ESTEBAN  
**Correo electrónico:** ecrespo@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 auditoría 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)
<b>02</b>	<b>ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS</b>
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 Auditoría de Sistemas (1 horas)
02.7	Funciones de Auditoría de Sistemas (2 horas)
02.8	Objetivos generales de la Auditoría de Sistemas (2 horas)
02.9	Normas generales de Auditoría (1 horas)
<b>03</b>	<b>INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION</b>
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)
<b>04</b>	<b>EL CONTROL INTERNO INFORMÁTICO - COBIT</b>
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)
<b>05</b>	<b>METODOLOGÍA PARA REALIZAR LA AUDITORÍA DE SISTEMAS</b>
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 auditoría 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)
<b>06</b>	<b>SEGURIDAD DE INFORMACIÓN Y ERM (ENTERPRISE RISK MANAGEMENT)</b>
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 estándares internacionales.

-Conoce las bases de seguridad informática.	-Prácticas de laboratorio -Reactivos -Resolución de ejercicios, casos y otros
-Conocer y utilizar software especializado para Auditoría de Sistemas.	-Prácticas de laboratorio -Reactivos -Resolución de ejercicios, casos y otros
-Conocer y utilizar software especializado para aumentar la seguridad en las aplicaciones.	-Prácticas de laboratorio -Reactivos -Resolución de ejercicios, casos y otros

#### ah. Planifica, evalúa 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.	-Prácticas de laboratorio -Reactivos -Resolución de ejercicios, casos y otros
-Aplica métodos y tecnologías aceptadas internacionalmente para realizar una auditoría exitosa.	-Prácticas de laboratorio -Reactivos -Resolución de ejercicios, casos y otros
-Conocer y aplicar Gobierno TI.	-Prácticas de laboratorio -Reactivos -Resolución de ejercicios, casos y otros
-Reconoce, instala, administra y documenta los mecanismos y herramientas de seguridad de la información aprendida.	-Prácticas de laboratorio -Reactivos -Resolución de ejercicios, casos y otros
-Usar prácticas de auditoría a nivel gerencial para la toma de decisiones.	-Prácticas de laboratorio -Reactivos -Resolución de ejercicios, casos y otros

### Desglose de evaluación

Evidencia	Descripción	Contenidos sílabo a evaluar	Aporte	Calificación	Semana
Prácticas de laboratorio	Prácticas de laboratorio	ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS, GOBIERNO EN TECNOLOGÍA DE LA INFORMACIÓN	APORTE	5	Semana: 4 (11/10/21 al 16/10/21)
Reactivos	Prueba con reactivos	ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS, GOBIERNO EN TECNOLOGÍA DE LA INFORMACIÓN	APORTE	5	Semana: 5 (18/10/21 al 23/10/21)
Resolución de ejercicios, casos y otros	Resolución de casos	EL CONTROL INTERNO INFORMATICO - COBIT, INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION	APORTE	5	Semana: 9 (15/11/21 al 17/11/21)
Reactivos	Prueba con reactivos	EL CONTROL INTERNO INFORMATICO - COBIT, INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION	APORTE	5	Semana: 10 (22/11/21 al 27/11/21)
Reactivos	Prueba con reactivos	METODOLOGÍA PARA REALIZAR LA AUDITORÍA DE SISTEMAS, SEGURIDAD DE INFORMACIÓN Y ERM (ENTERPRISE RISK MANAGEMENT)	APORTE	5	Semana: 14 (20/12/21 al 23/12/21)
Resolución de ejercicios, casos y otros	Resolución de casos	METODOLOGÍA PARA REALIZAR LA AUDITORÍA DE SISTEMAS, SEGURIDAD DE INFORMACIÓN Y ERM (ENTERPRISE RISK MANAGEMENT)	APORTE	5	Semana: 14 (20/12/21 al 23/12/21)
Reactivos	Examen con reactivos	ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS, EL CONTROL INTERNO INFORMATICO - COBIT,	EXAMEN	10	Semana: 19-20 (23-01-2022 al 29-01-2022)

Evidencia	Descripción	Contenidos sílabo a evaluar	Aporte	Calificación	Semana
		GOBIERNO EN TECNOLOGIA DE LA INFORMACIÓN, INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION, METODOLOGÍA PARA REALIZAR LA AUDITORÍA DE SISTEMAS, SEGURIDAD DE INFORMACIÓN Y ERM (ENTERPRISE RISK MANAGEMENT)			
Resolución de ejercicios, casos y otros	Resolución de un caso de auditoria	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	10	Semana: 19 (24/01/22 al 28/01/22)
Reactivos	Examen con 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	20	Semana: 21 (07/02/22 al 07/02/22)

### Metodología

La clase será impartida de manera magistral, y la aplicación de los conocimientos adquiridos se las realizará mediante estudios de casos. Al finalizar un tema se tomará una prueba con reactivos. En temas técnicos se realizarán trabajos mediante prácticas de laboratorio. En todos los trabajos se incluirá el siguiente párrafo al final: "POR MI ÉTICA Y POR MI HONOR, DECLARO QUE ESTE TRABAJO ES FRUTO DE MI PROPIO ESFUERZO".

### Criterios de Evaluación

Se tomarán lecciones con reactivos en la plataforma virtual y lecciones orales al final de cada tema o capítulo. De forma aleatoria, también se tomarán lecciones orales en clase.

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 con reactivos 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).

No se aceptarán trabajos extra temporáneos.

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
  - Creatividad
  - Control del tiempo asignado
  - Equilibrio del grupo (Participación de todos)
  - Manejo general de auditorio (manejo de preguntas y respuestas)
  - Utilización de apoyo visual
  - 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.
  - Durante y después de la exposición, los alumnos y el profesor podrán realizar preguntas a un miembro específico del grupo expositor sobre el contenido del caso
  - 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, márgenes superior e izquierdo de 3 cm. e inferior y derecho de 2 cm. y 1,5 de espacio entre líneas.
- En todos los trabajos se tomara 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	<a href="http://web.ebscohost.com/ehost/detail?vid=7&amp;hid=12&amp;sid=83bc99a6-b175-4870-9ab0-9a9bb232a099%">http://web.ebscohost.com/ehost/detail?vid=7&amp;hid=12&amp;sid=83bc99a6-b175-4870-9ab0-9a9bb232a099%</a>
Shahibi, Mohd. Sazili Fakeh, Shamsul Kamal	Security Factor And Trust In E-Commerce Transactions.	<a href="http://web.ebscohost.com/ehost/detail?vid=4&amp;hid=12&amp;sid=83bc99a6-b175-4870-9ab0-9a9bb232a099%">http://web.ebscohost.com/ehost/detail?vid=4&amp;hid=12&amp;sid=83bc99a6-b175-4870-9ab0-9a9bb232a099%</a>

#### Software

Autor	Título	Url	Versión
ACL	ACL		

### Bibliografía de apoyo

#### Libros

Autor	Título	Url	Versión
-------	--------	-----	---------

#### Software

Autor	Título	Url	Versión
-------	--------	-----	---------

Docente

Director/Junta

Fecha aprobación: 19/09/2021

Estado: Aprobado