Benemérita Universidad Autónoma de Puebla
Vicerrectoría de Docencia
Dirección de Educación Superior
Facultad de Ciencias de la Computación

PLAN DE ESTUDIOS (PE): Licenciatura en Ciencias de la Computación

AREA: Tecnología

ASIGNATURA: Seguridad en Redes

CÓDIGO: CCOA 260

CRÉDITOS: 6 créditos

FECHA: 29 de mayo de 2026

Marcelo Rivera Martínez

RECIBIDO
29 JUN 2026
SECRETARÍA ACADÉMICA

BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA · FACULTAD DE CIENCIAS DE LA COMPUTACIÓN - SECRETARÍA ACADÉMICA · 1578

Benemérita Universidad Autónoma de Puebla
Vicerrectoría de Docencia
Dirección de Educación Superior
Facultad de Ciencias de la Computación

1. DATOS GENERALES

Nivel Educativo:	Licenciatura
Nombre del Plan de Estudios:	Licenciatura en Ciencias de la Computación
Modalidad:	Escolarizada
Modalidad de impartición de la Asignatura:	Presencial
Nombre de la Asignatura:	Seguridad en Redes
Ubicación:	Nivel Formativo
rrelación:	
Asignaturas Precedentes:	Redes de Computadoras
Asignaturas Consecuentes:	Gestión de Proyectos Innovadores

CARGA HORARIA DEL ESTUDIANTE (Ver Malla)

Concepto	Horas por semana		Horas de trabajo independiente por periodo	Total, de horas por periodo	Total, de créditos
	Teoría	Práctica			
Horas teoría, práctica y trabajo independiente (16 horas = 1 crédito)	**3**	**2**	**0**	**90**	**6**

3. REVISIONES Y ACTUALIZACIONES

Autores:	Adriana Hernández Beristain Luis Enrique Colmenares Guillen Mariano Larios Gómez Yeiny Romero Hernández
Fecha de diseño:	9 de enero de 2026
Fecha de la última actualización:	Asignatura de nueva creación.
Fecha de aprobación por parte de la	29 de mayo de 2026

academia de área, departamento u otro.	
Revisores:	Asignatura de nueva creación.
Sinopsis de la revisión y/o actualización:	Asignatura de nueva creación.

4. PERFIL DESEABLE DEL PROFESOR (A) PARA IMPARTIR LA ASIGNATURA:

Disciplina profesional:	Ciencias de la computación, ciencias de la electrónica y áreas afines.
Nivel académico:	Maestría
Experiencia docente:	Mínima 2 años
Experiencia profesional:	Mínima 1 año

5. OBJETIVO: Identificar los servicios de seguridad que todo sistema de comunicación debe pro haciendo énfasis en los algoritmos y protocolos criptográficos definidos en la arquitectura de seguridad Internet a nivel de red, transporte y aplicación que proveen estos servicios de seguridad.

6. CONTENIDO

Unidad de Aprendizaje 1 Fundamentos de la Seguridad en redes de computadoras
Contenido Temático: 1.1 Introducción 1.2 Red de computadoras segura 1.3 Principios de confidencialidad, integridad y disponibilidad (CIA) 1.4 Amenazas y vulnerabilidades comunes en redes 1.5 Cibercrímenes y Hackers.
Referencias: 1. Stallings, W. (2023) Cryptography and Network Security, 8th edition. Ed. Pearson 2. Aumasson, J.-P. (2024) Serious Cryptography, A Practical Introduction to Modern Encryption, 2nd edition. Ed. No Starch Press 3. Menezes, A.J., Van Oorschot, P.C., Vanstone, S.A. (2018) Handbook of Applied Cryptography., 2nd edition. Ed. CRC Press 4. Anderson, R. (2020) Security Engineering: A Guide to Building Dependable Distributed Systems. (3rd edition). Ed. Wiley
Unidad 2 Criptografía y Seguridad de la Información

Contenido Temático:

2.1 Políticas de seguridad en redes
- 2.1.1 Problemas del soporte de políticas
- 2.1.2 Modelo formal de política de seguridad
- 2.1.3 Método para alcanzar objetivos

