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

ÁREA: Tecnología

ASIGNATURA: Seguridad en Redes

CÓDIGO: CCOS263

CRÉDITOS: 6 créditos

FECHA:

1. DATOS GENERALES

Nivel Educativo:	Licenciatura.
Nombre del Plan de Estudios:	Licenciatura en Ciencias de la Computación
Modalidad Académica:	Presencial.
Nombre de la Asignatura:	Seguridad en redes
Ubicación:	Nivel Formativo.
Correlación:	
Asignaturas Precedentes:	Redes de Computadoras
Asignaturas Consecuentes:	Redes Avanzadas

2. CARGA HORARIA DEL ESTUDIANTE

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

3. REVISIONES Y ACTUALIZACIONES

Autores:	
Fecha de diseño:	
Fecha de la última actualización:	11 de noviembre de 2022
Fecha de aprobación por parte de la academia de área, departamento u otro.	14 de noviembre de 2022
Revisores:	Soriano Rosas José Isabel Sánchez Rinza Bárbara Emma Hernández Beristain Adriana León Chávez Miguel Ángel Vázquez Ramírez Jesús
Sinopsis de la revisión y/o actualización:	Se actualiza la bibliografía del curso

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

Disciplina profesional:	Licenciado o Ingeniero en electrónica, o Ingeniero en computación.
Nivel académico:	Maestría o superior.
Experiencia docente:	1 año.
Experiencia profesional:	3 años.

5. PROPÓSITO:

Identificar las diferentes clases de riesgos que hay en las redes de computadoras, analizar y establecer una política correcta de protección de la información. Planificar estrategias para seleccionar y coordinar los protocolos encaminados a garantizar niveles estándares de seguridad en las redes de computadoras

6. COMPETENCIAS PROFESIONALES:

Para el estudio de este programa de asignatura, se cita la siguiente competencia definida en la Actualización del Plan de Estudios de la Licenciatura en Ciencias de la Computación Generación 2016:

“Entender la importancia de las redes computacionales y su aplicabilidad para obtener su mejor aprovechamiento en la solución de problemas actuales”.

Esta competencia contribuye al programa proporcionando los conceptos actuales y análisis necesarios en la seguridad de la red para entender los problemas de hoy en día que afectan a la red y definir posibles soluciones.

Unidad de Aprendizaje	Contenido Temático	Referencias
1 Introducción a la Seguridad en redes de computadoras	1.1 Introducción 1.2 Red de computadoras segura 1.3 Formas de protección 1.4 Estándares de protección	1. Cole, E. et al. (2015). Network Security Bible. (3nd edition). USA:Wiley Publishing, Inc. 2.- Pfleeger, C. (2016).Security in Computing.(5th edition) USA: Prentice Hall. 3. Ross Anderso, (2015) Security Engineering:, (2nd edition). USA: Wiley Publishing, Inc. 5. Stallings, W. (2020) Cryptography and Network Security: Principles and Practice. (8th Ed.) USA: Peaarson
2 Retos de la Seguridad en redes de computadoras	2.1 Preocupaciones y conceptos 2.2 Seguridad ante amenazas y ataques en redes 2.3 Vulnerabilidades en redes 2.4 Cyber crímenes y Hackers 2.5 Scripts hostiles 2.6 Políticas de seguridad en redes 2.6.1 Problemas del soporte de políticas 2.6.2 Modelo formal de política de seguridad 2.6.3 Método para alcanzar objetivos	1 Stallings, W. (2018) Effective Cybersecurity. (1st Ed.) USA: Pearson

3 Seguridad en Redes de computadoras.	3.1 Introducción 3.2 Elementos de un esquema de seguridad en red 3.3 Implementación de un esquema de seguridad en red 3.4 Niveles de seguridad 3.4.1 Primer nivel de seguridad 3.4.2 Segundo nivel de seguridad 3.4.3 Tercer nivel de seguridad 3.4.4 Cuarto nivel de seguridad 3.5 Servicios de seguridad en redes 3.5.1 Confidencialidad 3.5.2 Integridad 3.5.3 Autenticación y no repudio 3.5.4 Disponibilidad 3.6 Mecanismos de seguridad en redes 3.7 Criptografía y seguridad enredes 3.7.1 Cifrado link to link 3.7.2 Cifrado end to end 3.7.3 SILS ("Standard for Interoperability LAN Security") Retos de la criptografía en la seguridad en redes	1.- Edgar Vega Briceño, (2021), Seguridad de la información, (1ª edición),editoral Area de innovación y desarrollo S. L

