UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

COORDINACIÓN GENERAL DE FORMACIÓN BÁSICA
COORDINACIÓN GENERAL DE FORMACIÓN PROFESIONAL Y VINCULACIÓN UNIVERSITARIA
PROGRAMA DE UNIDAD DE APRENDIZAJE

I. DATOS DE IDENTIFICACIÓN

1. Unidad Académica: Facultad de Ingeniería, Mexicali, Facultad de Ingeniería, Arquitectura y Diseño, Ensenada y Facultad de Ciencias Químicas e Ingeniería, Tijuana.

2. Programa Educativo: Ingeniero en Computación

3. Plan de Estudios: 2020-1

4. Nombre de la Unidad de Aprendizaje: Gestión y Seguridad en Redes

5. Clave: 36298

6. HC: 01 **HL:** 02 **HT:** 01 **HPC:** 00 **HCL:** 00 **HE:** 01 **CR:** 05

7. Etapa de Formación a la que Pertenece: Terminal

8. Carácter de la Unidad de Aprendizaje: Obligatoria

9. Requisitos para Cursar la Unidad de Aprendizaje: Redes de Computadoras

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA
REGISTRADO
17 OCT 2019
REGISTRADO
COORDINACIÓN GENERAL DE FORMACIÓN BÁSICA

Equipo de diseño de PUA

Manuel Jiménez Orozco
Eduardo Ceseña Beltrán
Mabel Vázquez Briseño

Vo.Bo. de Subdirectores de Unidades Académicas

Alejandro Mungaray Moctezuma
Humberto Cervantes de Ávila
Rocío Alejandra Chávez Santoscoy

Fecha: 17 de octubre de 2019

II. PROPÓSITO DE LA UNIDAD DE APRENDIZAJE

La importancia de la gestión y la seguridad en redes consiste en lograr la operación eficiente de los recursos compartidos y conectividad de una organización.
La asignatura provee los conocimientos y habilidades para que el alumno conozca los principios fundamentales de la seguridad y administración de redes de cómputo y la trasmisión de datos actuales que le permitan prevenir y mitigar problemas de interconexión y comunicación de distintas organizaciones.
El curso de Gestión y seguridad en redes se encuentra ubicado en la etapa terminal, con carácter obligatorio. Pertenece al área de conocimiento Ingeniería aplicada.

III. COMPETENCIA DE LA UNIDAD DE APRENDIZAJE

Administrar sistemas de redes de computadoras de forma eficiente, utilizando normas, herramientas de configuración, monitoreo y seguridad de la red, para lograr la comunicación de datos óptima y uso eficiente de los recursos de cómputo, con actitud proactiva y honesta.

IV. EVIDENCIA(S) DE DESEMPEÑO

Reporte técnico sobre estrategia de seguridad a implementar en un caso de estudio particular.

V. DESARROLLO POR UNIDADES

UNIDAD I. Principios generales de seguridad y administración en redes de cómputo

Competencia:
Distinguir los conceptos básicos de seguridad y administración de redes, mediante una investigación documental en el ramo de telecomunicaciones, electrónica y estándares internacionales, para comprender su procedimiento de implementación dentro de la comunicación de datos, con actitud crítica y responsable.

Contenido: **Duración:** 1 hora

1.1 Principios básicos de seguridad
- 1.1.1 Integridad, disponibilidad y confiabilidad
- 1.1.2 Políticas de seguridad para redes de cómputo
- 1.1.3 Autenticación, Autorización, Accounting (AAA)

1.2 Principios básicos de administración

UNIDAD II. Sistemas operativos de red

Competencia:
Distinguir las características de los distintos sistemas operativos de red, administrando sus funcionalidades con base a buenas prácticas según sus respectivas listas de verificación, para comprender su funcionamiento y uso en redes de computadoras, con actitud analítica y responsable.

Contenido: **Duración:** 2 horas

2.1 Funciones de sistemas operativos de red
- 2.1.1 Windows
- 2.1.2 Linux
- 2.1.3 Otros

2.2 Listas de verificación de funciones de s.o. de red

UNIDAD III. Seguridad en redes de datos

Competencia:
Identificar los problemas de seguridad en redes de computadoras, mediante el análisis de su clasificación y procesos, para determinar los mecanismos de seguridad adecuados dentro de alguna organización, con responsabilidad y actitud crítica.

Contenido: **Duración:** 6 horas

3.1 Vulnerabilidades en redes de datos
3.2 Mecanismos de seguridad en redes de datos
3.2.1 STP, DoS, IP spoofing
3.4 Criptografía en la seguridad en redes
3.4.1 Certificados de SSL
3.4.2 VPN
3.5 Firewalls
3.5.1 NetFilter

UNIDAD IV. Tareas de administración de una red

Competencia:
Gestionar una red de computadoras, utilizando técnicas de administración de servicios adecuadas, para aplicar herramientas de administración en futuras implementaciones de redes, con eficacia y responsabilidad.

