PLAN DE ESTUDIOS (PE): Ingeniería en Tecnologías de la Información

AREA: Ciencias Básicas

ASIGNATURA: Redes y Servicios

CÓDIGO: ITIS-250

CRÉDITOS: 6

FECHA: 17 de Abril de 2017

1. DATOS GENERALES

Nivel Educativo:	Licenciatura
Nombre del Plan de Estudios:	Licenciatura en Ingeniería en Tecnologías de la Información
Modalidad Académica:	Presencial
Nombre de la Asignatura:	Redes y servicios
Ubicación:	Nivel Formativo
Correlación:	
Asignaturas Precedentes:	Redes de computadoras
Asignaturas Consecuentes:	Administración de redes

Conocimientos, habilidades, actitudes y valores previos:	**Conocimientos** • Identificar lo que son Redes LAN y WAN • Diseñar y configurar Redes LAN y WAN • Conocer las características de los diferentes protocolos de la capa de aplicación del modelo OSI. • Identificar los puertos en los que trabaja cada protocolo. **Habilidades** • Facilidad para tomar acciones remotas o locales • Administrar todo equipo de telecomunicaciones de voz, datos y video, así como capacidad de reconocer fallas y verificar el rendimiento de una red • Innovación para mejorar lo existente • Trabajo en equipo para enfrentar los retos tecnológicos y sociales • Capacidad de investigar y hacer juicios críticos • Aprender por si mismo • Trabajo en equipo para la resolución de problemas, **Actitudes y valores**
	Una actitud para aprender nuevos conceptos y realizar innovaciones. De honestidad, bien común y responsabilidad De respeto y empatía con las personas. De liderazgo y humanismo.

2. CARGA HORARIA DEL ESTUDIANTE

Concepto	Horas por periodo		Total de horas por periodo	Número de créditos
	Teoría	Práctica		

Horas teoría y práctica (16 horas = 1 crédito)	**3**	**2**	**90**	**6**

3. REVISIONES Y ACTUALIZACIONES

Autores:	Dra. Bárbara Sánchez Rinza Dr. Miguel Ángel León Chávez M.C. Edna Iliana Tamariz Flores
Fecha de diseño:	4 de julio de 2014
Fecha de la última actualización:	17 de abril de 2017
Fecha de aprobación por parte de la academia de área	17 de abril de 2017
Fecha de aprobación por parte de CDESC-UA	
Fecha de revisión del Secretario Académico	
Revisores:	Dra. Bárbara Emma Sánchez Rinza MC. Ana Claudia Zenteno Vázquez Dr. Miguel Ángel León Chávez Dr. Luis Enrique Colmenares Guillen MC. Apolonio Ata Pérez MC. Edna Iliana Tamariz Flores M.C. Adriana Hernández Beristain M.C. Yeiny Romero Hernández Dra. Elsa Chavira Martínez M.C. Guillermina Sánchez Román
Sinopsis de la revisión y/o actualización:	1. Se redefinieron dos temas de la Unidad 1 2. Se cambió la unidad 2 por Amenazas en los servicios de red

	3. La anterior unidad 2, pasa a ser la unidad 3 como Instalación, configuración y administración de servicios de red, donde se amplían más los temas de los servicios. 4. La unidad 3 anterior pasa a ser la unidad 4, Herramientas de monitoreo y supervisión para la red, y se actualizaron las herramientas. 5. En las unidades anteriores 4 y 5, se reordenaron los temas de seguridad para dejar sólo la unidad 5 como Seguridad en la Comunicación. 6. En la unidad 6, se agregó el tema DMZ.

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

Disciplina profesional:	Redes de computadoras y seguridad en redes
Nivel académico:	Maestría en áreas afines
Experiencia docente:	Mínima de 2 años
Experiencia profesional:	Mínima de 1 año

5. PROPÓSITO:

Comprender y configurar los diferentes servicios de red, manipular las diferentes herramientas de monitoreo para aprender identificar fallas y mantener una red operativa eficiente y segura.

6. COMPETENCIAS PROFESIONALES:

Esta materia se basa en la competencia definida en el Programa de Estudios de la Licenciatura en Ingeniería en Tecnologías de la Información, la cual se cita a continuación:
“Aplica el análisis, diseño e implementación para integrar elementos de seguridad y confiabilidad en las TI”.
De acuerdo a lo que se estudia en esta materia se cumple la competencia al mostrar la importancia de conocer los diferentes servicios de red que toda organización pequeña o grande debe contener, identificando los fallos o agujeros que un servicio débil puede tener, así como las herramientas de monitoreo actuales que darán a un red de computadoras seguridad y confiabilidad.

7. CONTENIDO

Unidad de Aprendizaje	Contenido Temático	Referencias
1 Introducción a la administración de redes	1.1 Servicios actuales en la red y algunas aplicaciones 1.2. Organizaciones que prestan servicios de red 1.2.1 IANA 1.2.2 Proveedores de servicios 1.3 Acuerdos de nivel de servicio 1.4 Políticas en la red	1. Tanenbaum, A. (2012). Redes de Computadoras. (5ª edición). México: Pearson Education. 2. Braga J., Zambenedetti L., O'Flaherty C., Moreiras A. M., (2014). El libro del IETF. Brasil: free distribution. 3. Díaz G., Alzórriz I., Sancristóbal E., Ruiz M., (2014). Procesos y herramientas para la seguridad de redes. Madrid: Universidad Nacional de Educación a distancia. 4. Dordoigne J., (2015), Redes informáticas Nociones fundamentales. (5ª edición). Barselona: Ediciones ENI.
2 Amenazas en los servicios de red	2.1 Evitar amenazas en los servicios de red 2.1.1 Confidencialidad 2.1.2 Integridad 2.1.3 Disponibilidad 2.1.4 Responsabilidad 2.1.5 Control de acceso 2.1.6 Autenticación	1. Tanenbaum, A. (2012). Redes de Computadoras. (5ª edición). México: Pearson Education. 2. Dordoigne J. (2015), Redes informáticas Nociones fundamentales. (5ª edición). Barselona: Ediciones ENI.

