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

ÁREA: Tecnología

ASIGNATURA: Intercomunicación y Seguridad en Redes

CÓDIGO: **ICCS 262**

CRÉDITOS: 6 créditos

FECHA: 4 de julio de 2017

1. DATOS GENERALES

Nivel Educativo:	Licenciatura
Nombre del Plan de Estudios:	Ingeniería en Ciencias de la Computación
Modalidad Académica:	Presencial
Nombre de la Asignatura:	Intercomunicación y Seguridad en Redes
Ubicación:	Nivel Formativo
Correlación:	
Asignaturas Precedentes:	Administración de redes
Asignaturas Consecuentes:	Ninguna

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:	Apolonio Ata Pérez Jorge Jiménez González Miguel Ángel León Chávez José Esteban Torres León
Fecha de diseño:	1 de junio de 2009
Fecha de la última actualización:	4 de julio de 2017
Fecha de aprobación por parte de la academia de área, departamento u otro.	4 de julio de 2017
Revisores:	Bárbara Emma Sánchez Rinza Miguel Ángel León Chávez Apolonio Ata Pérez Edna Iliana Tamariz Flores Verónica Edith Bautista López
Sinopsis de la revisión y/o actualización:	1. Se cambió el programa a competencias para aplicarlo a semestre. 2. Se actualizaron las referencias bibliográficas para cada una de las unidades. 3. Se reestructuró todo el programa para las nuevas tendencias.

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

Disciplina profesional:	Ciencias o Ingeniería en Computación y Ciencias o Ingeniería en Electrónica en el área de redes.
Nivel académico:	Maestría
Experiencia docente:	Mínima de 2 años
Experiencia profesional:	Mínima de 1 año

5. PROPÓSITO: Realizar análisis y comprensión de los principios de interconectividad de las redes actuales así como de identificar las diferentes clases de riesgos que hay en las redes de computadoras, analizando y estableciendo 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:

Esta materia se basa en tres competencias definidas en el Programa de Estudios de la Licenciatura en Ingeniería en Ciencias de la Computación, las cuales se citan a continuación:

"Analizar los principales problemas en su área, identificando los conocimientos necesarios y las herramientas adecuadas para proponer soluciones y divulgar los resultados obtenidos."

"Interactuar con el usuario entendiendo y atendiendo sus necesidades con el fin de generar soluciones en su competencia."

"Aplicar los avances tecnológicos más recientes en las áreas de desarrollo de aplicaciones de software, tratamiento de datos, redes de computadoras, sistemas empotrados, control digital y robótica con el fin de proponer soluciones innovadoras a problemas en el desarrollo científico-tecnológico del país"

De acuerdo a lo que se estudia en esta materia se cumplen las competencias al realizar un análisis de las necesidades y problemáticas de las redes actuales, cuyo tema principal es la integridad de los datos del usuario, por lo que es importante resaltar la seguridad en capa del modelo OSI y, con base en eso, se puedan proponer soluciones en la seguridad en redes actuales de acuerdo a las necesidades del usuario.

7. CONTENIDOS TEMÁTICOS

Unidad de Aprendizaje	Contenido Temático	Referencias
1. Interconectividad	1.1 Concepto de servicio universal 1.2 Interconectividad 1.3 Arquitectura de las Interredes 1.4 Protocolos de interconectividad	1. Tanenbaum, A. (2012). Redes de Computadoras. (5ª edición). México: Pearson Education. 2. Brown, A. (2013). Computer Networks. (1ª edición). USA

Unidad de Aprendizaje	Contenido Temático	Referencias
2. Protocolos de Interconexión	2.1 Servicios de IPv4 2.2 Servicios de IPv6	1. Douglas, E. (2015). Redes de Computadoras e Internet. (6ª edición). USA: Pearson Education. 2. Stallings, W. (2013). Data & Computer Communication. (10th edition). USA: Pearson Education. 3. Prakash, C. (2014). Data Communications and Computer Networks. (2014). USA: PHI Learning. 4. Snader, J. (2015). VPNs Ilustrated: tunnels, VPNs, and IPsec. Addison-Wesley Professional.
3. Servicios y Mecanismos de Seguridad	3.1 Servicios de seguridad del OSI 3.1.1 Definición de los servicios de seguridad OSI: autenticación, control de acceso, confidencialidad, no repudio, integridad y control de acceso. 3.2 Mecanismos de seguridad 3.2.1 Cifrado simétrico por bloques y por flujo 3.2.2 Funciones Hash y MAC 3.2.3 Cifrado asimétrico 3.2.4 Firma digital	1. Castro, G.,Díaz, O., Alzorriz A, y San Cristobal R. (2014). Procesos y Herramientas para la seguridad de Redes. España:UNED. 2. Opplige, R. (2016). SSL and TLS: Theory and Practice. Second Edition. Reino Unido: Artech House. 3. Stallings, W. (2016). Cryptography and Network Security: Principles and Practice. (7th Edition). USA: Pearson.
4. Seguridad a nivel de red	4.1 IPSEC 4.1.1 Servicios del encabezado AH 4.1.2 Servicios del encabezado ESP 4.2 Filtrado de paquetes 4.3 Túneles	1. Stallings, W. (2013). Data & Computer Communication. (10th edition). USA: Pearson Education.
5. Seguridad a nivel de transporte	5.1 SSL/TLS	1. Peña, V. (2015). De la firma manuscrita a las firmas electrónica y digital. Colombia: Universidad de Externado.

