4142 - AUDITORÍA Y SEGURIDAD INFORMÁTICA

I - Datos de identificación de la asignatura

Carrera:	Licenciatura en Análisis de Sistemas		
Código:	4142	**Plan:**	2024
Denominación:	Auditoría y seguridad informática		
Área:	Énfasis propio de la carrera		
Año:	Cuarto		
Horas con acompañamiento docente (HTD), semanal			4
Horas de Trabajo Independiente del estudiante (HTI), semanal			5
Horas semanales (HS)			9
Cantidad de sesiones			32
Total Horas de Trabajo con el docente (THTD)			128
THD teóricas	128	**THD prácticas**	0
Total de Horas de Trabajo Independiente del estudiante (THTI)			160
Total Horas Académicas (THA)			288
Crédito académico (CA)			11,5
Pre-requisito:	-		

II - Fundamentación

La asignatura tiene como objetivo principal abordar las prácticas asociadas con la garantía de operaciones comerciales seguras en el contexto de los adversarios. Se centra en la creación, operación, defensa, análisis y prueba de sistemas informáticos seguros para asegurar operaciones seguras en las organizaciones.

La informática segura es un campo interdisciplinario que abarca aspectos de informática, leyes, políticas, factores humanos, ética y gestión de riesgos. En esta asignatura, se abordarán competencias relacionadas con la seguridad de los datos, la seguridad del software, la seguridad humana, la seguridad social y la seguridad de la organización. Estas competencias se explorarán desde la perspectiva de los sistemas de información, considerando la importancia de garantizar que la información cumpla con los objetivos y demandas de los usuarios, tanto para la toma de decisiones como para el seguimiento de actividades.

Los temas tratados en la asignatura buscan mostrar la importancia del control y la evaluación de las diferentes áreas que componen los sistemas informáticos. Se introducirá una perspectiva general de la auditoría clásica y se adaptará esta función para abordar el control de las nuevas tecnologías de la información. Se explorarán estándares, políticas y procedimientos establecidos para respaldar la seguridad informática.

La naturaleza de la asignatura es teórico-práctica, lo que significa que los estudiantes tendrán la oportunidad de aplicar los conocimientos y técnicas adquiridas a través de casos prácticos reales. Estos casos prácticos permitirán reforzar los conceptos teóricos y desarrollar habilidades prácticas en la auditoría y seguridad informática.

Al finalizar la asignatura, los estudiantes estarán preparados para abordar los desafíos relacionados con la garantía de operaciones seguras en los sistemas informáticos. Tendrán una comprensión integral de los aspectos clave de la auditoría y la seguridad informática,

así como la capacidad de aplicar herramientas y técnicas para evaluar y mejorar la seguridad de los sistemas de información en las organizaciones.

III - Competencias a desarrollar

Competencias genéricas

1. Aplicar las tecnologías de la información y comunicación de manera efectiva.
2. Ajustar su conducta a las normas éticas universalmente establecidas.
3. Asumir el compromiso y la responsabilidad social en las actividades emprendidas hacia la búsqueda del mejoramiento de la calidad de vida.
4. Actuar de conformidad a los principios de prevención, higiene y seguridad en el trabajo.
5. Conocer y saber aplicar técnicas y herramientas actualizadas en sus áreas de competencia.
6. Conocer y aplicar el marco normativo y legal inherente a sus áreas de competencia.
7. Asimilar los cambios tecnológicos y sociales emergentes.

Competencias específicas

1. Aplicar de forma efectiva técnicas de transmisión segura de información, utilizando cifrado, firmas digitales, VPN y otros mecanismos, para proteger la confidencialidad, integridad y disponibilidad de los datos en una organización.
2. Comprender y explicar con claridad los principios y aplicaciones de la criptografía, describiendo algoritmos, modos de cifrado y gestión de claves, para asegurar la información durante su almacenamiento y transmisión.
3. Describir y aplicar adecuadamente mecanismos de autenticación, autorización, control de acceso e integridad de datos, para garantizar la identificación segura de usuarios y proteger los recursos de información ante accesos no autorizados.
4. Identificar e incorporar con criterio técnico los requisitos de seguridad en el diseño de software, abordando la gestión de contraseñas, sesiones seguras y prevención de vulnerabilidades como inyección de código, para fortalecer la seguridad desde el desarrollo.
5. Aplicar principios de diseño seguro desde las primeras etapas del desarrollo de sistemas informáticos, identificando riesgos potenciales, seleccionando controles de seguridad y evaluando su impacto, para construir sistemas robustos y confiables.
6. Analizar y aplicar medidas de protección de acceso en entornos informáticos, empleando autenticación de múltiples factores, certificados digitales y políticas de acceso, para resguardar personas, dispositivos y datos frente a amenazas externas.
7. Evaluar con sentido crítico los riesgos de privacidad en redes sociales, analizando la exposición de datos personales y aplicando medidas de protección adecuadas, para preservar la seguridad de la información en plataformas digitales abiertas.
8. Identificar y explicar los principales tipos de ciberataques (malware, phishing, ransomware, DDoS), describiendo técnicas de prevención y contramedidas, para mitigar los riesgos de ataques maliciosos en entornos organizacionales.

