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

AREA: Tecnología

ASIGNATURA: Seguridad en redes

CÓDIGO: CCOM-261

CRÉDITOS: 5 créditos

FECHA: 30 de septiembre de 2013

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
Conocimientos, habilidades, actitudes y valores previos:	**Conocimientos** • Identificar lo que son Redes LAN y WAN • Diseño e implementación de Redes LAN y WAN • Modelos de red y protocolos de comunicación de bajo y alto nivel. **Habilidades** • Creatividad para establecer algo nuevo a problemas planteados. • Innovación para mejorar lo existente en cuestiones algorítmicas. • Trabajo en equipo para enfrentar los retos tecnológicos y sociales • Capacidad de investigar y hacer juicios críticos • Aprender por si mismo • Comunicar lo aprendido • Resolver problemas **Actitudes y valores** • Comprometerse con los demás • Actitud para aprender nuevos conceptos y realizar innovaciones. • Búsqueda de la verdad

	• Trabajar con respeto y empatía con las personas. • Honestidad y responsabilidad. • Liderazgo y humanismo. • Actitud participativa.

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)	**48**	**32**	**80**	**5**
Total	**48**	**32**	**80**	**5**

3. REVISIONES Y ACTUALIZACIONES

Autores:	Miguel Ángel León Chávez José Esteban Torres León
Fecha de diseño:	1 de junio de 2009
Fecha de la última actualización:	27 de septiembre de 2013
Fecha de aprobación por parte de la academia de área	30 de septiembre de 2013
Fecha de aprobación por parte de CDESC-UA	16 de diciembre de 2013
Fecha de revisión del Secretario Académico	*20 de enero de 2014*
Revisores:	Miguel Ángel León Chávez Edna Iliana Tamariz Flores
Sinopsis de la revisión y/o actualización:	En esta revisión se optó por eliminar la unidad 9 “Seguridad en otras redes”, debido al tiempo del curso y porque trataba sobre redes inalámbricas, el cual se considera en la materia que lleva el mismo nombre.

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

Disciplina profesional:	Redes de computadoras y Tecnologías inalámbricas
Nivel académico:	Maestría

Experiencia docente:	Mínima de 2 años
Experiencia profesional:	Mínima de 1 año

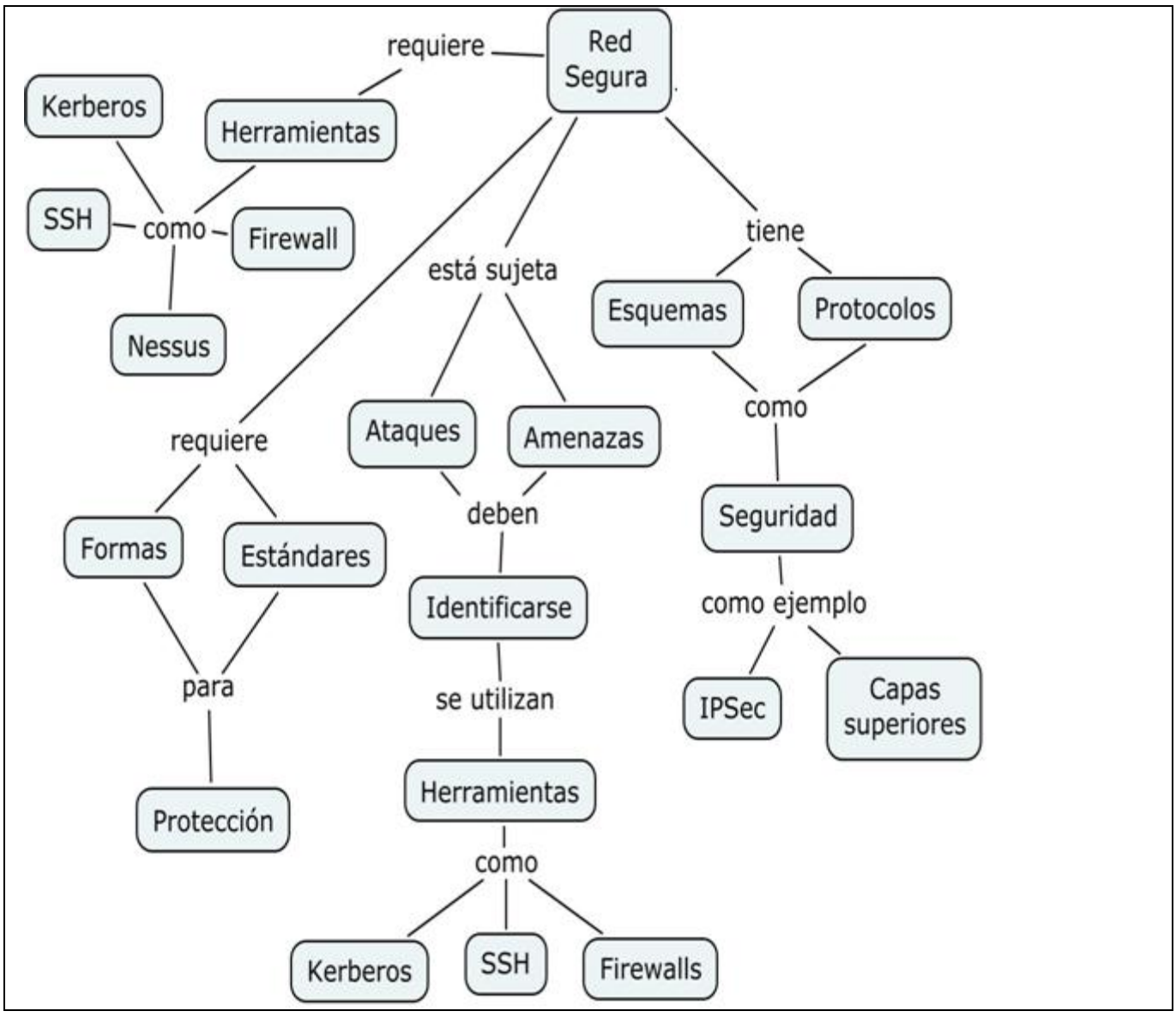
5. OBJETIVOS:

5.1 **General:** 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

5.2 Específicos:

- Definir lo que es seguridad para una red de computadoras, considerando tanto hardware y software, así como las formas de protección como no repudio, autenticación, confidencialidad integridad, y las normas establecidas para que una red sea segura.
- Identificar los ataques y amenazas que hacen que una red sea vulnerable así como las políticas que se deben seguir para establecer la seguridad en la red.
- Identificar, analizar e implementar los esquemas de seguridad en una red de computadoras, así como identificar los servicios y mecanismos de seguridad que hay.
- Identificar, analizar e implementar los protocolos de seguridad que hay en las diferentes capas del modelo TCP/IP.
- Definir e interpretar la seguridad en IPsec, qué ventajas tiene, qué características presenta su arquitectura, así de cómo se usa en la autenticación y como verificación de la integridad.
- Interpretar el protocolo Kerberos, cómo autentifica, cómo permite a usuarios, clientes y servidores autenticarse entre ellos.
- Identificar las principales amenazas de seguridad a las que se enfrentan la Web, qué consideraciones debe tomar y cómo se da seguridad a la capa socket y de transporte.
- Definir lo que es un Firewall, planificar estrategias para proponer el mejor, integrar y configurar para garantizar un nivel de seguridad a una red de computadoras.

6. REPRESENTACIÓN GRÁFICA DE LA ASIGNATURA:



7. CONTENIDO

Unidad	Objetivo Específico	Contenido Temático/Actividades de aprendizaje	Bibliografía	
			Básica	**Complementaria**
1. Introducción a la Seguridad en redes de computadoras	Definir lo que es seguridad para una red de computadoras, considerando tanto hardware y software, así como las formas de protección como no repudio, autenticación, confidencialidad integridad, y las normas establecidas para que una red sea segura.	1.1 Introducción 1.2 Red de computadoras segura 1.3 Formas de protección 1.4 Estándares de protección	1. Migga, J. (2009). A Guide to Computer Network Security. USA: Springer. 2. Cole, E. et al. (2009). Network Security Bible. (2nd edition). USA: Wiley Publishing, Inc.	1. Villalón, A. (2002). Seguridad en Unix y Redes Ver. 2.1. España: GNU Free Documentation License. 2. Pfleeger, C. (2006). Security in Computing. (4th Eedition). USA: Prentice Hall.
2. Retos de la Seguridad en redes de computadoras	Identificar los ataques y amenazas que hacen que una red sea vulnerable así como las políticas que se deben seguir para establecer la seguridad en la red.	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	1. Migga, J. (2009). A Guide to Computer Network Security. USA: Springer. 2. Cole, E. et al. (2009). Network Security Bible. (2nd edition). USA: Wiley Publishing, Inc.	1. Villalón, A. (2002). Seguridad en Unix y Redes Ver. 2.1. España: GNU Free Documentation License. 2. Pfleeger, C. (2006). Security in Computing. (4th Eedition). USA: Prentice Hall.

