PROGRAMA DE ESTUDIO POR COMPETENCIAS
SEGURIDAD EN REDES

I. IDENTIFICACIÓN DEL CURSO

<table>
<tr><td colspan="7">Espacio Educativo: Facultad de Ingeniería</td></tr>
<tr><td colspan="3">Licenciatura: Ingeniería en Computación

Año de aprobación por el Consejo Universitario:</td><td colspan="4">Área de docencia: Redes</td></tr>
<tr><td colspan="2">Aprobación por los H.H. Consejos Académico y de Gobierno</td><td>Fecha:</td><td colspan="2">Programa elaborado por:
Dra. Ma. Enriqueta Varilla Pérez
Ing. Alejandro Hernández Arriaga.
Ing. Alvaro Alfonso Lugo Avila
Ing. José Antonio Hernández Flores.
Ing. Juan Carlos Escobar González.
Ing. Mauricio Salinas Nava.
Ing. Pedro Pallares Jiménez.
Ing. Samuel Rosales Becerril.
Ing. Sergio Jonatan Reyes Pérez.
M. en C.C. Juan Carlos Matadamas Gómez.
Mtro. José Antonio Alvarez Lobato.
Mtro. Juan Lebario Menchaca.</td><td colspan="2">Programa revisado por:
Dra. Ma. Enriqueta Varilla Pérez
Ing. Alejandro Hernández Arriaga.
Ing. Alvaro Alfonso Lugo Avila
Ing. José Antonio Hernández Flores.
Ing. Juan Carlos Escobar González.
Ing. Mauricio Salinas Nava.
Ing. Pedro Pallares Jiménez.
Ing. Samuel Rosales Becerril.
Ing. Sergio Jonatan Reyes Pérez.
M. en C.C. Juan Carlos Matadamas Gómez.
Mtro. José Antonio Alvarez Lobato.
Mtro. Juan Lebario Menchaca.</td></tr>
<tr><td colspan="4"></td><td colspan="2">Fecha de elaboración : 9 Septiembre del 2009</td></tr>
<tr><td>Clave</td><td>Horas de teoría</td><td>Horas de práctica</td><td>Total de horas</td><td>Créditos</td><td>Tipo de curso</td><td>Núcleo de formación</td></tr>
<tr><td>L41044</td><td>4</td><td>1</td><td>5</td><td>9</td><td>Curso</td><td>Sustantivo</td></tr>
<tr><td colspan="4">Unidad de Aprendizaje Antecedente
Administración de Redes
Análisis y Diseño de Redes</td><td colspan="3">Unidad de Aprendizaje Consecuente
Ninguna</td></tr>
</table>

Programas educativos o espacios académicos en los que se imparte: Facultad de Ingeniería, UAP Atlacomulco, UAP Ecatepec, UAP Texcoco, UAP Valle de Chalco, UAP valle de México, UAP Valle de Teotihuacan, UAP Zumpango.

II. PRESENTACIÓN DEL PROGRAMA

Las actividades que se realizan en el área de Seguridad en Redes, demandan actuar con un alta capacidad de análisis, rapidez, precisión, corto tiempo y responsabilidad ante incidentes de seguridad, la unidad de aprendizaje proporcionará al estudiante de Ingeniería en computación las bases para realizar el diseño, implementación y el mantenimiento de la seguridad de distintas redes computacionales con las características anteriormente descritas; fomentará en el alumno la actualización e investigación constante y continua en tópicos de seguridad, en un campo tan cambiante como lo es la seguridad en cómputo y el manejo de la misma en las nuevas tecnologías.

III. LINEAMIENTOS DE LA UNIDAD DE APRENDIZAJE

DEL DOCENTE	DEL DISCENTE
▪ Establecer las políticas del curso. ▪ Respetar el horario del curso y la forma de evaluarlo. ▪ Cumplir el temario y el número de horas asignadas al curso. ▪ Asesorar y guiar el trabajo de las unidades de aprendizaje. ▪ Retroalimentar el trabajo de los alumnos. ▪ Fomentar la creatividad en los alumnos a través del desarrollo de proyectos. ▪ Preparar material y utilizar estrategias que permitan alcanzar los propósitos del curso. ▪ Asistir a todas las sesiones y estar a tiempo. ▪ Mantener el control dentro del aula y fomentar el trabajo en equipo. ▪ Mantener una actitud de respeto y tolerancia a los discentes.	▪ Asistir puntualmente ▪ Contar con la asistencia establecida en el reglamento de Facultades: o 80% para examen ordinario o 60% para examen extraordinario o 30% para examen a titulo de suficiencia ▪ Cumplir con las actividades encomendadas entregando con calidad en tiempo y forma los trabajos requeridos ▪ Participar activa y críticamente en el proceso de enseñanza-aprendizaje