Contenido: **Duración:** 7 horas

4.1 Monitoreo de redes
- 4.1.1 Bitácoras de evento
- 4.1.2 SNMP

4.2 Configuraciones básicas de dispositivos
- 4.2.1 Conmutadores
- 4.2.2 Servidores
- 4.2.3 Workstations

4.3 Administración de servicios de redes
- 4.3.1 Servidor HTTP
- 4.3.2 Servidor FTP
- 4.3.3 Servidor de bases de datos
- 4.3.3 Servidor de bitácoras

VI. ESTRUCTURA DE LAS PRÁCTICAS DE TALLER				
No. de Práctica	**Competencia**	**Descripción**	**Material de Apoyo**	**Duración**
UNIDAD I				
	Identificar las características básicas de las herramientas de seguridad de redes, mediante una investigación documental y la argumentación de sus conceptos, para comprender la importancia de seguridad en redes, con actitud investigadora y proactiva.	Examina los conceptos básicos de seguridad mediante un debate grupal. Entrega un reporte de definiciones en consenso	Computadora con acceso a Internet.	4 horas
UNIDAD II				
2	Describir las características de los sistemas operativos de red, mediante su instalación y análisis, para adquirir las bases necesarias sobre el funcionamiento de los mismos, con actitud crítica e investigadora.	Investiga las características de un sistema operativo de red. Entregar un reporte con el siguiente formato: Introducción, metodología, resultados, conclusiones y referencias	Computadora con acceso a Internet.	4 horas
UNIDAD III				
3	Identificar las vulnerabilidades de los sistemas operativos de red, mediante el uso de una herramienta de análisis, para distinguir problemas potenciales de seguridad, con actitud reflexiva y tenacidad.	Investiga el tema de vulnerabilidades de sistema. Entrega un reporte con el siguiente formato: Introducción, metodología, resultados, conclusiones y referencias	Computadora con acceso a Internet.	4 horas
4	Aplicar mecanismos de seguridad, mediante la configuración y activación de una herramienta de simulación de tipos de redes, para implementarlo en alguna organización en el futuro, con responsabilidad y honestidad.	Investiga sobre mecanismos de seguridad en redes. Entrega un reporte con el siguiente formato: Introducción, metodología, resultados, conclusiones y referencias	Computadora con acceso a Internet.	4 horas

VI. ESTRUCTURA DE LAS PRÁCTICAS DE LABORATORIO				
No. de Práctica	**Competencia**	**Descripción**	**Material de Apoyo**	**Duración**
UNIDAD II				
1	Realizar la instalación de un sistema operativo de red, siguiendo manuales adecuados y requerimientos definidos, para verificar sus funcionalidades, con actitud crítica e investigadora	Instala un sistema operativo de red. Verifica la funcionalidad con la que se instaló el sistema operativo. Ajusta la instalación de acuerdo a los requerimientos definidos. Entrega un reporte con el siguiente formato: Introducción, metodología, resultados, conclusiones y referencias	Computadora con acceso a Internet. Sistema operativo de red.	2 horas
UNIDAD III				
2	Instalar herramientas de análisis de vulnerabilidades en sistemas operativos de red, en apego a los lineamientos de seguridad existentes, para distinguir problemas potenciales de seguridad, con actitud reflexiva y tenacidad.	Instala y ejecuta un sistema de análisis de vulnerabilidades en el sistema operativo de red. Entrega un reporte con el siguiente formato: Introducción, metodología, resultados, conclusiones y referencias.	Computadora con acceso a Internet Software de análisis de vulnerabilidades.	2 horas
3	Instalar una herramienta de simulación de redes, siguiendo los manuales adecuados, para aplicar mecanismos de seguridad, con responsabilidad y honestidad.	Resuelve loops de interconexión. Configura y activa un estándar basado en STP. Entrega un reporte con el siguiente formato: Introducción, metodología, resultados, conclusiones y referencias	Computadora con acceso a Internet. Estándares de STP.	2 horas
4	Aplicar un mecanismo de seguridad, mediante la generación de un componente de seguridad, para	Crea un certificado de seguridad utilizando SSL. Entrega un reporte en el que se	Computadora con acceso a Internet. OpenSSL	2 horas