Unidad	Objetivo Específico	Contenido Temático/Actividades de aprendizaje	Bibliografía	
			Básica	**Complementaria**
		de seguridad 2.6.3 Método para alcanzar objetivos		
3. Seguridad en Redes de computadoras.	Identificar, analizar e implementar los esquemas de seguridad en una red de computadoras, así como identificar los servicios y mecanismos de seguridad que hay.	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 en Redes 3.7.1 Cifrado link to link 3.7.2 Cifrado end to end 3.7.3 SILS ("Standard for Interoperability LAN Security")	1. Migga, J. (2009). A Guide to Computer Network Security. USA: Springer. 2. Cole, E. et al. (2009). Network Security Bible. (2nd edition). USA: Wiley Publishing, Inc.	1. Villalón, A. (2002). Seguridad en Unix y Redes Ver. 2.1. España: GNU Free Documentation License. 2. Pfleeger, C. (2006). Security in Computing. (4th Eedition). USA: Prentice Hall.

Unidad	Objetivo Específico	Contenido Temático/Actividades de aprendizaje	Bibliografía	
			Básica	**Complementaria**
		3.7.4 Retos de la Criptografía en la seguridad en Redes		
4. Protocolos de seguridad en redes de computadoras	Identificar, analizar e implementar los protocolos de seguridad que hay en las diferentes capas del modelo TCP/IP.	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	1. Migga, J. (2009). A Guide to Computer Network Security. USA: Springer. 2. Cole, E. et al. (2009). Network Security Bible. (2nd edition). USA: Wiley Publishing, Inc.	1. Villalón, A. (2002). Seguridad en Unix y Redes Ver. 2.1. España: GNU Free Documentation License. 2. Pfleeger, C. (2006). Security in Computing. (4th Eedition). USA: Prentice Hall.

Unidad	Objetivo Específico	Contenido Temático/Actividades de aprendizaje	Bibliografía	
			Básica	**Complementaria**
		enlace and sobre LANS 4.5.1 Protocolo punto a punto (PPP) 4.5.2 Servicio de autenticación remota de usaurio de dial (RADIUS) 4.5.3 Sistema de control de acceso para controlar el acceso a la terminal (TACACS)		
5. Seguridad en IP (IPSec)	Definir e interpretar la seguridad en IPsec, qué ventajas tiene, qué características presenta su arquitectura, así de cómo se usa en la autenticación y como verificación de la integridad.	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")	1. Migga, J. (2009). A Guide to Computer Network Security. USA: Springer. 2. Cole, E. et al. (2009). Network Security Bible. (2nd edition). USA: Wiley Publishing, Inc.	1. Villalón, A. (2002). Seguridad en Unix y Redes Ver. 2.1. España: GNU Free Documentation License. 2. Pfleeger, C. (2006). Security in Computing. (4th Eedition). USA: Prentice Hall.
6. Herramientas de Seguridad en Red.	Interpretar el protocolo Kerberos, cómo autentifica, cómo	6.1 Concepto de protocolo 6.1 Kerberos 6.1.1 Introducción 6.1.2 La idea de Kerberos	1. Migga, J. (2009). A Guide to Computer Network Security. USA:	1. Villalón, A. (2002). Seguridad en Unix y Redes Ver. 2.1. España: GNU Free

Unidad	Objetivo Específico	Contenido Temático/Actividades de aprendizaje	Bibliografía	
			Básica	**Complementaria**
	permite a usuarios, clientes y servidores autenticarse entre ellos.	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 de dominios 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 6.4.3 Utilización	Springer. 2. Cole, E. et al. (2009). Network Security Bible. (2nd edition). USA: Wiley Publishing, Inc.	Documentation License. 2. Pfleeger, C. (2006). Security in Computing. (4th Eedition). USA: Prentice Hall.
7. Seguridad en Web	Identificar las principales amenazas de seguridad a las que se enfrentan la Web, qué consideraciones	7.1 Introducción 7.2 Consideraciones de Seguridad en Web 7.2.1 Amenazas a la Seguridad en Web 7.2.2 Seguridad del Tráfico Web 7.3 SSL ("Secure Socket Layer")	1. Migga, J. (2009). A Guide to Computer Network Security. USA: Springer. 2. Cole, E. et al.	1. Villalón, A. (2002). Seguridad en Unix y Redes Ver. 2.1. España: GNU Free Documentation License.

Unidad	Objetivo Específico	Contenido Temático/Actividades de aprendizaje	Bibliografía	
			Básica	**Complementaria**
	debe tomar y cómo se da seguridad a la capa socket y de transporte.	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)	(2009). Network Security Bible. (2nd edition). USA: Wiley Publishing, Inc.	2. Pfleeger, C. (2006). Security in Computing. (4th Eedition). USA: Prentice Hall.
8. Firewalls	Definir lo que es un Firewall, planificar estrategias para proponer el mejor, integrar y configurar para garantizar un nivel de seguridad a una red de computadoras.	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 de Paquetes 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	1. Migga, J. (2009). A Guide to Computer Network Security. USA: Springer. 2. Cole, E. et al. (2009). Network Security Bible. (2nd edition). USA: Wiley Publishing, Inc.	1. Villalón, A. (2002). Seguridad en Unix y Redes Ver. 2.1. España: GNU Free Documentation License. 2. Pfleeger, C. (2006). Security in Computing. (4th Eedition). USA: Prentice Hall.