IV. PROPÓSITO DE LA UNIDAD DE APRENDIZAJE

Que los alumnos sean capaces de realizar el diseño, implementación y el mantenimiento de la seguridad de distintas redes computacionales.

V. COMPETENCIAS GENÉRICAS

Alta capacidad para analizar y sintetizar la operación de redes de computadoras.
Buen conocimiento en el manejo de software para diseño y administración de redes.
Alta capacidad de realizar trabajo de investigación en equipo.
Facilidad y gusto para usar herramientas matemáticas, estadísticas e informáticas para el diseño, implementación y mantenimiento de la seguridad de redes computacionales.

VI. ÁMBITOS DE DESEMPEÑO PROFESIONAL

Ingeniero de seguridad en cómputo y telecomunicaciones tanto, en empresas públicas como privadas.

Investigación de nuevas soluciones para la seguridad en redes de computadoras en los entornos laborales.

Docencia a cualquier nivel de aprendizaje escolarizado.

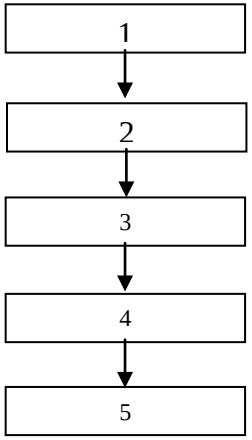
VII. ESCENARIOS DE APRENDIZAJE

Aula, sala de cómputo, laboratorio, taller.

VIII. ESTRUCTURA DE LA UNIDAD DE APRENDIZAJE

1.-Fundamentos de la seguridad en redes.
2.-Arquitectura de seguridad del modelo de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection).
3.- Criptografía y **autenticación**.
4.- Arquitecturas de componentes de seguridad (Firewalls, IDS, Analizadores de contenido).
5.- Hardening a servidores y dispositivos de red.

SECUENCIA DE LA UNIDAD



IX. DESARROLLO DE LA UNIDAD DE APRENDIZAJE

<table>
<tr><td rowspan="2">UNIDAD DE COMPETENCIA I</td><td colspan="4">ELEMENTOS DE COMPETENCIA</td></tr>
<tr><td>Conocimientos</td><td>Habilidades</td><td>Actitudes</td><td>Valores</td></tr>
<tr><td>Identifica los elementos de seguridad y el ciclo de vida de las operaciones y las políticas de seguridad.</td><td>Definición de la Seguridad en Redes.
Conceptos asociados a la Seguridad de redes.
Amenazas a la seguridad de la red.
Las políticas de seguridad.</td><td>Razonamiento lógico.
Capacidad de abstracción.
Capacidad de identificación de los componentes de seguridad de las redes.</td><td>Receptiva
Analítica
Prepositiva</td><td>Cumplir con las actividades asignadas.
Respetar al docente y a los compañeros mediante un comportamiento socialmente aceptable.</td></tr>
<tr><td colspan="2">Estrategias Didácticas:
Lecturas de casos, investigación por los estudiantes. Uso de software de libre distribución para análisis de trafico en la red.</td><td colspan="2">RECURSOS REQUERIDOS
Pizarrón, pintarrones.
Computadoras, servidores.
Acceso a Internet</td><td>TIEMPO DESTINADO
10 Hrs.</td></tr>
<tr><td rowspan="2">CRITERIOS DE DESEMPEÑO I</td><td colspan="3">EVIDENCIAS</td></tr>
<tr><td colspan="2">DESEMPEÑO / PRODUCTOS</td><td>CONOCIMIENTOS</td></tr>
<tr><td>Identificación de los elementos de seguridad de redes.</td><td colspan="2">Respuesta adecuada a los cuestionamientos sobre características de los elementos y las políticas de seguridad de redes.</td><td>Comprensión y elaboración de las políticas de seguridad, así como de los elementos de seguridad en redes.</td></tr>
</table>

