UNIVERSIDAD AUTÓNOMA DE CHIHUAHUA	**DES:**	**INGENIERÍA**
	Programa académico	Ingeniería en Computación
	Tipo de materia (Obli/Opta):	Optativa
	Clave de la materia:	OPCO805
	Semestre:	Octavo
	Área en plan de estudios:	Específica
	Total de horas por semana:	6
	Teoría: Presencial o Virtual	0
	Laboratorio o Taller:	4
	Prácticas:	0
	Trabajo extra-clase:	2
	Créditos Totales:	6
UNIDAD ACADÉMICA: FACULTAD DE INGENIERÍA	**Total de horas semestre (x sem):**	96
PROGRAMA ANALÍTICO DE LA UNIDAD DE APRENDIZAJE:	Fecha de actualización:	Febrero 2024.
SEGURIDAD INFORMÁTICA Y TELECOMUNICACIONES	*Prerrequisito (s):*	CO401 Sistemas Operativos

DESCRIPCIÓN:

El alumno comprenderá y utilizará los métodos y elementos que le permitan realizar auditorías de seguridad informática a equipos y a infraestructura de telecomunicaciones.

COMPETENCIAS PARA DESARROLLAR:

B4. Transformación Digital Transforma la cultura digital en la sociedad, en las organizaciones e instituciones educativas para aprovechar al máximo el potencial de las tecnologías y herramientas digitales; propiciar su uso responsable y ético que estimule la creatividad, innovación, la comunicación efectiva y el trabajo colaborativo e interdisciplinar en la solución de problemas de la sociedad digital; promoviendo la privacidad y la seguridad, así como el respeto a los derechos de autor y la propiedad intelectual.

P2. Desarrollo de proyectos de ingeniería: Desarrolla proyectos de ingeniería complejos en sus etapas de planeación, análisis y diseño, utilizando las tecnologías y los principios de la administración para la optimización de los recursos con base en procesos de calidad, mejora continua y teniendo en cuenta la seguridad, el costo del ciclo de vida, el carbono neto cero y la salud según sea necesario, atendiendo las necesidades de sostenibilidad.

E2. Gestión de infraestructura tecnológica: Realizar el análisis, diseño, gestión de infraestructura tecnológica, aplicando conocimientos avanzados en sistemas operativos, redes de dispositivos electrónicos, administración de infraestructura tecnológica y seguridad informática. Se centra en garantizar la eficiencia, seguridad y escalabilidad, requiriendo un enfoque analítico para identificar y solucionar problemas complejos en infraestructuras de TI.

DOMINIOS	OBJETOS DE ESTUDIO	RESULTADOS DE APRENDIZAJE	METODOLOGÍA	EVIDENCIAS
B4.1 Desarrolla habilidades digitales de forma crítica que impacten positivamente en la vida cotidiana y en las organizaciones e instituciones para la comunicación efectiva en entornos digitales. **E2. Gestión de infraestructura tecnológica** Administrar sistemas operativos y servidores, garantizando su funcionamiento eficiente y seguro en entornos económicos. Diseñar y gestionar infraestructuras de redes complejas, asegurando su escalabilidad, eficiencia y seguridad. Implementar y mantener protocolos de seguridad informática para proteger datos y sistemas contra amenazas cibernéticas.	**Objeto de estudio 1: Seguridad de la información en la red** 1.1 Auditorías de seguridad en sistemas en red. 1.2 Identificación de vulnerabilidades. 1.3 Evaluación de controles de seguridad en red. 1.4 Planificación de la auditoría de seguridad informática.	Reconoce los conceptos de seguridad informática, amenazas y objetivos de las normas aplicadas al área. Reporta elementos que describen la evolución de la seguridad informática.	Encuadre. Aprendizaje interactivo. Investigación de tópicos con preguntas guía. Instalación de sistema operativo para modificación, configuración y prácticas de servicios de seguridad informática.	Informe por escrito describiendo el origen y evolución de los sistemas de seguridad informática basadas en las normas ISO 17799 e ISO15408 Contextualización de la información obtenida en un adecuado marco de referencia. Presentaciones.

