UNIVERSIDAD AUTÓNOMA DE CHIHUAHUA PROGRAMA ANALITICO DE LA UNIDAD DE APRENDIZAJE: **REDES**		
	DES:	Ingeniería
	Programa(s) Educativo(s):	Ingeniería en Ciencias de la Computación
	Tipo de materia:	Obligatoria
	Clave de la materia:	IA978
	Semestre:	9°
	Área en plan de estudios:	Ciencias de la ingeniería
	Créditos	3
	Total de horas por semana:	
	Teoría:	3
	Práctica	0
	Taller:	0
	Laboratorio:	0
	Prácticas complementarias:	0
	Trabajo extra clase:	0
	Total de horas semestre:	48
	Fecha de actualización:	Febrero 2023
	Materia requisito:	

Propósito del curso:

Provee información para que el estudiante sea capaz de identificar las vulnerabilidades de los sistemas de información de una organización, para configurar la seguridad en la transferencia y almacenamiento de los datos de los equipos de cómputo.

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).
Competencias Básicas: • Solución de problemas. Aplica la tecnología a la solución de problemáticas	**Unidad I. Introducción a la Seguridad de la Información** 1.1 Seguridad de la Información. 1.2 Código malicioso. Políticas de seguridad	Describe los tipos de seguridad informática y los conceptos de disponibilidad, integridad, confidencialidad y control de acceso para establecer medidas preventivas y correctivas contra los gusanos, virus, troyanos y ataques comunes a la red.
Competencias Específicas: • Fundamentos de Ciencias de la Computación Diseña y aplica algoritmos, estructuras y representación de datos para soluciones computacionales.	**Unidad II. Configuración de seguridad para accesos LAN y WAN** 2.3 Seguridad de Puertos Ethernet en Switches 2.4 Listas de Control de Acceso estándar. 2.5 Listas de Control de Acceso	Aplica comandos de configuración para seguridad en puertos Ethernet de los switches en las redes de computadoras. Elabora un esquema de políticas de control de acceso

	Extendidas	de información donde se aplican comandos de configuración ACL extendidas para control de uso de servicios TCP y UDP.
Distingue los conceptos básicos de redes de computadoras para la creación de redes funcionales de cómputo.	**Unidad III. Métodos de autenticación** 3.1 Servicios AAA. 3.2 Algoritmos de Hash MD5 y SHA-1. 3.3 Certificados digitales.	Explica el procedimiento para la configuración de RADIUS así como la interpretación del funcionamiento de los Algoritmos de Hash Aplica el procedimiento para la configuración de certificados digitales para correo electrónico.
	Unidad IV. Firewalls 4.1 Medidas de seguridad preventivas y correctivas aplicables a un Firewall. 4.2 Técnicas de implementación de Firewall para control de ancho de banda, IDS, IPS, Web Filtering y Código malicioso	Identifica las medidas de seguridad aplicables a un Firewall y las diferentes técnicas de implementación de Firewall a nivel de red y Firewall a nivel de aplicación. Configura las restricciones Para la detección de intrusiones t en soluciones appliance (Cisco Fortigate de Fortinet)
	Unidad V. VPN 5.1 Conceptos y fundamentos de VPN 5.2 Servicios y tipos de VPN. 5.3 Protocolos VPN: PPTP, L2F, L2TP. 5.4 Configuración de VPN.	Describe las principales características de una VPN y la Seguridad (IPSec) para la configuración de una VPN.

OBJETO DE ESTUDIO	**METODOLOGIA** (Estrategias, secuencias, recursos didácticos)	**EVIDENCIAS DE APRENDIZAJE.**

Unidad I. Introducción a la Seguridad de la Información Unidad II. Configuración de seguridad para accesos LAN y WAN Unidad III. Métodos de autenticación. Unidad IV. Firewalls. Unidad V. VPN.	Lectura. Lectura Comentada Expositiva Materiales Gráficos: Artículos, libros, Cañón Pizarrón Equipo de cómputo Software de simulación de Redes	Tareas de Investigación Prácticas de Laboratorio Exposiciones

FUENTES DE INFORMACIÓN (Bibliografía, Direcciones electrónicas)	**EVALUACIÓN DE LOS APRENDIZAJES** (Criterios e instrumentos)
1. Royer, J. (2004) *Seguridad en la informática de empresa: riesgos, amenazas, prevención y soluciones*, Paris Francia. ENI Ediciones 2. Stallings, W.(2013).*Cryptography and Network Security* .(6 Ed). Indianapolis,EE.UU. Prentice Hall 3. Deal, Richard. (2005).*Complete Cisco VPN Configuration Guide, The Indianapolis*.(1era Ed).EE.UU.Pearson Education, Cisco Press 4. Olifer N: Olifer V.(2012). *Redes de Computadoras.*México.(5ta. Ed).D.F. McGraw-Hill	**INSTRUMENTOS:** • Prueba escrita • Solución de ejercicios (aplicación de conocimientos • Prácticas de laboratorio • Lista de cotejo (Respeto y participación al trabajo dentro del salón de clase, interés por la asignatura **CRITERIOS DE DESEMPEÑO:** • La solución de ejercicios se realiza en clase en forma individual o por pares según amerite. • **Exposición:** presentadas en orden lógico: 1. Introducción resaltando el objetivo a alcanzar 2. Desarrollo temático, responder preguntas y aclarar dudas 3. Concluir. • **Los trabajos extracurriculares** Toda actividad complementaria al curso se podrá llevar a cabo en forma individual o por equipo según amerite el tema. Estos se reciben únicamente en tiempo y forma previamente establecidos. • **Prácticas de Laboratorio**:

	Se realizan las prácticas en el software de simulación de redes. • **Exámenes escritos**: Primer parcial: Comprende lo visto en la unidad I y unidad II. - 50% Tareas y ensayo de investigación - 50% Examen objetivo de preguntas de relación y opción múltiple. Segundo parcial: Comprende lo visto en la unidad III. - 60% Reportes de prácticas de laboratorio - 40% Examen objetivo de preguntas de relación y opción múltiple Tercer parcial: Comprende lo visto en la unidad IV. - 60% Reportes de prácticas de laboratorio - 40% Examen objetivo de preguntas de relación y opción múltiple **LAS ACTIVIDADES NO REALIZADAS EN TIEMPO Y FORMA SE CALIFICAN CON CERO**. **Nota:** para acreditar el curso se deberá tener calificación aprobatoria tanto en la teoría como en las prácticas.

Cronograma Del Avance Programático

S e m a n a s

Objeto de Estudio	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Unidad I. Introducción a la Seguridad de la Información																
Unidad II. Configuración de seguridad para accesos LAN y WAN																
Unidad III. Métodos de autenticación																
Unidad IV. Firewalls																
Unidad V. VPN																