<table>
<tr><td rowspan="2">UNIDAD DE COMPETENCIA II</td><td colspan="4">ELEMENTOS DE COMPETENCIA</td></tr>
<tr><td>Conocimientos</td><td>Habilidades</td><td>Actitudes</td><td>Valores</td></tr>
<tr><td>Arquitectura de seguridad del modelo de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection)</td><td>Ataques a la seguridad.
Mecanismos de seguridad.
Servicios de seguridad.
Normas ISO 2700:2005 Gestión de la Seguridad de la Información.</td><td>Capacidad de abstracción.
Razonamiento sistémico</td><td>Dedicación
Esfuerzo
Puntualidad</td><td>Cumplir con las actividades asignadas.
Respetar al docente y a los compañeros mediante un comportamiento socialmente aceptable.</td></tr>
<tr><td colspan="2">Estrategias Didácticas:
Lectura de normas, investigaciones extraclase.</td><td colspan="2">RECURSOS REQUERIDOS

Pizarrón, pintarrones.
Computadora.
Normas ISO 2700:2005</td><td>TIEMPO DESTINADO

15 Hrs</td></tr>
<tr><td rowspan="2">CRITERIOS DE DESEMPEÑO II</td><td colspan="3">EVIDENCIAS</td></tr>
<tr><td colspan="2">DESEMPEÑO / PRODUCTOS</td><td>CONOCIMIENTOS</td></tr>
<tr><td>Rapidez de análisis y síntesis para identificar las características de la arquitectura de seguridad de OSI y de las Normas ISO2700:2005</td><td colspan="2">Manejo de la terminología de seguridad de OSI y de ISO 2700:2005</td><td>Arquitectura de seguridad del modelo de Interconexión de Sistemas Abiertos y de ISO 2700:2005.</td></tr>
</table>

<table>
<tr><td rowspan="2">UNIDAD DE COMPETENCIA III</td><td colspan="4">ELEMENTOS DE COMPETENCIA</td></tr>
<tr><td>Conocimientos</td><td>Habilidades</td><td>Actitudes</td><td>Valores</td></tr>
<tr><td>Adquirir los conocimientos generales sobre criptografía y autenticación para aplicarlas a la seguridad en redes.</td><td>Criptografía

Autenticación</td><td>Capacidad de abstracción y análisis.
Búsqueda, instalación y configuración de software de seguridad.
Manejo de terminología</td><td>Dedicación
Esfuerzo
Puntualidad.</td><td>Cumplir con las actividades asignadas.
Respetar al docente y a los compañeros mediante un comportamiento socialmente aceptable</td></tr>
<tr><td colspan="2">Estrategias Didácticas:
Investigaciones extraclase, búsqueda, instalación, configuración y puesta en funcionamiento de software de libre distribución,</td><td colspan="2">RECURSOS REQUERIDOS

Pizarrón, pintarrones.
Computadora.
Acceso a Internet</td><td>TIEMPO DESTINADO

15 Hrs.</td></tr>
<tr><td rowspan="2">CRITERIOS DE DESEMPEÑO III</td><td colspan="4">EVIDENCIAS</td></tr>
<tr><td colspan="2">DESEMPEÑO / PRODUCTOS</td><td colspan="2">CONOCIMIENTOS</td></tr>
<tr><td>Entrega de trabajos extraclase</td><td colspan="2">Configuración de equipos y software para criptografía y autenticación.
Reporte de actividades extraclase</td><td colspan="2">En software y dispositivos fiscos para realizar criptografía y autenticación.</td></tr>
</table>

UNIDAD DE COMPETENCIA IV	ELEMENTOS DE COMPETENCIA			
	Conocimientos	**Habilidades**	**Actitudes**	**Valores**
Componentes de seguridad: Firewalls, Detectores de Intrusos, Prevensores de Intrusos, Analizadores de contenido, Anti-Spam.	Zona Militarizda y Desmilitarizada Arquitectura de Firewalls, Sistemas Detectores y Prevensores de intrusos (IDS). Componentes de Analizadores de contenidos y Anti-Spam	Capacidad de abstracción y análisis. Búsqueda, instalación y configuración de software de seguridad. Manejo de terminología	Dedicación Esfuerzo Puntualidad	Cumplir con las actividades asignadas. Respetar al docente y a los compañeros mediante un comportamiento socialmente aceptable

Estrategias Didácticas:	**RECURSOS REQUERIDOS**	**TIEMPO DESTINADO**
Lecturas de casos, investigación por los estudiantes, exposición de conocimientos teóricos por parte del docente y solución de ejercicios en clase con la participación de los alumnos, instalación de firewall y analizador de contenidos en entorno Linux	Pizarrón, pintarrones. Computadora. Servidores de cómputo Acceso a Internet	15 hrs.