E2. Gestión de infraestructura tecnológica Diseñar y gestionar infraestructuras de redes complejas, asegurando su escalabilidad, eficiencia y seguridad. Implementar y mantener protocolos de seguridad informática para proteger datos y sistemas contra amenazas cibernéticas.	**Objeto de estudio 2: Políticas de seguridad informática.** 2.1 Políticas de buenas prácticas informáticas. 2.2 Políticas de riesgos informáticos. 2.3 Elementos que conforman una política de seguridad informática. 2.4 Cumplimiento de regulaciones y leyes.	Reconoce el flujo y estados de los servicios de seguridad informática para la planificación en un sistema informático.	Aprendizaje interactivo. Técnica expositiva por parte de los estudiantes. Trabajo colaborativo. Trabajo individual en solución de ejercicios vía configuración o desarrollo de programas. Discusión dirigida	Contextualización de la información obtenida en un adecuado marco de referencia. Reportes técnicos producto de simulaciones de diferentes facilidades de los servicios de seguridad informática. Presentaciones.
P2. Desarrollo de proyectos de ingeniería Identifica los principales factores involucrados en la solución de problemas de ingeniería para desarrollar propuestas utilizando herramientas de ciencias básicas e ingeniería aplicada. Implementar y/o administrar soluciones de cómputo basados en la nube, utilizando diferentes arquitecturas de software e introducirlo al mundo del gobierno de la	**Objeto de estudio 3:** **Análisis de seguridad de la red y análisis de riesgos.** 3.1 Firewall 3.2 Sistemas de Control de Acceso a la Red (NAC). 3.3 Sistemas de Detección y Prevención de Intrusiones (IDPS). 3.4 Redes Privadas Virtuales (VPN).	Reconoce el flujo y estados de las amenazas informáticas	Aprendizaje interactivo. Técnica expositiva por parte de los estudiantes. Trabajo colaborativo. Trabajo individual en solución de ejercicios vía configuración o desarrollo de programas. Discusión dirigida	Contextualización de la información obtenida en un adecuado marco de referencia. Reportes técnicos producto de simulaciones de diferentes facilidades de los servicios de seguridad informática. Presentaciones.

infraestructura tecnológica.				
P2. Desarrollo de proyectos de ingeniería Identifica los principales factores involucrados en la solución de problemas de ingeniería para desarrollar propuestas utilizando herramientas de ciencias básicas e ingeniería aplicada. Diseñar y gestionar infraestructuras de redes complejas, asegurando su escalabilidad, eficiencia y seguridad. Implementar y mantener protocolos de seguridad informática para proteger datos y sistemas contra amenazas cibernéticas.	**Objeto de estudio 4: Herramientas para realizar auditorías de seguridad informática.** 4.1 Sistemas detectores de intrusiones (IDS) 4.2 Seguridad en gestión de redes (SNMP)	Reconoce el flujo y estados de las técnicas de intrusión y ataques informáticos	Aprendizaje interactivo. Técnica expositiva por parte de los estudiantes. Trabajo colaborativo. Trabajo individual en solución de ejercicios vía configuración o desarrollo de programas. Discusión dirigida	Contextualización de la información obtenida en un adecuado marco de referencia. Reportes técnicos producto de simulaciones de diferentes facilidades de los servicios de seguridad informática. Presentaciones.

FUENTES DE INFORMACIÓN (Bibliografía, direcciones electrónicas)	**EVALUACIÓN DE LOS APRENDIZAJES** (Criterios, ponderación e instrumentos)
Stallings, William (2004). Fundamentos de seguridad en redes. Aplicaciones y estándares. Segunda edición. España: Pearson Prentice Hall. ISBN: 84-205-4002-1 https://books.google.com.cu/books?id=cjsHVSwbHwoC&printsec=frontcover#v=onepage&q&f=false Firtman, Sebastian (2005). Seguridad Informatica, Manuales USERS: Las amenazas y vulnerabilidades mas peligrosas al desnudo (Spanish Edition). M.P. Ediciones. ISBN 10: 9875263133. ISBN 13: 9789875263130 https://www.everand.com/book/503723747/Fundamentos-de-Seguridad-de-la-Red La seguridad de las telecomunicaciones y las tecnologías de la información. Visión general de asuntos relacionados con la seguridad de las telecomunicaciones y la implementación de las Recomendaciones UIT-T existentes. 2006. UIT-T – Oficina de Normalización de las Telecomunicaciones (TSB) Place des Nations – CH-1211 Ginebra 20 – Suiza E-mail: tsbmail@itu.int Web: www.itu.int/ITU-T García Teodoro, Pedro (2020). Seguridad en Redes y Sistemas de Comunicación. Teoría y Práctica. Universidad de Granada. ISBN: 9798605091257 McClure, Stuart / Scambray, Joel / Kurtz, George (2005). Hackers 4. Secretos y Soluciones para la Seguridad de Redes. Mc Graw Hill. IBN: 8448139798, 978-8448139797	El curso se evalúa en 3 momentos, las fechas se establecen por la secretaría académica: ● Examen escrito. ● Informes escritos. ● Presentaciones. Conocimientos: 55% (aspectos teóricos) Habilidades: 35% (análisis, argumentación, redacción, uso de tecnología, comunicación, efectiva, , resolución de ejercicios con aplicación metodológica). Valores y actitudes: 10% (colaboración, orden, lenguaje apropiado, respeto, puntualidad). CRITERIOS DE DESEMPEÑO: Los informes por escrito: valoran el nivel de argumentación en relación al hecho que se quiere demostrar. Manejo de lenguaje técnico, coherencia entre párrafos y global, redacción, ortografía y presentación. Se utiliza una rúbrica para evaluación. LAS ACTIVIDADES NO REALIZADAS EN TIEMPO Y FORMA SE CALIFICAN CON CERO. **La calificación mínima aprobatoria será de 7.0** **Las actividades asignadas, así como tareas deben presentar rubricas y/o listas de cotejo.**

CRONOGRAMA

Objetos de estudio	**Semanas**															
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
Introducción a la seguridad																
Servicios de Seguridad																
Amenazas																
Identificación de ataques y técnicas de intrusión																