3 Instalación, configuración y administración de servicios de red	3.1 Servicios de red básicos 3.1.1 HTTP 3.1.2 SMTP Y POP 3.1.3 FTP 3.1.4 DHCP 3.1.5 TELNET 3.1.6 DNS 3.1.7 WINS 3.2 Administrar accesos remotos seguros 3.3 Control del acceso a la red 3.4 Prevención de intrusos en la red	1. Tanenbaum, A. (2012). Redes de Computadoras. (5ª edición). México: Pearson Education. 2. Al-Shaer E., (2014). Automated Firewall Analytics. NC. USA: Springer 3. Carrell J. L., Chappell L. A., (2014). Guide to TCP/IP. Fourth edition). USA: Tittel. 4. Dordoigne J., (2015), Redes informáticas Nociones fundamentales. (5ª edición). Barselona: Ediciones ENI. 5. McNab C., (2016). Network Security Assessment. (3ª edición). USA: OReilly Media, Inc.

Unidad de Aprendizaje	Contenido Temático	Referencias
	3.5 Administrar servicios de proxy 3.6 Servicios administrativos 3.7 Administrar Servidor DNS Administrar Servidor HTTP	

4 Herramientas de monitoreo y supervisión para la red	4.1 Clasificación de las herramientas de monitoreo de red 4.2 Monitoreo del rendimiento de dispositivos, servidores y aplicaciones 4.3 Herramientas para auto descubrir los servicios en la red 4.4 Monitoreo de redes LAN 4.5 Monitoreo del rendimiento de ordenadores, redes y aplicaciones 4.6 Herramientas para supervisar los recursos de la red y detectar problemas 4.7 Comparación de las herramientas	1. Tanenbaum, A. (2012). Redes de Computadoras. (5ª edición). México: Pearson Education. 2. Calvo A., (2014). Gestión de redes telemáticas. (1ª edición). España: ic editorial 3. Cardador L., (2014). Dimensionar, instalar y optimizar el hardware. (1ª edición). España: ic editorial.
5 Seguridad en la comunicación	5.1 HTTPS 5.2 SSH 5.3 IPsec (Protocolo de seguridad para Internet) 5.4 RRAS (Servicio de enrutamiento y acceso remoto) 5.5 Redes privadas virtuales 5.6 Seguridad inalámbrica 5.6.1 Seguridad del 802.11 5.6.2 Seguridad de Bluetooth	1. Díaz G., Alzòrriz I., Sancristóbal E., Ruiz M. (2014). Procesos y herramientas para la seguridad de redes. Madrid: Universidad Nacional de Educacion a distancia. 2. Al-Shaer E. (2014). Automated Firewall Analytics. NC. USA: Springer 3.McNab C. (2016). Network Security Assessment. (3ª edición). E.U.: OReilly Media, Inc.
Unidad de Aprendizaje	**Contenido Temático**	**Referencias**

	5.6.3 Seguridad de (wap, wep, wep2)	
6 Administración de cortafuegos	6.1 Introducción 6.2 Tipos de cortafuegos 6.2.1 Filtro de paquetes 6.2.2 Paquetes con estado 6.2.3 Nivel de aplicación 6.3 Cortafuegos de nodo y red 6.4 Ubicación de los cortafuegos y topología de red 6.5 Instalación y configuración de cortafuegos 6.6 DMZ	1. Vacca. (2014). Managing Information Security. (2° edición). USA: Elsevier. 2. Al-Shaer E. (2014). Automated Firewall Analytics. NC. USA: Springer 3. Vacca. (2013). Computer and Information Security Handbook. (2° edición). USA: Elsevier.

8. ESTRATEGIAS, TÉCNICAS Y RECURSOS DIDÁCTICOS

Estrategias y técnicas didácticas	Recursos didácticos

Estrategias de aprendizaje: • Lectura y comprensión, • Reflexión, • Comparación, • Resumen • Casos extremos de caídas de sistema y seguridad • Análisis comparativo de casos de estudio propuestos • Recuperación de accesos al sistema 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 • 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 la configuración de los servicios de red, considerando algún sistema (LINUX o Windows) y monitorear su operatividad mediante las herramientas para la detección de fallas y mejora de dichos servicios. .
Desarrollo de Habilidades del Pensamiento Complejo	Capacidad de analizar el monitoreo de los servicios de red e identificar las fallas mediante el aprendizaje y aplicaciones de las diferentes herramientas de monitoreo.
Lengua Extranjera	Bibliografía, programas y herramientas en el idioma inglés.
Innovación y Talento Universitario	Identificar y dar solución a problemas de acceso y seguridad de los servicios de redes, reconociendo diferentes mecanismos de control y monitoreo según sea el caso.
Educación para la Investigación	Estudio y aplicación de casos reales en el proyecto final, y lecturas de bibliografía de trabajos de investigación actuales.

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
La calificación mínima para considerar un curso acreditado será de 6
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.