



UNIVERSIDAD DE GUADALAJARA

CENTRO UNIVERSITARIO DE LA COSTA SUR

DIVISIÓN DE DESARROLLO REGIONAL

DEPARTAMENTO DE INGENIERÍAS

1. IDENTIFICACIÓN DEL CURSO

Nombre de la materia	
	Auditoria Informatica

Profesor(es)	
	José Guadalupe Alvarado Ornelas

Clave	NRC	Horas Teoría	Horas Práctica	Horas Totales	Créditos	Tipo de curso
IN255	54662	40	60	100	8	Curso-Taller

Flujo de materias	
Prerrequisito formal	Redes III
Prerrequisito recomendado	
Consecutiva recomendado	

Academia	TECNOLOGIA Y EDUCACION	
Historial de revisiones		
Acción	Fecha	Responsable
Evaluación	Junio 2023	José Guadalupe Alvarado Ornelas
Actualización	Junio 2024	José Guadalupe Alvarado Ornelas
Aprobación por la Academia		
Cargo	Nombre	Firma
Presidente		
Secretario		

Nivel	Clave	Descripción
I	AE1	Aplica los conocimientos de matemáticas, informática y fundamentos de ingeniería, así como conceptos avanzados en sistemas de información y comunicación digital, para identificar, analizar y resolver problemas específicos en el ámbito de la Ingeniería Teleinformática.
M		
A		
I	AE2	Identifica, analiza y resuelve problemas complejos de las áreas de sistemas de información y comunicación digital, aplicando conocimientos de ingeniería, matemática y ciencias básicas, además formula conclusiones fundamentadas en investigaciones y bibliografía especializada, considerando los principios integrales que promuevan el desarrollo sostenible.
M		
A		
I	AE3	





UNIVERSIDAD DE GUADALAJARA

CENTRO UNIVERSITARIO DE LA COSTA SUR

DIVISIÓN DE DESARROLLO REGIONAL

DEPARTAMENTO DE INGENIERÍAS

	M		Diseña, desarrolla y administra sistemas de información y comunicación digital resolviendo problemas complejos de ingeniería a partir de la integración de soluciones creativas para satisfacer las necesidades identificadas, considerando cuando sea necesario aspectos clave como la salud y la seguridad pública, la eficiencia en el costo del ciclo de vida, la sostenibilidad ambiental, así como los impactos culturales, sociales y ambientales asociados al uso y gestión de las tecnologías de la información.
	A		
	I	AE4	Reproduce ambientes simulados que facilitan la investigación de problemas complejos en las áreas de sistemas de información y comunicación digital utilizando métodos de investigación, diseño de experimentos y análisis e interpretación de datos, integrando conocimiento especializado para sintetizar información y obtener conclusiones fundamentadas y válidas.
	M		
	A		
	I	AE5	Crea, selecciona y aplica sistemas de información y comunicación digital reconociendo las limitaciones de estos recursos al aplicar métodos de predicción y modelización para abordar problemas complejos del área de la Ingeniería Teleinformática.
	M		
	A		
	I	AE6	Desarrolla ambientes simulados que permiten analizar e interpretar datos en sistemas de información y comunicación digital, evaluando los impactos sociales, económicos, legales, ambientales y de sostenibilidad, para proponer soluciones integrales a problemas complejos en el área de la Ingeniería Teleinformática.
	M		
	A		
	I	AE7	Practica su responsabilidad ética y profesional en los diferentes ámbitos de la Ingeniería en Teleinformática, considerando el impacto económico, social y ambiental de sus decisiones y cumpliendo con las leyes nacionales e internacionales pertinentes.
X	M		
	A		
	I	AE8	Se desempeña y trabaja efectivamente como individuo, miembro o líder en equipos diversos, inclusivos y multidisciplinarios, estableciendo metas, planeando tareas, y analizando riesgos e incertidumbres en entornos presenciales, remotos o distribuidos.
X	M		
	A		
	I	AE9	Se comunica de manera efectiva e inclusiva, tanto de manera oral como escrita, adaptándose al tipo de audiencia. Además, tiene la capacidad de redactar informes y documentación técnica de manera clara y comprensible.
	M		
	A		
	I	AE10	Aplica los conocimientos y principios de la gestión y la toma de decisiones al desarrollar y/o gestionar proyectos de manera individual o como líder de un equipo en entornos multidisciplinarios.
	M		
	A		
	I	AE11	Reconoce la necesidad de aprendizaje continuo e independiente durante toda la vida, demostrando capacidad para localizar, evaluar, integrar y aplicar conocimiento de su área profesional de manera adecuada, así como para adaptarse a las tecnologías nuevas y emergentes.
X	M		
	A		

