UNIVERSIDAD AUTÓNOMA DE CHIHUAHUA Clave: 08MSU0017H Clave: 08USU4053W **FACULTAD DE INGENIERÍA** **PROGRAMA DEL CURSO:** **SEGURIDAD EN REDES**	**DES:**	Ingeniería
	Programa(s) Educativo(s):	Ingeniería de Software
	Tipo de materia:	Obligatoria
	Clave de la materia:	AC703
	Semestre:	Séptimo.
	Área en plan de estudios:	Ciencias de la Computación e Informática
	Créditos	4
	Total de horas por semana:	4
	Teoría:	2
	Práctica	2
	Taller:	
	Laboratorio:	
	Prácticas complementarias:	
	Trabajo extra clase:	
	Total de horas semestre:	64
	Fecha de actualización:	Enero del 2011
	Materia requisito:	Redes II (Cve. AC603)

Propósito del curso:
El alumno será capaz de diseñar y Configurar la seguridad en una red de computo, utilizando las diferentes funcionalidades que ofrecen los diferentes equipos de seguridad de cisco (Switches , Routers y Firewalls) para configurar la seguridad de los datos de los equipos de cómputo conectados entre sí.

Al final del curso el estudiante:

- Describir y detectar necesidades de seguridad en centros y lugares de red y uso compartido.
- Diseñar sistemas de seguridad para aplicaciones móviles y de red.
- Utilizar sistemas Cisco para facilitar los paradigmas de seguridad.
- Aplicar técnicas de adaptación y rediseño de esquemas de seguridad.
- Aplicar metodologías variadas de seguridad en redes de acuerdo con las características de instalaciones y equipos disponibles.

COMPETENCIAS (Tipo Y Nombre de la competencias que nutre la materia y a las que contribuye).	**DOMINIOS COGNITIVOS.** (Objetos de estudio, temas y subtemas)	**RESULTADOS DE APRENDIZAJE.** (Por objeto de estudio).
El curso promueve la siguientes competencias: **Competencias Básicas:**	**UNIDAD I: INTRODUCCIÓN A SEGURIDAD EN REDES**	Demuestra la instalación y configurar equipos cisco (Switches,

• Solución de problemas. • Trabajo en equipo y liderazgo. • Comunicación.	1.1 Breve descripción del porque la seguridad en Redes 1.2 Problemas derivados de la falta de seguridad en Redes	Routers y Firewalls) para cubrir las necesidades de seguridad de la información que en la organización se requiera.
Competencias Profesionales: • Proyectos de Ingeniería • Ingeniería de Proceso	**UNIDAD II: EQUIPOS DE SEGURIDAD TECNOLOGÍA Y FUNCIONALIDAD** 2.1 Firewalls 2.2 Equipos de Seguridad	Demuestra y maneja los conceptos de seguridad en nivel lógico y a nivel físico. Utiliza herramientas para poner en práctica sus conceptos.
Competencias Específicas: • Básicos de Computación en Ingeniería del Software	**UNIDAD III: FAMILIAS DE EQUIPOS DE SEGURIDAD** 3.1 Modelos y funcionalidades de los equipos 3.2 Licenciamiento PIX 3.3 Licenciamiento ASA	Clasifica la jerarquía de equipos físicos especializados en implementar seguridad. Comprende su uso en general y a detalle.
	UNIDAD IV: CONFIGURANDO SEGURIDAD EN EQUIPOS CISCO (SWICTHES, ROUTERS Y FIREWALLS) 4.1 Interface de Usuario 4.2 Manejo de Archivos 4.3 Niveles de seguridad en los equipos 4.4 Configuración básica de un equipo de seguridad 4.5 Estatus de los equipos de seguridad 4.6 Configurando NTP Configuración de Syslog	Aplica la forma de implementar seguridad a nivel de red y a nivel físico en equipos basados en tecnología Cisco.

	UNIDAD V: CONFIGURACIÓN DE FIREWALL TRANSPARENTE. 5.1 Descripción de Firewall Modo Transparente 5.2 Habilitando mode transparente de firewall 5.3Monitoreando y manteniendo Firewall en modo Transparente	Describe las generalidades del uso del firewall a nivel lógico y físico como una herramienta más de seguridad. Comprende sus limitaciones y la forma de complementar este nivel de seguridad con otros niveles de ella.
	UNIDAD VI: CONFIGURACIÓN DE CONTEXTOS DE SEGURIDAD 6.1 Descripción de Contextos de Seguridad 6.2 Manejo de Recursos 6.3 Habilitando el modo de múltiples contextos 6.4 Manejando Contextos de seguridad	Describe el concepto de contexto de seguridad. Identifica a relacionarlo con los distintos niveles de protocolos de comunicación y de casos de uso.
	UNIDAD VII: USING ACLS AND CONTENT FILTER (SWITCHES ROUTERS Y FIREWALLS) 7.1 ACLS (Switches, Routers and Firewalls) 7.2 Malicious active Code Filtering 7.3 URL Filtering 7.4 Packet Tracer	Aplica el concepto de filtrado como otra forma más de seguridad, en particular comprende su uso a nivel de red y físico de comunicación.
	UNIDAD VIII: CONFIGURACIÓN DE OBJECT GROUPING	Reconoce el concepto de agrupado de objetos como estilo de