CRITERIOS DE DESEMPEÑO IV	EVIDENCIAS	
	DESEMPEÑO / PRODUCTOS	**CONOCIMIENTOS**
Entrega de trabajos extraclase	Configuración de equipos y software para firewalls y analizadores de contenidos. Reporte de actividades extraclase	En software y dispositivos fiscos de seguridad.

UNIDAD DE COMPETENCIA V	ELEMENTOS DE COMPETENCIA			
	Conocimientos	**Habilidades**	**Actitudes**	**Valores**
Hardening a servidores y dispositivos de red.	Tipos de servidores. Sistemas operativos. Dispositivos de interconexión de Redes. Hardering a sistemas operativos Windows y Unix (Linux). Hardening a dispositivos de Interconexión de Redes.	Capacidad de abstracción y análisis. Búsqueda, instalación y configuración del sistema operativo Linux en la distribución acordada. Instalación y configuración del sistema operativo Windows en la versión acordada Manejo de terminología	Dedicación Esfuerzo Puntualidad.	Cumplir con las actividades asignadas. Respetar al docente y a los compañeros mediante un comportamiento socialmente aceptable

Estrategias Didácticas:	**RECURSOS REQUERIDOS**	**TIEMPO DESTINADO**
Realización del Hardering en entornos Windows y Linux	Pizarrón, pintarrones. Computadora. Servidores de cómputo Acceso a Internet	15 hrs.

CRITERIOS DE DESEMPEÑO IV	**EVIDENCIAS**	
	DESEMPEÑO / PRODUCTOS	**CONOCIMIENTOS**
Entrega de trabajos extraclase	Entrega de trabajo y equipo de computo para revisión donde se compruebe la realización del Hardering en entornos Windows y Linux	En arquitectura e instalación de los sistemas operativos Windows y Linux.

X. EVALUACIÓN Y ACREDITACIÓN

Dos Exámenes parciales con peso 25%.
Trabajos de investigación, tareas, prácticas 25%.
Proyecto de investigación final 30%.
Examen Ordinario 20%.
Se requiere un promedio de 8.0 para exentar.
Extraordinario y Título: 1 examen escrito único 100%

XI. REFERENCIAS

Stallings, W. "Fundamentos de seguridad en redes: aplicaciones y estándares" (2ª Ed). Pearson-Prentice Hall, 2004.
Stallings, W. "Network Security Essentials – Applications and Standars" 3a edición
Carracedo, "J. Seguridad en Redes Telemáticas". Mc Graw Hill, 2004.
Elizabeth D. Zwicky, Simon Cooper "Building Internet Firewalls" (2ª Ed). O'Reilly & Associates,2000
Housley, R., Ford, W. and Solo, D. Internet X.509 Public Key Infrastructure. "Certificate and CRL Profile." RFC 3280, 2002.
McClure, S., Scambray, J. and Kurtz, G. "Hackers. Secretos y soluciones para la seguridad de redes." McGraw-Hill, 2000.
McClure, S., Scambray, J. and Kurtz, G. "Hackers 2. Secretos y soluciones para la seguridad de redes." McGraw-Hill, 2001.
McClure, S., Scambray, J. and Kurtz, G. "Hackers 3. Secretos y soluciones para la seguridad de redes." McGraw-Hill, 2002
Garfinkel, S., Spafford, G. "Practical UNIX & Internet security" (2ª Ed). O'Reilly & Associates Inc. Abr. 1996
McClure, S., Scambray, J. and Kurtz, G. "Hacking Exposed. Network Security Secrets and Solutions" (Third Edition). McGraw-Hill, 2001.
Pastor, J. y Sarasa, M.A. **"Criptografía digital: fundamentos y aplicaciones."** Zaragoza: Prensas Universitarias, 1998.
http://www.cert.org/
http://www.sans.org/
http://www.securityfocus.com