UNIVERSIDAD AUTÓNOMA DE CHIHUAHUA **UNIDAD ACADÉMICA:** **FACULTAD DE INGENIERÍA** **PROGRAMA ANALÍTICO DE** **LA UNIDAD DE APRENDIZAJE:** **FUNDAMENTOS DE CIBERSEGURIDAD**	**DES:**	**INGENIERÍA**
	Programa académico	Ingeniería en Computación
	Tipo de materia (Obli/Opta):	Obligatoria
	Clave de la materia:	CO603
	Semestre:	Sexto
	Área en plan de estudios:	Específica
	Total de horas por semana:	4
	Teoría: Presencial o Virtual	0
	Laboratorio o Taller:	4
	Prácticas:	0
	Trabajo extra-clase:	0
	Créditos Totales:	4
	Total de horas semestre (x sem):	64
	Fecha de actualización:	Octubre 2024
	Prerrequisito (s):	CO401 Sistemas Operativos

DESCRIPCIÓN:

El alumno comprenderá y utilizará los métodos y elementos que le permitan organizar el desarrollo de una arquitectura de seguridad, con base en la identificación y análisis de amenazas, ataques y vulnerabilidades en los sistemas y en las redes de cómputo.

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
B4.4 Analiza los desafíos éticos en la era digital y promueve el uso seguro y responsable de la tecnología; toma en cuenta la protección de datos personales en el entorno digital. **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	**Objeto de estudio 1 Introducción a la seguridad** 1.1 Concepto de la seguridad informática 1.2 Objetivos y misión de Seguridad informática 1.3 Amenazas a los sistemas y redes 1.4 Normas de Seguridad 1.4.1 ISO 17799 1.4.2.ISO 15408	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.

y mantener protocolos de seguridad informática para proteger datos y sistemas contra amenazas cibernéticas.				
E2. Gestión de infraestructura tecnológica. Diseñar y gestionar infraestructuras de redes complejas, asegurando su escalabilidad, eficiencia y seguridad. Implementar y mantener protocolos de seguridad	**Objeto de estudio 2 Servicios de Seguridad** 2.1 Confidencialidad 2.2 Autenticación 2.3 Integridad 2.4 No repudio 2.5 Control de Acceso 2.6 Disponibilidad	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	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.

informática para proteger datos y sistemas contra amenazas cibernéticas.			desarrollo de programas. Discusión dirigida	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 mundodel gobierno de la infraestructura tecnológica.	**Objeto de estudio 3 Amenazas** 3.1 Definición 3.2. Fuetes de Amenaza de tipo internos 3.3. Fuetes de Amenaza de tipo externo 3.4 Vulnerabilidades 3.4.1 Física 3.4.2 Natural 3.4.3 Hardware 3.4.4 Software	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.
P2. Desarrollo de proyectos de ingeniería Identifica los	**Objeto de estudio 4 Identificación de ataques y técnicas de intrusión**	Reconoce el flujo y estados de las técnicas de	Aprendizaje interactivo. Técnica expositiva	Contextualización de la información obtenida en un adecuado marco

principales factores involucrados en la solución de problemas de ingeniería para desarrollar propuestas utilizando herramientas de ciencias básicas e ingeniería aplicada.	4.1 Identifica y Explotación de la Información 4.1.1 Bases de Datos Públicas 4.1.2 WEB 4.1.3 DNS 4.1.4 Keyloggers 4.1.5 Ingeniería Social 4.1.6 SQL Injection 4.1.7 Virus y Gusanos	intrusión y ataques informáticos	por parte de los estudiantes. Trabajo colaborativo. Trabajo individual en solución de ejercicios vía configuración o desarrollo de programas. Discusión dirigida	de referencia. Reportes técnicos producto de simulaciones de diferentes facilidades de los servicios de seguridad informática. Presentaciones.
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.				

FUENTES DE INFORMACIÓN (Bibliografía, direcciones electrónicas)	**EVALUACIÓN DE LOS APRENDIZAJES** (Criterios, ponderación e instrumentos)
● Abad Parrales, W. M., Cañarte Rodríguez, T. C., Villamarin Cevallos, M. E., Mezones Santana, H. L., Delgado Pilozo, Á. R., Toala Arias, F. J., Figueroa Suárez, J. A., & Romero Castro, V. F. (2019). La ciberseguridad práctica aplicada a las redes, servidores y navegadores web (Vol. 59 de Ingeniería y Tecnología). 3Ciencias. ISBN 978-84-121167-6-2. ● Bhusan, M., Rathore, R. S., & Jamshed, A. (2020). *Fundamental of cyber security: Principles, theory and practices*. BPB Publications. ISBN 978-9386551559. ● Easttom, C. (2019). *Computer security fundamentals* (4th ed.). Pearson IT Certification. ISBN 9780135774779. ● 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/Fundam entos-de-Seguridad-de-la-Red	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** **Se usará rúbrica para la entrega de actividades o tareas a realizar.**

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																