Unidad de Aprendizaje	Contenido Temático	Referencias
4 Protocolos de seguridad en redes de computadoras	4.1 Introducción 4.2 Seguridad en la capa de aplicación 4.2.1 PGP (Pretty Good Privacy) 4.2.2 Seguro / Extensión del correo multipropósito de internet (S/MIME) 4.2.3 Seguridad -HTTP (S-HTTP) 4.2.4 Protocolo de transferencia de hipertexto sobre Secure Socket Layer (HTTPS) 4.2.5 Seguridad en transacciones electrónicas (SET) 4.2.6 Kerberos 4.3 Seguridad en la capa de transporte 4.3.1 SSL (Secure Socket Layer) 4.3.2 Seguridad en la capa de transporte (TLS) 4.4 Seguridad en la capa de red 4.4.1 Seguridad en el protocolo Internet (IPSec) 4.4.2 Redes virtuales privadas (VPN) 4.5 Seguridad en la capa de enlace and sobre LANS 4.5.1 Protocolo punto a punto (PPP) 4.5.2 Servicio de autenticación remota de usuario de dial (RADIUS) 4.5.3 Sistema de control de acceso para controlar el accesoa laterminal (TACACS)	A Hertzog (2019). Experto En Seguridad: Análisis de Riesgo. Editorial Kindle James S. Tiller (2000). A Technical Guide to IPSec Virtual Private Networks. (1st Edición). Auerbach Publications.

Unidad de Aprendizaje	Contenido Temático	Referencias
5 Seguridad en IP (IPSec)	5.1 Introducción 5.2 Aplicaciones de IPSec 5.3 Beneficios y ventajas de IPSec 5.4 Aplicaciones de ruteo 5.5 Arquitectura de IPSec 5.5.1 Servicios IPSec 5.5.2 Asociaciones de seguridad 5.5.3 Modos de uso: transporte y túnel 5.6 Authentication Header (AH) 5.6.1 Servicio anti réplica 5.6.2 Valor de verificación de integridad 5.7 ESP ("Encapsulating Security Payload")	A Hertzog (2019). Experto En Seguridad: Análisis de Riesgo. Editorial Kindle James S. Tiller (2000). A Technical Guide to IPSec Virtual Private Networks. (1st Edición). Auerbach Publications.

6 Herramientas deSeguridad en Red.	6.1 Concepto de protocolo 6.1 Kerberos 6.1.1 Introducción 6.1.2 La idea de Kerberos 6.1.3 Suposiciones que hace Kerberos 6.1.4 Protocolo de Kerberos 6.1.5 Análisis de Kerberos 6.1.6 Servicio de autenticación (AS) 6.1.7 Servidor de tickets 6.1.8 Autenticación a través dedominios 6.2 SSH ("Secure Shell") 6.2.1 Introducción 6.2.2 La idea de SSH 6.2.3 Funcionamiento de SSH 6.2.4 Distribuciones de SSH 6.3 Nessus 6.3.1 Introducción 6.3.2 Características 6.3.3 Reportes 6.3.4 Distribución 6.4 John the Ripper 6.4.1 Introducción 6.4.2 Modos de operación Utilización	1. D'Agostino, G. (2019). Data Security in Cloud Computing, Volume I: Vol. First edition. Momentum Press. 2. D'Agostino, G. (2019). Data Security in Cloud Computing, Volume I: Voll. First edition. Momentum Press. 3. Galindo Ramírez, X., Gómez Duarte, M. A., & Hernández Gutiérrez, J. (2019). Seguridad en la nube, evolución indispensable en el siglo XXI. Revista Vínculos, 16(1), 110–127