2. PRESENTACIÓN

Descripción

Este curso está diseñado para proporcionar a los estudiantes los conocimientos y habilidades necesarios para evaluar la seguridad, integridad y eficiencia de los sistemas de información en una organización. A lo largo del curso, se explorarán metodologías, herramientas y técnicas para realizar auditorías efectivas, identificar vulnerabilidades y proponer mejoras. Se enfocará en áreas clave como seguridad informática, cumplimiento normativo, gestión de riesgos y continuidad del negocio. Los estudiantes aplicarán estos conceptos en un proyecto práctico, simulando auditorías reales en entornos empresariales.





UNIVERSIDAD DE GUADALAJARA

CENTRO UNIVERSITARIO DE LA COSTA SUR

DIVISIÓN DE DESARROLLO REGIONAL

DEPARTAMENTO DE INGENIERÍAS

3. OBJETIVO

General

Formar profesionales capaces de planificar, ejecutar y evaluar auditorías informáticas mediante el uso de metodologías, herramientas y técnicas especializadas, para garantizar la seguridad, eficiencia y cumplimiento normativo de los sistemas de información, contribuyendo a la mejora continua de los procesos tecnológicos en las organizaciones.

- Desarrollar habilidades para identificar y analizar riesgos en los sistemas de información, evaluando su impacto en la seguridad y operatividad de la organización.
- Aplicar herramientas y técnicas de auditoría informática para revisar la infraestructura tecnológica, las políticas de seguridad y los procedimientos operativos.
- Evaluar el cumplimiento normativo y regulaciones vigentes en relación con la gestión de la tecnología de la información.
- Diseñar planes de mejora y mitigación de riesgos basados en los hallazgos obtenidos durante el proceso de auditoría.
- Promover la implementación de buenas prácticas en la gestión de TI, garantizando la integridad, disponibilidad y confidencialidad de la información empresarial.

4. CONTENIDO

Temas y subtemas

1. Introducción a la auditoría informática

- 1.1. Definición y objetivos: Comprender qué es una auditoría informática y sus principales objetivos.
- 1.2. Tipos de auditorías: Auditoría interna, externa, de sistemas, de seguridad, entre otras.
- 1.3. Normativas y estándares: Introducción a los principales marcos regulatorios y estándares, como ISO 27001, COBIT, y NIST.

2. Planificación y Organización de la Auditoría

- 2.1. Metodologías de auditoría: Ciclo de vida de una auditoría (planificación, ejecución, reporte).
- 2.2. Planificación de la auditoría: Definición de objetivos, alcance, y recursos.
- 2.3. Evaluación de riesgos: Identificación y valoración de riesgos en sistemas de información.

3. Auditoría de Redes de Computadoras

- 3.1. Evaluación de la arquitectura de red: Revisar la configuración y seguridad de las redes.
- 3.2. Herramientas de auditoría de redes: Uso de herramientas como Wireshark, Nmap, y Nessus.
- 3.3. Detección de vulnerabilidades y pruebas de penetración: Identificación de fallos de seguridad y pruebas de penetración

4. Auditoría de Seguridad Informática.

- 4.1. Revisión de políticas de seguridad: Evaluación de la implementación de políticas y procedimientos de seguridad.
- 4.2. Auditoría de control de acceso: Verificación de la gestión de usuarios, contraseñas, y accesos.
- 4.3. Análisis de incidentes de seguridad: Revisión de logs y eventos de seguridad para detectar y analizar incidentes.

5. Auditoría de Sistemas Operativos y Aplicaciones

- 5.1. Evaluación de la seguridad del sistema operativo: Análisis de configuraciones y permisos en sistemas como Windows y Linux.





UNIVERSIDAD DE GUADALAJARA

CENTRO UNIVERSITARIO DE LA COSTA SUR

DIVISIÓN DE DESARROLLO REGIONAL

DEPARTAMENTO DE INGENIERÍAS

5.2. Auditoría de aplicaciones: Evaluación de la seguridad en aplicaciones empresariales, incluyendo pruebas de caja blanca y negra.

