UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN
ESCUELA CONTABILIDAD SUPERIOR

1. Datos

Materia: AUDITORÍA DE SISTEMAS Y TIC

Código: FAD0081

Paralelo: A

Periodo : Septiembre-2020 a Febrero-2021

Profesor: PINTADO ZUMBA PABLO FERNANDO

Correo electrónico: ppintado@uazuay.edu.ec

Prerrequisitos:

Código: FAD0041 Materia: AUDITORÍA DE GESTIÓN I

Nivel: 9

Distribución de horas.

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

2. Descripción y objetivos de la materia

Los objetivos que se persiguen en la enseñanza de Auditoria de Sistemas y TIC, se basan en el hecho de que los futuros Ingenieros en Contabilidad, alcancen un conocimiento general sobre los diversos tópicos de los sistemas de computación e informática que deben ser auditados al interior de las empresas y los principales marcos de trabajo aplicables a auditoria de sistemas de información. Logrando que estén capacitados para controlar, supervisar y administrar auditorias especializadas de sistemas.

El tratamiento de la Auditoria de Sistemas se inicia con una Introducción a los Principios de Gobierno de TI; Proceso de Auditoría de Sistemas basados en los marcos entregados por ISACA (Information System Audit and Control Association), permitiendo tener una visión clara del entorno Tecnológico Auditable; Marco de Gobierno Empresarial de TI Cobit 5, el mismo que permitirá conocer como la implementación de mejores practicas apoyan a la entrega de valor desde TI al Negocio; Infraestructura de TI y herramientas de auditoria como apoyo a la labor de los auditores.

La aplicación de la Auditoría de Sistemas se relaciona básicamente con las materias de: Auditoria de Gestión y Auditoria Financiera, que se consideran de vital importancia para el mejoramiento del ambiente de control dentro de las organizaciones.

3. Contenidos

1.	**GOBIERNO EN TECNOLOGÍA DE LA INFORMACIÓN**
1.1	Que es IT Governance?, responsabilidades del Gobierno TI (1 horas) (1 horas)
1.2	Evolución, Cambio e Innovación en la Organización de TI (1 horas) (1 horas)
1.3	Estrategias, Estándares y lineamientos de TI (1 horas) (1 horas)
1.4	Marco de Gobernabilidad de las TI (2 horas) (2 horas)
1.5	Herramientas, Procesos e Indicadores de TI (1 horas) (1 horas)
1.6	Estructura de la organización, roles y responsabilidades, relacionadas con el uso y la administración de TI (1 horas) (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 horas)
2.	**ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS**
2.1	Antecedentes, Definición y Conceptos de la Auditoría (1 horas) (1 horas)
2.2	Clasificación de los tipos de Auditoría (1 horas) (1 horas)
2.3	Auditoría Forense (1 horas) (1 horas)

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

4. Sistema de Evaluación

Resultado de aprendizaje de la carrera relacionados con la materia

Resultado de aprendizaje de la materia	Evidencias
ap. Evaluar los procesos de la empresa como auditor interno.	
-Conocer las principales fases de auditoria de sistemas de informaciónElaborar planes de auditoria basados en riesgosConocer los elementos fundamentales del marco de control interno COBITConocer y usar las características más importantes de una herramienta CAAT¿SConocer e identificar los elementos de infraestructura tecnológica como soporte a los procesos de negocioConocer los elementos fundamentales de Gobierno de TI	-Evaluación escrita -Evaluación oral -Trabajos prácticos - productos
aq. Revisar los estados financieros como auditor externo.	
-Ejecutar evaluaciones de controles a aplicaciones financierasElaborar matrices de riesgos de seguridad de información	-Evaluación escrita -Evaluación oral -Trabajos prácticos - productos

Desglose de evaluación

Evidencia	Descripción	Contenidos sílabo a evaluar	Aporte	Calificación	Semana
Trabajos prácticos - productos	trabajo practico	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)	APORTE DESEMPEÑO	5	Semana: 15 (02/01/21 al 02/01/21)
Evaluación escrita	evaluación escrita	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)	APORTE DESEMPEÑO	5	Semana: 15 (02/01/21 al 02/01/21)
Evaluación escrita	Examen supletorios asincrono	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 FINAL ASINCRÓNICO	10	Semana: 19 (25/01/21 al 30/01/21)
Evaluación escrita	examen suspensión	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 FINAL SINCRÓNICO	10	Semana: 19 (25/01/21 al 30/01/21)
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)	SUPLETORIO SINCRÓNICO	10	Semana: 19-20 (25-01-2021 al 30-01-2021)
Evaluación escrita	Examen final	ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS, EL CONTROL INTERNO INFORMATICO - COBIT, GOBIERNO EN TECNOLOGÍA DE	SUPLETORIO ASINCRÓNICO	10	Semana: 19-20 (25-01-2021 al 30-01-2021)

Evidencia	Descripción	Contenidos sílabo a evaluar	Aporte	Calificación	Semana
		LA INFORMACIÓN, INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION, METODOLOGÍA PARA REALIZAR LA AUDITORÍA DE SISTEMAS, SEGURIDAD DE INFORMACIÓN Y ERM (ENTERPRISE RISK MANAGEMENT)			

Metodología

Por esta ocasión especial, se tomará en cuenta la participación de los estudiantes en clase con su respectiva puntuación. 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
- 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
• 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

- 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) hasta la fecha y hora 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. Además, debe llevar en la portada los siguientes datos centrados:

UNIVERSIDAD DEL AZUAY
FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN
ESCUELA DE CONTABILIDAD SUPERIOR
AUDITORIA DE SISTEMAS Y TIC
TEMA O TRABAJO O CASO
NOMBRE DE LA PERSONA O GRUPO
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 porque 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.
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

5. Referencias

Bibliografía base

Libros

Autor	Editorial	Título	Año	ISBN

Autor	Editorial	Título	Año	ISBN
Instituto de auditores internos		Developing the IT Audit Plan	2008	
ISO		ISO/IEC 27002	2013	
ISACA		ITAF	2008	
CALDER, A., & WATKINS, S.	Kogan Page	IT GOVERNANCE A MANAGER'S GUIDE TO DATA SECURITY AND ISO 27001 / ISO 27002	2008	9780749452711
ISACA	ISACA	COBIT 5 EL MARCO	2013	9781604202823
ISO	ISO	ISO/IEC 27005	2008	NO INDICA
ISO	ISO	ISO/IEC 27001	2013	NO INDICA
ISO	ISO	ISO/IEC 31000	2009	NO INDICA
INSTITUTO DE AUDITORES INTERNOS	IIA	AUDITAR CONTROLES DE APLICACIONES	2007	NO INDICA
Pablo Pintado		Material de Apoyo de Auditoría de Sistemas y TIC `s	2019	

Web

Autor	Título	Url
ISACA	ISACA	https://www.isaca.org

Software

Autor	Título	Url	Versión
Caseware	Idea	NO INDICA	8.4

Bibliografía de apoyo

Libros

Autor	Editorial	Título	Año	ISBN
Pablo Pintado	Profesor	Material de Apoyo de Auditoría de Sistemas y TIC `s	2020	

Web

Software

Docente

Director/Junta

Fecha aprobación: 17/09/2020

Estado: Aprobado