

1. Datos Generales de la asignatura

Nombre de la asignatura:	Administración de Servicios de Red ₂
Clave de la asignatura:	SED-1703
SATCA¹:	<u>(2 - 3 - 5)</u>
Carrera:	Ingeniería en Tecnologías de la Información y Comunicaciones Ingeniería en Sistemas Computacionales Ingeniería Informática

2. Presentación

Caracterización de la asignatura
<p>La asignatura de Administración de Servicios de Red aporta al perfil del Ingeniero en Sistemas Computacionales la habilidad de utilizar las herramientas de software y hardware que le permitan vigilar el comportamiento de un sistema en red, así como la capacidad de emplear los recursos necesarios para administrar eficientemente la seguridad y la prestación de estos servicios</p> <p>Esta asignatura agrupa los conocimientos necesarios para realizar eficientemente las tareas administrativas de una red</p> <p>Esta es una asignatura que requiere la aplicación de los conocimientos previos de administración de Sistemas y de diseño de redes</p>
Intención didáctica
<p>La asignatura está integrada por cinco unidades, dentro de las cuales el alumno conocerá la manera de administrar los servicios de red más comunes, analizando de manera particular cada uno de ellos.</p> <p>En las actividades de aprendizaje sugeridas, se propone la formalización y aplicación de los conceptos aprendidos a través de diversas prácticas de laboratorio y la resolución de diversas situaciones concretas.</p> <p>En el transcurso de las actividades programadas es muy importante que el estudiante aprenda a aplicar de manera concreta cada uno de los conceptos cubiertos, de forma que desarrolle hábitos de trabajo enfocados hacia la seguridad y confiabilidad de los servicios que presta</p>

¹ Sistema de Asignación y Transferencia de Créditos Académicos

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico de Morelia, del 9 al 13 de enero de 2012	Los miembros de la línea de investigación de Seguridad y Administración de la Información	Diseño del módulo de especialidad
Instituto Tecnológico de Morelia, 1 de julio de 2015.	Juan Manuel García García Anastacio Antolino Hernandez Heberto Ferreira Juan Jesús Ruiz lagunas	Diseño Curricular basado en Competencias del Módulo.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Este curso proporciona a los estudiantes de este módulo de especialidad las habilidades necesarias para administrar sistemas de redes para protegerlos de cualquier riesgo interno o externo, y les ofrece las características más actuales de las medidas de seguridad, capacidades y riesgos asociados a los sistemas y servicios de red más comúnmente empleados en la actualidad.

5. Competencias previas

<ul style="list-style-type: none"> • Tener y aplicar habilidades de programación y diseño de redes. • Capacidad de toma de decisiones. • Conocer los elementos esenciales de configuración de servicios de red. • Conocer los conceptos de administración de sistemas. • Conocimiento de administración del sistema operativo LINUX.

6. Temario

No.	Temas	Subtemas
1	Diseño y Construcción de una red de área local.	1. Red interna, DMZ y seguridad perimetral. 2. Implementación usando redes virtuales en VMWare
2	Implementación de un firewall y proxy transparente	1. Enmascaramiento y NAT con IPTables.



		2. Filtraje de contenido con Squid y SquidGuard.
3	Implementación de servicios en Zona DesMilitarizada (DMZ)	<ol style="list-style-type: none"> 1. Implementación de un servidor de resolución de nombres con BIND. 2. Implementación de servicio Web con Apache. 3. Implementación de servicio de correo con Exim. 4. Configuración de red interna para acceso a servicios mediante IPTables. 5. Configuración de clientes de correo de Outlook
4	Implementación de acceso remoto mediante IPSec	<ol style="list-style-type: none"> 1. Configuración de IPSec mediante OpenSwan. 2. Configuración de túnel para conexión de red remota y red local