9. Aplicar metodologías de gestión de riesgos, identificando, evaluando y priorizando amenazas sobre los activos de información, para diseñar estrategias de seguridad basadas en criterios objetivos y decisiones informadas.
10. Reconocer e interpretar los marcos legales, normativas y estándares de seguridad informática, para asegurar el cumplimiento regulatorio y alinear las políticas organizacionales con buenas prácticas internacionales.
11. Realizar auditorías de sistemas informáticos, evaluando la seguridad, detectando vulnerabilidades, revisando procedimientos y elaborando informes técnicos, para verificar la eficacia de los controles implementados y proponer mejoras preventivas y correctivas.

IV - Cuerpo de conocimientos

Unidad 1: Auditoria Informática
Contenidos:

- Concepto de auditoría. Origen y desarrollo. Clasificación. Objetivos. Alcance.
- Perfil del auditor informático
- Metodologías de control y auditoría de sistemas de información
- Etapas para el desarrollo de una auditoria: Planeación, ejecución y dictamen de la auditoria de sistemas computacionales
- Modelos de informes de auditoria
- Confirmación de la documentación de la auditoria informática
- Informe Final de la Auditoria Informática
- Dictamen Final de la Auditoria Informática

Unidad 2: Leyes, regulaciones y estándares de seguridad
Contenidos:

- Importancia de las leyes, regulaciones y estándares de seguridad
- Marco legal y regulaciones relevantes
- Estándares de seguridad: ISO/IEC 27001, NIST, COBIT, PCI DSS, entre otros.
- Implementación de políticas y procedimientos de seguridad.

Unidad 3: Técnicas para transmitir y asegurar la información en una organización
Contenidos:

- Amenazas a la seguridad de la información
- Tecnologías y soluciones de seguridad.
- Políticas de backup.
- Amenazas a la privacidad de la información.
- Consecuencias de las violaciones de la privacidad de la información.
- Componentes clave de las redes.
- Métodos para transmitir información usando redes (incluyendo comunicación, aplicaciones Web 2.0 y Web 3.0, IoT, crowdsourcing).
- Tecnologías y soluciones para la privacidad de la información.
- Prácticas justas de información y políticas de privacidad.
- Regulaciones gubernamentales de privacidad de la información.

Unidad 4: Requisitos de seguridad importantes durante el diseño de software
Contenidos:

- Seguridad por diseño
- Sanitización de datos
- Validación de entrada y saneamiento de datos
- Vulnerabilidad de seguridad

Unidad 5: Diseño inicial para la seguridad del sistema

Contenidos:

- Suposición de casos extremos y vulnerabilidades
- Técnicas de código para la seguridad
- Técnicas de implementación para la seguridad
- Mantenimiento actualizado del entorno de implementación:
- Mantenimiento actualizado de las dependencias del software
- Relación entre deuda técnica y diseño de valores

Unidad 6: Criptografía y comunicaciones de datos

Contenidos:

- Transmisión de datos
- Criptografía

Unidad 7: Importancia de la privacidad y seguridad en las redes sociales

Contenidos:

- Compensaciones y riesgos de privacidad en el contexto social
- Contexto organizacional

Unidad 8: Ciberataques

Contenidos:

- Tipos de ciberataques
- Anatomía de los ciberataques
- Mecanismos de mitigación de ciberataques

Unidad 9: Gestión de riesgos

Contenidos:

- Identificar y priorizar los factores de riesgo
- Técnicas de gestión de riesgos
- Amenazas potenciales, vulnerabilidades y riesgos asociados con un sistema de tecnología de la información
- Controles para reducir o eliminar el riesgo
- Gestión de riesgos: identificación y evaluación de riesgos
- Mitigación de riesgos: pasos para reducir el riesgo a un nivel aceptable

Unidad 10: Autenticación, autorización, control de acceso e integridad de datos en el contexto de la comunicación de datos

Contenidos:

- Autenticación: Métodos y técnicas utilizados para verificar la identidad de los usuarios y dispositivos en el proceso de comunicación de datos.
- Autorización: Mecanismos utilizados para otorgar o denegar acceso a recursos y servicios basados en la identidad verificada.
- Control de acceso: Técnicas y herramientas utilizadas para controlar y gestionar el acceso a los datos y recursos en un entorno de comunicación.
- Integridad de los datos: Métodos y técnicas utilizados para garantizar la integridad de los datos durante su transmisión y almacenamiento.

Unidad 11: Identificación, autenticación y autorización de acceso en el contexto de la protección de personas y dispositivos

Contenidos:

- Identificación: Métodos y técnicas utilizados para identificar de manera única a las personas y los dispositivos en un entorno de seguridad.
- Autenticación: Exploración de los mecanismos de autenticación utilizados para verificar la identidad de las personas y los dispositivos.
- Autorización de acceso: Análisis de los procesos y políticas utilizados para otorgar o denegar acceso a recursos y servicios basados en la identidad y autenticación de los usuarios y dispositivos.

– Pistas de auditoría y registros: Estudio de la importancia de registrar y auditar las actividades de acceso en un sistema de seguridad.

V - Estrategias didácticas a ser implementadas en el proceso de enseñanza aprendizaje. (abarcando actividades de formación e investigación)

Utilizar metodología que promueva la integración de la teoría y la práctica, así como la activa participación de los alumnos durante el desarrollo de las clases. El docente deberá planificar y desarrollar estrategias didácticas que permita al alumno aplicar en forma permanente los conocimientos.

Las competencias se adquirirán preferentemente a través de:

- Clase magistral.
- Resolución de problemas.
- Proyecto áulico.
- Trabajo colaborativo.

Se dispondrá de un espacio virtual de la asignatura en la plataforma virtual para el intercambio de información con los alumnos (apuntes, ejercicios, etc.) y como medio de comunicación (foros, chats, etc.). Las entregas de trabajos también se realizarán mediante esta plataforma.

VI - Estrategias de evaluación.

La evaluación será formativa y procesual, se realizará a través de pruebas (exámenes) que podrán ser escritas, orales o de ejecución que a su vez podrá ser mediante trabajos individuales o grupales. La materia consta de dos pruebas parciales, con un recuperatorio y tres oportunidades para la prueba final.

En estos parciales, así como en el examen final, se evaluarán las competencias alcanzadas a través de actividades de contenido teórico y práctico que permitan dar cuenta del avance conceptual en los temas que se han desarrollado, se incorporan preguntas específicas tipo sobre “donde cree Ud. que es aplicable este conocimiento/método” y se refleja en la corrección de las pruebas del alumno.

En algunos temas se trabaja también con ejercitaciones de aplicación en clase, que requieren de un ejercicio de integración de conceptos y que complementan la evaluación a través de los parciales.

Para la obtención de calificaciones parciales y finales se tendrá en cuenta el Reglamento Académico de la universidad.

VII - Actividades de extensión y de responsabilidad social universitaria.

Rige de acuerdo al reglamento de la Universidad y el reglamento interno de la facultad.

VIII - Fuentes bibliográficas

Básica

- Piattini Velthuis, M. G. & Del Peso Navarro, E. (2000). Auditoría Informática: un enfoque práctico. Editorial RA-MA S.A.
- Muñoz Razo, Carlos. (2002). Auditoria en Sistemas Computacionales. PEARSON EDUCACIÓN, México

- Llamas Covarrubias, J. Z. & Llamas Covarrubias, I. N. (2018). Internet, ¿Arma o Herramienta?
- Romero Castro, M. I. & Figueroa Morán, G. L. (2018). Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades.

Complementaria

- De Pablos Heredero, C. et.al. (2ª Ed.). Dirección y gestión de los sistemas de información de la empresa. ESIC Editorial: Madrid.