5.3. Gestión de parches y actualizaciones: Revisión de la política y práctica de actualización de software.

6. Auditoría de Bases de Datos.

6.1. Revisión de la integridad de datos: Evaluación de la calidad y consistencia de la información en las bases de datos.

6.2. Auditoría de acceso a bases de datos: Análisis de permisos y accesos a los sistemas de gestión de bases de datos, encriptación de datos, y copias de seguridad.

6.3. Herramientas de auditoría de bases de datos: Uso de herramientas como SQL Server Audit, Oracle Audit Vault

7. Evaluación de Controles Internos y Cumplimiento.

7.1. Análisis de controles internos: Evaluación de la efectividad de los controles implementados en la organización.

7.2. Cumplimiento normativo: Verificación del cumplimiento de regulaciones y normativas aplicables.

7.3. Informe de hallazgos y recomendaciones: Cómo redactar y presentar un informe de auditoría.

8. Herramientas de Auditoría Informática.

8.1. Uso de herramientas automatizadas: Introducción a software de auditoría como ACL, IDEA, y otros.

8.2. Auditoría continua y monitoreo: Implementación de auditoría continua usando herramientas de monitoreo y herramientas de análisis de logs.

9. Estudios de Caso y Prácticas de Auditoría.

9.1. Análisis de casos reales: Revisión de auditorías informáticas famosas y sus resultados.

9.2. Simulación de auditoría: Realización de una auditoría completa sobre un entorno controlado.

9.3. Presentación de resultados: Elaboración y presentación de un informe de auditoría basado en la simulación.

10. Tendencias y Futuro de la Auditoría Informática

10.1. Impacto de las tecnologías emergentes: Auditoría en entornos de computación en la nube, IoT, y blockchain.

10.2. Automatización y Auditoría con IA: Uso de inteligencia artificial y automatización en auditorías.

10.3. El rol del auditor en la era digital: Nuevos desafíos y habilidades requeridas para los auditores informáticos.

Prácticas

1.-	Evaluación de Políticas de Seguridad: Análisis de Cumplimiento y Gaps
2.-	Identificación de Vulnerabilidades en Infraestructura de TI mediante Escáneres de Seguridad
3.-	Pruebas de Penetración Controladas: Simulación de Ataques Externos e Internos
4.-	Auditoría de Accesos: Verificación de Registros y Políticas de Control de Usuarios
5.-	Revisión de Copias de Seguridad: Procedimientos y Recuperación de Datos
6.-	Análisis de Logs del Sistema: Identificación de Incidentes y Actividades Sospechosas
7.-	Auditoría Física de Centros de Datos: Seguridad Perimetral y Acceso Restringido
8.-	Evaluación de Cumplimiento Normativo: Auditoría Basada en ISO/IEC 27001
9.-	Gestión de Riesgos: Identificación y Priorización de Amenazas en TI
10.-	Creación de un Informe de Auditoría: Redacción de Hallazgos y Recomendaciones

5. EVALUACIÓN

Ponderación de unidad de competencia para calificación

Exposición de temas	Porcentaje
Tareas e investigaciones	30%
Prácticas	30%
Proyecto Final	40%



Av. Independencia nacional No. 151, Col. Centro C.P. 48900

Autlán de Navarro, Jalisco. México Tel. (317) 382 5010

www.cucsur.udg.mx



UNIVERSIDAD DE GUADALAJARA

CENTRO UNIVERSITARIO DE LA COSTA SUR

DIVISIÓN DE DESARROLLO REGIONAL

DEPARTAMENTO DE INGENIERÍAS

6. CRITERIOS Y MECANISMOS PARA LA ACREDITACIÓN

Descripción

De conformidad a lo que establece el Capítulo IV en los artículos 19 al 22 y Capítulo V en los artículos 23 al 29 del Reglamento General de Evaluación y Promoción de la Universidad de Guadalajara.

7. BIBLIOGRAFÍA

Básica

Autores	Título	Editorial	Año	Clasificación de Biblioteca
Julio César Mateus Santamaría	<i>Control y Auditoría de Sistemas de Información.</i>	Paraninfo	2009	
Marcos Báez y Rafael Pastor	<i>Auditoría y Control Interno de los Sistemas de Información.</i>	Centro de Formación de Ingeniería de Sistemas Informáticos (CFISI)	2016	

Complementaria

Autores	Título	Editorial	Año	Otra información
Greg Shields	Auditing: The Ultimate Guide to Performing Internal and External Audits	Independently Published	2024	