7. Actividades de aprendizaje de los temas

Nombre de tema	
Diseño y Construcción de una red de área local	
Competencias	Actividades de aprendizaje
<p>Específica(s):</p> <ul style="list-style-type: none"> - Conocer y explotar las diversas características de ambientes de red bajo sistemas operativos Windows y Linux <p>Genéricas:</p> <ul style="list-style-type: none"> - Construcción de Redes de Area Local 	<ol style="list-style-type: none"> 1. Instalación de Servicios en Sistemas Operativos Linux. 2. Instalación de Linux en servidores reales y virtuales 3. Implementación de un firewall, usando iptables en ambiente Linux. 4. Diseño e implementación de toologias seguras en ambientes reales y virtuales
Nombre de tema	
Implementación de un firewall y proxy transparente	
Competencias	Actividades de aprendizaje
<p>Específica(s):</p> <ul style="list-style-type: none"> - Podrá instalar e implementar políticas de administración de tráfico usando un firewall - Podrá instalar e implementar políticas de tráfico en proxys transparentes para la red local <p>Genéricas:</p> <ul style="list-style-type: none"> - Conocer y construir un firewall y proxy's transparentes para la administración del tráfico desde y hacia la red local, asi como desde y hacia internet 	<ol style="list-style-type: none"> 1. Conocer el funcionamiento de un firewall 2. Conocer los distintos tipos de proxys. 3. Implementar las 3 zonas de un firewall con trafico controlado entre ellas 4. Implementar un proxy normal en red local. 5. Implementar un proxy transparente en red local.
Nombre de tema	
Implementación de servicios en Zona DesMilitarizada (DMZ)	

Competencias	Actividades de aprendizaje
<p>Específica(s):</p> <ul style="list-style-type: none"> - Implementar un firewall dentro del servidor, para asegurar el nivel de integridad de los servicios implementados - Implementar políticas de uso y llevar a cabo auditorias a dichos servicios. <p>Genéricas:</p> <ul style="list-style-type: none"> - Implementar el nivel de seguridad requerido por los servidores en la zona Desmilitarizada. 	<ol style="list-style-type: none"> 1. Implementar políticas de seguridad en los servidores y servicios instalados. 2. Confinamiento de procesos. 3. Implementación de herramientas de monitoreo remoto y local a los servicios instalados 4. Establecer procedimientos de auditoria a dichos servicios.
<p>Nombre de tema</p> <p>Implementación de acceso remoto mediante IPsec</p>	
Competencias	Actividades de aprendizaje
<p>Específica(s):</p> <ul style="list-style-type: none"> - Implementar mecanismos de administración remota de manera intra-red. - Implementar mecanismos de administración remota inter-redes. <p>Genéricas:</p> <ul style="list-style-type: none"> - Conocera e implementara mecanismos de administración remota hacia. 	<ol style="list-style-type: none"> 1. Implementación de herramientas de sesiones remotas seguras. 2. Implementación de redes privadas virtuales seguras.

8. Práctica(s)

1. Todo el contenido se llevara a cabo de manera práctica dentro de los equipos de computo de los estudiantes, asi como en los servidores del laboratorio de gestión informática.

SEP

SECRETARÍA DE
EDUCACIÓN PÚBLICA



TECNOLÓGICO NACIONAL DE MÉXICO

9. Proyecto de asignatura

Diseño, implementación y puesta a punto de una red propuesta por el docente, que incluya todos los elementos vistos en el semestre, la cual incluya firewall, servidores, red local y conexiones de red privada virtual.

10. Evaluación por competencias

Instalar y configurar diversos servicios en ambiente Linux.

Realizar comparativos sobre el desempeño de las mismas herramientas en diversas plataformas y configuraciones.

Configurar y administrar un servidor con servicios seguro.

11. Fuentes de información

[1] S.SHAH; W.SOYINKA. "Linux Administration", Mac Graw Hill, 2005.

[2] H.BRELSFORD. "Windows 2000 Server" Arrayan, 2007.

[3] G.MARK "Commands, Editors, and shell Programming "

[4] TANENBAUM A. (2003). Redes de computadoras. Prentice Hall. Cuarta ed. Mexico.

[5] Página dedicada a la seguridad desarrollada por Universidad Nacional Autónoma de México.

<http://www.seguridad.unam.mx>.

[6] Red Hat Enterprise Linux (RHEL), (2008), Deployment Guide 5.1, Red Hat Inc, USA.

[https://www.redhat.com/docs/manuals/enterprise/RHEL-5-manual/en-US/RHEL510/Deployment Guide/index.html](https://www.redhat.com/docs/manuals/enterprise/RHEL-5-manual/en-US/RHEL510/Deployment%20Guide/index.html)

[7] Scarfone K., Mell P., (2007) Guide to Intrusion Detection and Prevention

Systems (IDPS), NIST.

<http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf>

[8] Wack J., Cutler K., y Pole J. (2002), Guidelines on Firewalls and Firewall Policy, NIST, Computer Security Division.

<http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf>

[9] Ferrer J., Fernández-Sanguino J., (s.f.), El sistema operativo GNU/Linux y sus herramientas libres en el mundo de la seguridad: estudio del estado del arte.

<http://mmc.igeofcu.unam.mx/LuCAS/Presentaciones/200103hispalinux/ferrer/pdf/seguridad-y-sw-libre v1.0.pdf>