	8.1 Descripción de Object Grouping 8.2 Configuración y uso de Object Groups	organización y encapsulamiento de información para agregar seguridad lógica.
	UNIDAD IX: CONFIGURACIÓN DE AUTENTICACIÓN, AUTORIZACIÓN Y CUENTAS 9.1 Introducción a AAA 9.2 Instalación de Cisco secure ACS for Windows 9.3 Configuración de autenticación 9.4 Autenticación de Accesos de Tunel 9.4 Configuración de Autorización 9.6 Configuración de cuentas.	Practica y desarrolla la configuración para la autentificación de redes Cisco en Windows.
	UNIDAD X: SWITCHING AND ROUTING EN LOS EQUIPOS DE SEGURIDAD DE CISCO 10.1 VLANs 10.2 Ruteo Dinámico y Estático 10.3 Multicasting	Emplea el uso de metodologías físicas y lógicas implementadas en equipos Cisco, como ilustración del concepto de ruteo de datos.
	UNIDAD XI: CONFIGURACIÓN DE POLÍTICAS (ROUTERS , SWITCHES Y FIREWALLS) 11.1 Introducción a el modelo de políticas 11.2 Configuración de un Class Map 11.3 Configuración de un Policy Map 11.4 Configuración de un Service Policy	Ilustra como son las organizaciones y clasificaciones de transmisión de datos a nivel físico y de red, como distintas formas de proteger información y lo que esto implica

	UNIDAD XII: INTRODUCCIÓN A CISCO ASA SSMS 12.1 Introducción Cisco ASA SSM 12.2 Introducción Cisco ASA AIP SSM 12.3 Cargar Software Cisco ASA AIP SSM 12.4 Introducción ASA CSC SSM 12.5 Configuración de una política de seguridad en cisco ASA	Demuestra el uso y aplicación de las reglas ASA de Cisco para la transmisión de datos a niveles físicos y de red, como complemento a las distintas metodologías de seguridad vistas anteriormente
	UNIDAD XIII: MANEJANDO LOS ACCESOS AL SISTEMA 13.1 Manejando niveles de acceso de usuarios 13.2 Manejando licencias de software y configuraciones 13.3 Actualizaciones de imágenes y activation keys 13.4 Configuración y manejo de protocolos avanzados	Clasifica el uso de jerarquías de usuario de red con respecto a derechos y reservas de acceso a la información en red. También se revisa el concepto de licenciamiento en red y el uso de protocolos avanzados a nivel de aplicación para protección de datos.
	UNIDAD XIV: MANEJO DE PROTOCOLOS AVANZADOS 14.1 Mapa de Inspección y Políticas de inspección 14.2 Expresiones regulares 14.3 Inspección de FTP 14.4 Inspección de http 14.5 Inspección de mensajería instantánea 14.6 Inspección de ESMTP 14.7 Inspección de DNS 14.8 Inspección de aplicaciones de protocolo 14.9 Soporte Multimedia	Emplea las metodologías “rápidas” de inspección de datos a nivel de aplicación, para implementar un nivel personalizado de seguridad y monitoreo.

	Configuración de VPNs	
	UNIDAD XV: VPNS SEGURAS 15.1 Como funciona IPSEC 15.2 Configuración de tareas de IPSEC 15.3 VPN Support 15.4 Configuración de parámetros IKE 15.5 Configuración de parámetros IPSEC 15.6 Verificación y prueba de Configuración VPN	Practica el concepto de seguridad a nivel VPN, sus muy particulares protocolos de seguridad basados en IPSEC
	UNIDAD XVI: REDES INALÁMBRICAS 16.1 Introducción al Wi-Fi 16.2 Tipos de redes inalámbricas 16.3 Elementos de seguridad Wi-Fi 16.4 Recomendaciones	Identifica el concepto de seguridad en redes inalámbricas, los detalles que le distinguen de otros tipos de red.
	UNIDAD XVII: SOLUCIONES DE MOVILIDAD 17.1 Introducción 17.2 17.2 Amenazas y riesgos en redes móviles 17.3 GSM 17.4 GPRS 17.5 WAP 17.6 UMTS 17.7 Amenazas y riesgos en los dispositivo	Opera los distintos protocolos de activación y acceso en redes inalámbricas en particular en redes móviles.