	implementarlo en alguna organización en el futuro, con responsabilidad y honestidad.	incluya el certificado generado. El reporte debe tener el siguiente formato: Introducción, metodología, resultados, conclusiones y referencias.		
5		Implementa un esquema VPN en arquitectura cliente-servidor utilizando el certificado de seguridad correspondiente e instalándolo en OpenVPN.	Computadora con acceso a Internet. OpenSSL OpenVPN	4 horas
6	Experimentar las capacidades de filtrado de tráfico, implementando reglas, para permitir o denegar la comunicación, con iniciativa y responsabilidad.	Implementa un conjunto de reglas mediante la herramienta de software adecuada para simular un Firewall.	Computadora con acceso a Internet IPTables	2 horas
7		Implementa un conjunto de reglas para simular un Firewall mediante traducción de direcciones de red.	Computadora con acceso a Internet IPTables	4 horas
UNIDAD IV				
8	Administrar de forma eficiente diferentes servicios de redes, mediante la configuración correcta de las herramientas, para asegurar el funcionamiento adecuado de cada una de las tecnologías, con visión e integridad.	Implementa un servidor de bitácoras utilizando herramientas de bitácoras tales como syslog-ng para documentar el funcionamiento del sistema y posibilitar el seguimiento de errores. Entrega un reporte con el siguiente formato: Introducción, metodología, resultados, conclusiones y referencias	Computadora con acceso a Internet. Syslog-ng, rsyslog	2 horas
9		Configura una herramienta basada en SNMP. Demuestra que obtuvieron resultados de administración de la red con la herramienta instalada. Entrega un reporte con el siguiente formato: Introducción,	Computadora con acceso a Internet. Herramienta basada en SNMP	4 horas

		metodología, resultados, conclusiones y referencias.		
10		Configura el servicio HTTP cumpliendo con requisitos de seguridad, siguiendo alguna de las estrategias de seguridad de dicho protocolo. Entrega un reporte con el siguiente formato: Introducción, metodología, resultados, conclusiones y referencias	Computadora con acceso a Internet. Servidor HTTP.	4 horas
11		Configura el servicio FTP, siguiendo estrategias de seguridad adecuada para el protocolo. Entregar un reporte con el siguiente formato: Introducción, metodología, resultados, conclusiones y referencias	Computadora con acceso a Internet. Servidor FTP.	2 horas
12		Configura el servicio MySQL cumpliendo con requisitos de seguridad, mediante estrategias adecuadas. Entrega un reporte con el siguiente formato: Introducción, metodología, resultados, conclusiones y referencias	Computadora con acceso a Internet. Servidor MySQL.	2 horas

VII. MÉTODO DE TRABAJO

Encuadre: El primer día de clase el docente debe establecer la forma de trabajo, criterios de evaluación, calidad de los trabajos académicos, derechos y obligaciones docente-alumno.

Estrategia de enseñanza (docente)

- Exposición de los temas por parte del maestro
- Planteamiento y resolución de algún caso real
- Resolución de problemas en clase

Estrategia de aprendizaje (alumno)

- Resolución de problemas en clase
- Resolución de problemas de tarea
- Resolución de algún caso real
- Investigación de algún tema relacionado con el material del curso
- Configuración y utilización de herramientas de administración y seguridad de redes

VIII. CRITERIOS DE EVALUACIÓN

La evaluación será llevada a cabo de forma permanente durante el desarrollo de la unidad de aprendizaje de la siguiente manera:

Criterios de acreditación

- Para tener derecho a examen ordinario y extraordinario, el estudiante debe cumplir con los porcentajes de asistencia que establece el Estatuto Escolar vigente.
- Calificación en escala del 0 al 100, con un mínimo aprobatorio de 60.

Criterios de evaluación

- 2 Evaluaciones parciales……30 %
- Tareas/Investigaciones ……..20 %
- Reportes Laboratorios/Taller…….……20 %
- Evidencia de desempeño……30 %
  (Reporte técnico sobre estrategia de seguridad a implementar en un caso de estudio particular.)

Total…….. 100%

IX. REFERENCIAS

Básicas	Complementarias
Limoncelli, T. A., Hogan, C. J., y Chalup, S. R. (2016). *The practice of system and network administration*. Estados Unidos: Pearson Education. Stallings, W. (2017). *Network security essentials: applications and standards*. (6ª ed.). Inglaterra: Pearson. Terán, D.M. (2018). *Administración y seguridad en redes y computadoras*. México: Alfaomega	Cisco Networking Cisco Networking Academy. (2018). *CCNA Cybersecurity Operations Lab Manual* (6ª ed.). Nueva York, Estados Unidos: Cisco Press. Stallings, W. (2018) *Data & Computer Communications.* (10ª ed.) Estados Unidos: Prentice Hall [clásica] Universitat de Valencia (s.f.). *Manuales de Referencia CISCO*. Recuperado de https://www.uv.es/uvweb/servicio-informatica/es/telefonia-ip/manuales/manuales-cisco-1285904417859.html

X. PERFIL DEL DOCENTE

El docente debe contar con título de ingeniero en computación o área afín preferentemente contar con posgrado en el área de ciencias experimentales. Con al menos dos años de experiencia en la industria de telecomunicaciones o en la docencia. Ser una persona proactiva y comprometida con el aprendizaje significativo de los estudiantes