Unidad de Aprendizaje	Contenido Temático	Referencias
7 Seguridad en Web	7.1 Introducción 7.2 Consideraciones de seguridaden Web 7.2.1 Amenazas a la seguridad enWeb 7.2.2 Seguridad del tráfico Web 7.3 SSL ("Secure Socket Layer") 7.3.1 Arquitectura SSL 7.3.2 SSL Record protocol 7.3.3 Change Cipher Protocol 7.3.4 Alert Protocol 7.3.5 Handshake Protocol 7.4 TLS (Transport Layer Security)	Suárez Vargas, F. C. (2020). *Sistema de comunicaciones.*. Jorge Sarmiento Editor - Universitas. GUTIÉRREZ, O. E. **Comunicaciones móviles y redes inalámbricas**. ed. Córdoba: Jorge Sarmiento Editor - Universitas, 2020. 200 p. Disponible en: Danizio, P. E. (2020). *Teoría da las comunicaciones.*. Jorge Sarmiento Editor - Universitas. Danizio, P. E. (2020). *Teoría da las comunicaciones.*. Jorge Sarmiento Editor - Universitas.

8 Firewalls	8.1 Introducción 8.2 Objetivos y alcances 8.3 Decisiones de diseño 8.4 Preocupaciones y problemas con firewalls 8.5 Tipos de firewalls 8.5.1 Ruteador filtrador depaquetes 8.5.2 Utilización de gateways 8.5.3 Host Bastión 8.5.4 Ejemplos de utilización de gateways 8.5.5 Beneficios de los gateways 8.5.6 Firewalls tipo gateway de doble domicilio 8.5.7 Firewalls tipo anfitrión oculto 8.5.8 Firewalls tipo subred oculta 8.6 Integración de modems con firewalls 8.7 Requerimientos y configuraciónde firewalls	Danizio, P. E. (2019). *Sistemas de comunicaciones.*. Jorge Sarmiento Editor - Universitas. Pineda Sanchez, S. & Morales Delgadillo, H. (2020). *Topología aplicada en redes ad hoc. Mare Ingenii. Ingenierías, 2 (1), 18-26.*. Fundación Universitaria San Mateo. Tello Portillo, J. P. (2017). *Introducción a las señales y sistemas.*. Universidad del Norte.

8. ESTRATEGIAS, TÉCNICAS Y RECURSOS DIDÁCTICOS

Estrategias y técnicas didácticas	Recursos didácticos
Estrategias de aprendizaje: • Lectura y comprensión, • Reflexión, • Comparación, • Resumen. Estrategias de enseñanza: • ABP, • Aprendizaje activo, • Aprendizaje cooperativo, • Aprendizaje colaborativo, • Basado en el descubrimiento. Ambientes de aprendizaje: • Aula, • Laboratorio, • Simuladores. Actividades y experiencias deaprendizaje: • Visita a empresas.Técnicas • grupales, • de debate, • del diálogo, • de problemas, • de estudio de casos, • cuadros sinópticos, • mapas conceptuales, • para el análisis, • comparación,	Materiales: • Proyectores • TICs • Plumón y pizarrón • Libros, fotocopias yartículos • Equipo de laboratorio

Estrategias y técnicas didácticas	Recursos didácticos
• síntesis, • mapas mentales, • lluvia de ideas, • analogías, • portafolio, • exposición.	

9. EJES TRANSVERSALES

Eje (s) transversales	Contribución con la asignatura
Formación Humana y Social	Las prácticas se elaboran en equipo fomentando la 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 red de computadoras, identificando cómo participan el 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 Web.
Lengua Extranjera	Bibliografía 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 de casos reales en elproyecto final.

10. CRITERIOS DE EVALUACIÓN

Criterios	Porcentaje
▪ Exámenes	**50%**
▪ Trabajos de investigación y/o de intervención	10%
▪ Prácticas de laboratorio	20%
▪ Proyecto final	20%
Total	100%

11. 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%delas 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 realizarse en formato electrónico, vía oficio emitido por la Dirección o Secretaría Académica a la Dirección General de Educación Superior.

b) La planeación didáctica deberá ser entregada a la coordinación de la licenciatura en los tiempos y formas acordados por la Unidad Académica.