OBJETO DE ESTUDIO	METODOLOGIA (Estrategias, secuencias, recursos didácticos)	EVIDENCIAS DE APRENDIZAJE.
UNIDAD I: INTRODUCCIÓN A SEGURIDAD EN REDES UNIDAD II: EQUIPOS DE SEGURIDAD TECNOLOGÍA Y FUNCIONALIDAD UNIDAD III: FAMILIAS DE EQUIPOS DE SEGURIDAD UNIDAD IV: CONFIGURANDO SEGURIDAD EN EQUIPOS CISCO (SWICTHES, ROUTERS Y FIREWALLS) UNIDAD V: CONFIGURACIÓN DE FIREWALL TRANSPARENTE. UNIDAD VI: CONFIGURACIÓN DE CONTEXTOS DE SEGURIDAD UNIDAD VII: USING ACLS AND CONTENT FILTER (SWITCHES ROUTERS Y FIREWALLS) UNIDAD VIII: CONFIGURACIÓN DE OBJECT GROUPING UNIDAD IX: CONFIGURACIÓN DE AUTENTICACIÓN,	Lectura. Lectura Comentada Expositiva Materiales Gráficos: artículos, libros, Cañón Pizarrón	Tareas de Investigación Prácticas de Laboratorio Exposiciones

AUTORIZACIÓN Y CUENTAS UNIDAD X: SWITCHING AND ROUTING EN LOS EQUIPOS DE SEGURIDAD DE CISCO UNIDAD XI: CONFIGURACIÓN DE POLÍTICAS (ROUTERS , SWITCHES Y FIREWALLS) UNIDAD XII: INTRODUCCIÓN A CISCO ASA SSMS UNIDAD XIII: MANEJANDO LOS ACCESOS AL SISTEMA UNIDAD XIV: MANEJO DE PROTOCOLOS AVANZADOS UNIDAD XV: VPNS SEGURAS UNIDAD XVI: REDES INALÁMBRICAS UNIDAD XVII: SOLUCIONES DE MOVILIDAD		

FUENTES DE INFORMACIÓN (Bibliografía, Direcciones electrónicas)	**EVALUACIÓN DE LOS APRENDIZAJES** (Criterios e instrumentos)
1. Cisco Systems, Inc. (2002). *Academia de Networking de Cisco Systems.* (Segunda edición). Pearson Educación, S.A. Madrid a. ISBN: 84-205-3297-5 2. William Stallings. (2000). *Comunicaciones y redes de computadores.* (Sexta edición).	Se toma en cuenta para integrar calificaciones parciales: • Discusión Individual y por equipo, tareas y prácticas, lo cual otorga un valor del 20% • 3 Exámenes parciales escritos donde se evalúan conocimientos, comprensión y aplicación con un valor de 80% cada uno.

Pearson Educación, S.A. Madrid. a. ISBN: 84-205-2986-9 3. . Andrew S. Tanenbaum. (2003). *Redes de computadoras.* (Cuarta Edición). Editorial Pearson	La acreditación del curso se integra por promedio de las 3 calificaciones parciales. Nota: para acreditar el curso la calificación mínima aprobatoria será de 6.0

Cronograma Del Avance Programático

S e m a n a s

Objetos de estudio	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
I. INTRODUCCIÓN A SEGURIDAD EN REDES																
II. EQUIPOS DE SEGURIDAD TECNOLOGÍA Y FUNCIONALIDAD																
III. FAMILIAS DE EQUIPOS DE SEGURIDAD																
IV. CONFIGURANDO SEGURIDAD EN EQUIPOS CISCO (SWICTHES, ROUTERS Y FIREWALLS																
V. CONFIGURACIÓN DE FIREWALL TRANSPARENTE.																
VI. CONFIGURACIÓN DE CONTEXTOS DE SEGURIDAD																
VII. USING ACLS AND CONTENT FILTER (SWITCHES ROUTERS Y FIREWALLS)																
VIII. CONFIGURACIÓN DE OBJECT GROUPING																
IX. CONFIGURACIÓN DE AUTENTICACIÓN, AUTORIZACIÓN																

Y CUENTAS															
X. SWITCHING AND ROUTING EN LOS EQUIPOS DE SEGURIDAD DE CISCO															
XI. CONFIGURACIÓN DE POLÍTICAS (ROUTERS , SWITCHES Y FIREWALLS)															
XII. INTRODUCCIÓN A CISCO ASA SSMS															
XIII. MANEJANDO LOS ACCESOS AL SISTEMA															
XIV. MANEJO DE PROTOCOLOS AVANZADOS															
XV. VPNS SEGURAS															
XVI. REDES INALÁMBRICAS															
XVII. SOLUCIONES DE MOVILIDAD															