2.2 Mecanismos de seguridad en redes
2.3 Criptografía y seguridad en redes
- 2.3.1 Introducción a la criptografía: conceptos y algoritmos.
- 2.3.2 Algoritmos de cifrado de llave simétrica
- 2.3.3 Algoritmos de cifrado de llave asimétrica

2.4 Protocolos de seguridad: SSL/TLS, IPsec, VPNs.
- 2.4.1 Arquitectura de IPSec
- 2.4.2 Servicios IPSec
- 2.4.3 Arquitectura SSL
- 2.4.4 Transport Layer Security (TLS)

2.5 Seguridad en el almacenamiento y transmisión de datos

Referencias:

1. Stallings, W. (2023) Cryptography and Network Security, 8th edition, Ed. Pearson
2. Aumasson, J.-P. (2024) Serious Cryptography, A Practical Introduction to Modern Encryption, 2nd edition. Ed. No Starch Press
3. Menezes, A.J., Van Oorschot, P.C., Vanstone, S.A. (2018) Handbook of Applied Cryptography., 2nd edition. Ed. CRC Press
4. Anderson, R. (2020) Security Engineering: A Guide to Building Dependable Distributed Systems. (3rd edition). Ed. Wiley

Marcela Rivera Martínez

Unidad de Aprendizaje 3 Seguridad en Redes Inalámbricas y Móviles

Contenido Temático:

3.1 Riesgos asociados con redes inalámbricas (WLAN)
3.2 Protocolos de seguridad en redes inalámbricas (WPA, WPA2, WPA3)
3.3 Seguridad de dispositivos móviles y BYOD (Bring Your Own Device)
3.4 Evolución del 5G y sus implicaciones en la seguridad de redes
3.5 Creciente vulnerabilidad de dispositivos IoT

Referencias:

1. Stallings, W. (2023) Cryptography and Network Security, 8th edition, Ed. Pearson
2. Aumasson, J.-P. (2024) Serious Cryptography, A Practical Introduction to Modern Encryption, 2nd edition. Ed. No Starch Press

3. Avast. (2025). Seguridad Wi-Fi: ¿Qué son WEP, WPA, WPA2 y WPA3? [Seguridad en línea]. Recuperado de AvastPortnox.
4. Kaspersky. (2024). ¿Qué es WEP, WPA, WPA2 y WPA3 y cuáles son sus diferencias? [Centro de recursos]. Recuperado de KasperskyEsecurity
5. Planet. (2026). Seguridad en redes inalámbricas: WEP, WPA, WPA2 y WPA3 explicados en 2026. Recuperado de Esecurity Planet3.3 Seguridad de dispositivos móviles y BYOD (Bring Your Own Device)
6. Anderson, R. (2020) Security Engineering: A Guide to Building Dependable Distributed Systems. (3rd edition). Ed. Wiley

Unidad de Aprendizaje 4 Mejores practicas

ntenido Temático:

Importancia de la seguridad de redes en la actualidad
Marco legal y regulatorio en seguridad informática
Seguridad en Dispositivos Finales
Seguridad en Aplicaciones y Datos
Estrategias de defensa en profundidad
Métodos de detección y prevención de intrusiones (IDS/IPS)
Seguridad en Entornos Virtualizado

ferencias:

1. Mora, M., & Vaca, J. (2021). Métodos para detección de intrusiones y análisis de firmas. En Seguridad de la información: Enfoques prácticos y metodologías (pp. 45-62). Editorial 3Ciencias. 3Ciencias Repository [1]
2. Sánchez Torres, J. A. (2021). Diseño de una estrategia de seguridad basada en el modelo de defensa en profundidad (Trabajo de grado, Universidad Piloto de Colombia). Repositorio Institucional Unipiloto. unipiloto.edu.co
3. Rodríguez, A. J. (2025). Ciberseguridad: Métodos de defensa ante ataques de infiltración y uso de reglas heurísticas. RIDE Revista Iberoamericana para la Investigación y el Desarrollo Educativo, 16(31), 112-128. RIDE Editorial
4. CyberH2O. (2025). Módulo 1: Marco legal y regulatorio en ciberseguridad. cyberh2o.es
5. Sánchez, M. A. (2023). Introducción a la seguridad en cloud computing y riesgos del "Shadow IT". Universitat Oberta de Catalunya UOC Open AccessSantoro
6. Recio, A. (2026). Seguridad y trabajo colaborativo en la nube: Gestión de riesgos en infraestructuras lógicas. Ra-Ma Editorial. Ra-Ma Libros