Unidad	Objetivo Específico	Contenido Temático/Actividades de aprendizaje	Bibliografía	
			Básica	Complementaria
		Configuración de Firewalls		

8. CONTRIBUCIÓN DEL PROGRAMA DE ASIGNATURA AL PERFIL DE EGRESO

Asignatura	Perfil de egreso (anotar en las siguientes tres columnas, cómo contribuye la asignatura al perfil de egreso)		
	Conocimientos	**Habilidades**	**Actitudes y valores**
Seguridad en redes	Identificar la seguridad para una red de computadoras. Identificar como participan el hardware y software en la seguridad. Identificar las formas de protección que hay como no repudio, confidencialidad, autenticación, integridad, Conocer las normas que rigen la seguridad en redes	Cuestionar la información y encontrar respuestas respecto a la seguridad en redes de computadoras. Trabajar en equipo Resolver problemas	Buscar el bien común al trabajar en equipo. Ser responsable y ético. Apertura al dialogo. Responsabilidad y solidaridad.
	Identificar los ataques y amenazas que hacen que una red sea vulnerable. Identificar las políticas que se deben debe seguir para establecer la seguridad en la red.	Trabajar en equipo y comunicar puntos de vista sobre la vulnerabilidad de una red en cuanto a ataques y amenazas. Resolver problemas	Buscar el bien común al trabajar en equipo. Ser responsable y ético. Apertura al dialogo. Responsabilidad y solidaridad.
	Identificar los esquemas de seguridad en una red de computadoras. Identificar los servicios y mecanismos de seguridad que hay en las redes.	Crear o establecer un nuevo modelo de servicio de seguridad Trabajar en equipo Resolver problemas	Buscar el bien común al trabajar en equipo. Ser responsable y ético. Apertura al dialogo. Responsabilidad y solidaridad.
	Identificar los protocolos de seguridad que hay en las diferentes capas del modelo	Trabajar en equipo Resolver problemas Mejorar algún protocolo de	Buscar el bien común al trabajar en equipo. Ser responsable y ético.

Asignatura	Perfil de egreso (anotar en las siguientes tres columnas, cómo contribuye la asignatura al perfil de egreso)		
	Conocimientos	**Habilidades**	**Actitudes y valores**
	TCP/IP.	seguridad del mo9delo TCP-IP.	Apertura al dialogo. Responsabilidad y solidaridad.
	Definir la seguridad en IPsec Identificar las ventajas que tiene IPSec. Identificar las características que presenta su arquitectura. Identificar como se usa en la autenticación y verificación la integridad.	Cuestionar la información y encontrar respuestas respecto a la seguridad IPSec.. Trabajar en equipo Resolver problemas	Buscar el bien común al trabajar en equipo. Ser responsable y ético. Apertura al dialogo. Responsabilidad y solidaridad.
	Interpretar el protocolo Kerberos y como se autentifica. Interpretar como permite que usuarios, clientes y servidores se autentican entre ellos.	Trabajar en equipo Resolver problemas Mejorar algunas herramientas de seguridad para redes de computadoras.	Buscar el bien común al trabajar en equipo. Ser responsable y ético. Apertura al dialogo. Responsabilidad y solidaridad.
	Identificar las amenazas a la seguridad que se enfrentan la Web. Interpretar la seguridad en la capa socket y de transporte.	Mejorar la seguridad WEB. Trabajar en equipo Resolver problemas	Buscar el bien común al trabajar en equipo. Ser responsable y ético. Apertura al dialogo. Responsabilidad y solidaridad.
	Definir lo que es un Firewall Planificar estrategias para proponer mejoras a los firewalls. Integrar y configurar un firewall.	Mejorar o establecer un nuevo modelo de firewall. Trabajar en equipo Resolver problemas	Buscar el bien común al trabajar en equipo. Ser responsable y ético. Apertura al dialogo. Responsabilidad y solidaridad.


BENEMERITA
Vicerrectoría
de DOCENCIA
dgés

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

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 el proyecto final.

10. ORIENTACIÓN DIDÁCTICO-PEDAGÓGICA. ***(Enunciada de manera general para aplicarse durante todo el curso)***

Estrategias y Técnicas de aprendizaje-enseñanza	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 • Equipo de laboratorio

11. CRITERIOS DE EVALUACIÓN

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

13. Anexar (copia del acta de la Academia y de la CDESC- UA con el Vo. Bo. del Secretario Académico)