Unidad de Aprendizaje	Contenido Temático	Referencias
		2. Shaw, M., Blanning, R., Strader, T. and Whinston, A. (2012).Handbook on Electronic Commerce. 1ª edición. USA: Springer. 3. Panek, W. (2015), MCSA Windows Server 2012 R2 Administration Study Guide. John Wiley & Sons. 4. Stallings, W. (2016). Cryptography and Network Security: Principles and Practice. (7th Edition). USA: Pearson.
6. Seguridad a nivel de aplicación	6.1 IPSEC 6.1.1 Servicios de ISAKMP 6.1 Características y Servicios de seguridad que ofrece Kerberos 6.3 Características y servicios de seguridad que debe ofrecer E-Cash 6.4 Características y servicios de seguridad que ofrecen los EFS (Encrypting File System, Sistemas de Archivos Criptográficos) 6.5 Características y Servicios de seguridad que ofrece el protocolo SET (Secure Electronic Transaction, Transacciones Electrónicas Seguras)	1. Peña, V. (2015). De la firma manuscrita a las firmas electrónica y digital. Colombia: Universidad de Externado. 2. Shaw, M., Blanning, R., Strader, T. and Whinston, A. (2012).Handbook on Electronic Commerce. 1ª edición. USA: Springer. 3. Panek, W. (2015), MCSA Windows Server 2012 R2 Administration Study Guide. John Wiley & Sons. 4. Stallings, W. (2016). Cryptography and Network Security: Principles and Practice. (7th Edition). USA: Pearson.
7. Sistemas de gestión de incidentes	7.1 Concepto del incidente de seguridad 7.2 Tipos de incidentes: acceso no autorizado, código malicioso, denegación de servicios, intentos de obtención de información y mal uso de los recursos. 7.3 Sistemas de detección de intrusiones (IDS,Intruder Detection System) 7.3.1 IDS basados en red (NIDS) 7.3.2 IDS basados en host (HIDS) 7.3.3 IDS de detección de abusos o firmas 7.3.4 IDS de detección de anomalías	1. Stallings, W. (2013). Data & Computer Communication. (10th edition). USA: Pearson Education. 2. Panek, W. (2015).MCSA Windows Server 2012 R2 Administration Study Guide. John Wiley & Sons. 3. Al-Shaer E. (2014). Automated Firewall Analytics. NC. USA: Springer. 4. Chicano, T. (2015). Gestión de Incidentes de Seguridad

Unidad de Aprendizaje	Contenido Temático	Referencias
	7.4 Firewall como sistema de detección de intrusiones 7.4.1 Firewall de capa de red 7.4.2 Firewall de capa de aplicación 7.5 Sistemas de Prevención de intrusiones (IPS, Intruder Prevention System) 7.5.1 IPS de filtrado de paquetes 7.5.2 IPS de bloqueo de IP 7.5.3 IPS con acción de decepción 7.6 Algunas herramientas disponibles en el mercado (IDS/IPS): snort, hogwash , snort_inline,snortsam. Honeyd, specter y Toolkit Decepcion.	Informática. IFCT0109. IC Editorial.

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 de aprendizaje: • Visita a empresas. Técnicas • grupales, • de debate, • del diálogo, • de problemas, • de estudio de casos, • cuadros sinópticos, • mapas conceptuales, • para el análisis, • comparación, • síntesis, • mapas mentales, • lluvia de ideas, • analogías, • portafolio, • exposición.	Materiales: • Proyectores • TICs • Plumón y pizarrón • Libros, fotocopias y artículos en inglés • Equipo de laboratorio

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 identificar e implementar algoritmos para que una red sea segura.
Desarrollo de Habilidades del Pensamiento Complejo	Capacidad de identificar en una red la prevención y detección de incidentes.
Lengua Extranjera	Investigaciones y bibliografía en el idioma inglés.
Innovación y Talento Universitario	Configuración de los dispositivos que componen el diseño de una red aportando mejorías a la seguridad.
Educación para la Investigación	Estudio y aplicación de casos reales en el proyecto final.

10. CRITERIOS DE EVALUACIÓN

Criterios	Porcentaje
▪ Exámenes	40%
▪ Prácticas de laboratorio	40%
▪ 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% de las sesiones para tener derecho al examen extraordinario
Cumplir con las actividades académicas y cargas de estudio asignadas que señale el PE
La calificación mínima para considerar un curso acreditado será de 6

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.