7. CONTRIBUCIÓN DEL PROGRAMA DE ASIGNATURA AL PERFIL DE EGRESO

Benemérita Universidad Autónoma de Puebla
Vicerrectoría de Docencia
Dirección de Educación Superior
Facultad de Ciencias de la Computación

Perfil de egreso		
Conocimientos	**Habilidades**	**Actitudes y valores**
Fundamentos Matemáticos y teorías de Ciencias de la Computación. Adquiridos a partir del uso y práctica de la criptografía moderna, Analizando los algoritmos y protocolos criptográficos para implementar servicios de seguridad. **radigmas de Programación.** ntificar los servicios de guridad que todo sistema de municación debe de proveer: tenticación, integridad, nfidencialidad, no rechazo y ntrol de acceso. **ndamentos y tecnologías de eligencia Artificial.** ntificar las arquitecturas de guridad en una red de mputadoras. A través del ntificar los ataques y amenazas e hacen que una red de municaciones sea insegura. **Metodologías de la investigación.** Conocer y Planificar estrategias para seleccionar y coordinar los protocolos encaminados a garantizar la seguridad en las redes de computadoras. **Tecnologías emergentes.** Integrar los servicios de seguridad	**Analizar y generar modelos matemáticos.** Cuestionar la información y encontrar respuestas respecto a la seguridad en redes de computadoras. **Interactuar con usuarios y especialistas de diversas áreas de conocimiento.** Trabajar en equipo y comunicar puntos de vista sobre la vulnerabilidad de una red en cuanto a ataques y amenazas. **Razonar de manera computacional.** Investigar y analizar casos de inseguridad para poner en práctica su conocimiento adquirido. **Desarrollar y aplicar metodologías para el análisis, diseño e implementación de sistemas de cómputo.** Desarrollar y aplicar metodologías para el desarrollo de aplicaciones seguras. **Comunicar ideas y transferir conocimiento.** A través de la investigación y del uso de herramientas y tecnologías innovadoras ayudará a resolver problemas	**Mentalidad positiva ante los cambios científicos y tecnológicos.** Estar dispuesto a adaptarse a los constantes cambios actualizaciones de los ataques y manera de prevenirlos. **Actualización disciplin permanente.** Ser autodidacta en los proces investigación y actualización. **Trabajo en equipo.** Buscar el bien común al trabaj equipo. **Emprender y/o liderar proyectos de cómputo.** Enfocar sus conocimientos en garantizar la seguridad de su software. **Adaptabilidad y resiliencia.** Apertura al diálogo para resolv problemas de inseguridad en s aplicaciones. **Participación en la transformaci de la sociedad.** Usar sus conocimientos pa garantizar la seguridad de s productos. **Responsabilidad en su actuar profesional**.

Perfil de egreso		
Conocimientos	**Habilidades**	**Actitudes y valores**
en las redes con las aplicaciones y cómputo centrado en la red.	de seguridad en la red indicando el proceso a seguir. **Comunicarse en una lengua extranjera** Hacer uso de otro lenguaje para configurar herramientas o poner en práctica software de seguridad.	Trabajar en los tiempos y c acciones pertinentes para lograr objetivo del trabajo. **Respeto.** Actuar con respeto responsabilidad hacia s compañeros, así como en el traba que realizan en pro de la seguridad de los sistemas. **Integridad.** Manejarse con rectitud y coherencia en su actuar durante los trabajos realizados, así como en la protección de los sistemas. **Honestidad.** Actuar con transparencia en la protección de la información en todo momento

Describa cómo el eje o los ejes transversales contribuyen al desarrollo de la asignatura

(s) transversales	Contribución con la asignatura
mación humana y social	Las prácticas se elaboran en equipo fomentando responsabilidad y respeto entre los integrantes.
Desarrollo de habilidades en el uso de las Tecnologías de la Información y la Comunicación	Las prácticas se basan en la seguridad para una re de computadoras, identificando cómo participan hardware y software en la seguridad.
Desarrollo de habilidades del pensamiento complejo	Capacidad de identificar cada una de las amenazas a la seguridad que se enfrentan la red.
Lengua Extranjera	Bibliografía y artículos de interés en el idioma inglés.
Innovación y talento universitario	Planificar estrategias para proponer mejoras a la seguridad de día a día.
Educación para la Investigación	Estudio y aplicación en Proyectos

9. Criterios y Acciones del SEAES relacionados con el perfil de egreso

Criterio(s)	Acción (es)	Contribución con el Perfil de Egreso
Compromiso con la responsabilidad social	2. Impulso de la responsabilidad ciudadana y participación democrática, en el contexto de las problemáticas más sensibles de las comunidades cercanas.	Identificar las diferentes clases de riesgos que hay en las redes de computadoras, analizar y establecer una política corre de protección de la informac Planificar estrategias p seleccionar y coordinar protocolos encaminados garantizar niveles estándares seguridad en las redes computadoras.
uidad social y género	2. Construcción de relaciones sociales, económicas y culturales basadas en el respeto de los derechos humanos.	Mediante el trabajo en equipo y colaborativo, fomentar la responsabilidad y solidaridad.
lusión	6. Promoción de medidas, proyectos y planes, que contribuyan a impulsar la inclusión social.	Emprender y/o liderar proyectos de cómputo con responsabilidad y solidaridad.
elencia	1. Desarrollo del pensamiento crítico a partir de la libertad, el análisis, la reflexión y la argumentación.	Definir lo que es seguridad para una red de computadoras, considerando las formas de protección, entre ellas tomando en cuenta el triángulo de l seguridad (CID). Innovaciones en las formas d cómputo centrado en la red.
Vanguardia	1. Conocimiento de las principales innovaciones científicas y tecnológicas, así como de las humanidades, relacionadas con la profesión.	Saber Identificar los ataques amenazas que hacen que una re sea vulnerable y las políticas que se deben seguir para establecer la seguridad en la red.

Innovación social	4. Competencia para formar parte de proyectos que permitan la transformación social.	Saber Identificar las principales amenazas de seguridad a las que se enfrentan las redes para contribuir a un buen desarrollo de investigación, que derive en nuevas alternativas del uso de tecnologías de la computación.
Interculturalidad	6. Desarrollo de habilidades de comunicación efectiva utilizando diversos lenguajes y tecnologías.	Interactuar con usuarios especialistas de diversas áreas conocimiento. Comunicarse una lengua extranjera, con finalidad de compa experiencias y soluciones.

10. ESTRATEGIAS, TÉCNICAS Y RECURSOS DIDÁCTICOS

Estrategias y Técnicas didácticas	Recursos didácticos
• *Aprendizaje basado en problemas* • *Aprendizaje basado en proyectos* • *Aprendizaje colaborativo* • *Aprendizaje reflexivo* • *Ejercicios dentro de clase* • *Exposición audiovisual* • *Portafolios y documentación de avances* • *Prácticas de campo* • *Prácticas de laboratorio* • *Trabajo de investigación* • *Trabajo en equipo*	• *Impresos (textos): libros, documentos...* • *Materiales de laboratorio* • *Materiales audiovisuales* • *Software especializado* • *Plataformas educativas (LMS)*

11. CRITERIOS DE EVALUACIÓN

Criterios	Porcentaje
• *Exámenes*	*30%*
• *Informe de prácticas*	*60%*
• *Presentación en clase*	*10%*
Total	*100%*

12. REQUISITOS DE ACREDITACIÓN

Estar inscrito como alumno en la Unidad Académica en la BUAP.
Asistir como mínimo al 80% de las sesiones para tener derecho a exentar por evaluación continua y/o presentar el examen final en ordinario o extraordinario.
Asistir como mínimo al 70% de las sesiones para tener derecho al examen extraordinario.
Cumplir con las actividades académicas y cargas de estudio asignadas que señale el PE.

Notas:

a) La entrega del programa de asignatura, con sus respectivas actas de aprobación, deberá realiza formato electrónico, vía oficio emitido por la Dirección o Secretaría Académica, a la Dirección de Edu Superior.