1. Datos Generales de la asignatura

Nombre de la asignatura:	Seguridad De Redes
Clave de la asignatura:	CIB-2602
SATCA[1]:	2-3-5
Carrera:	Ingeniería Informática

2. Presentación

Caracterización de la asignatura
Desarrolla habilidades para proteger infraestructuras de red mediante controles de seguridad.
Intención didáctica
Aprendizaje práctico con laboratorios y simulaciones reales.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Villa Montemorelos, Dgo., a 20 de abril de 2026	Ana Laura Chavira Campos Ramiro Robles Villanueva	Reunión de Academia de Ingeniería en Informática para la elaboración de Especialidades

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Implementa mecanismos de seguridad en redes de datos.

5. Competencias previas

Redes de computadoras, Interconectividad de Redes

[1] Sistema de Asignación y Transferencia de Créditos Académicos

6. Temario

No.	Temas	Subtemas
1	Fundamentos de Seguridad de Redes	1.1 Principios de seguridad 1.2 Amenazas comunes 1.3 Arquitecturas seguras 1.4 Defensa en profundidad 1.5 Buenas prácticas
2	Hardening de Dispositivos	2.1 Concepto de hardening 2.2 Seguridad en routers 2.3 Seguridad en switches 2.4 Control administrativo 2.5 Mantenimiento seguro
3	Firewalls e IDS/IPS	3.1 Tipos de firewalls 3.2 Políticas de filtrado 3.3 IDS 3.4 IPS 3.5 Integración
4	VPN y Segmentación	4.1 VPN 4.2 Tipos de VPN 4.3 VLANs 4.4 Segmentación 4.5 Acceso remoto

7. Actividades de aprendizaje de los temas

1. Fundamentos de Seguridad de Redes	
Competencias	Actividades de aprendizaje
Comprende y aplica los principios básicos de la seguridad de redes para identificar amenazas y proponer arquitecturas seguras.	• Investigación documental sobre principios de seguridad, amenazas comunes y modelos de defensa en profundidad. • Análisis de casos reales de incidentes de seguridad en redes. • Elaboración de mapas conceptuales sobre arquitecturas seguras y buenas prácticas. • Discusión grupal y presentación de conclusiones utilizando terminología técnico-científica adecuada.
2. Hardening de Dispositivos	
Competencias	Actividades de aprendizaje
Aplica técnicas de hardening en dispositivos de red considerando controles administrativos y mantenimiento seguro.	• Búsqueda y análisis de guías de hardening para routers y switches. • Configuración básica de dispositivos de red en entorno simulado aplicando medidas de seguridad. • Trabajo colaborativo para documentar políticas de control administrativo. • Resolución de problemas prácticos relacionados con vulnerabilidades en dispositivos de red.
3. Firewalls e IDS/IPS	
Competencias	Actividades de aprendizaje
Configura y evalúa firewalls e IDS/IPS para la protección de redes de datos.	• Investigación comparativa de tipos de firewalls, IDS e IPS. • Diseño de políticas de filtrado de tráfico. • Simulación de escenarios de ataque y

	detección mediante IDS/IPS. • Análisis y reporte de resultados obtenidos en prácticas de laboratorio.
4. VPN y Segmentación	
Competencias	Actividades de aprendizaje
Implementa soluciones de VPN y segmentación de red para garantizar el acceso seguro y la protección de la información.	• Investigación sobre tipos de VPN y tecnologías de segmentación (VLANs). • Configuración de una VPN básica en entorno de simulación. • Diseño de esquemas de segmentación de red para distintos contextos. • Integración de conocimientos en un caso práctico integral.

8. Práctica(s)

- Análisis de vulnerabilidades en una red simulada y propuesta de medidas de seguridad.
- Configuración segura (hardening) de routers y switches.
- Implementación de un firewall con políticas de filtrado y pruebas de IDS/IPS.
- Configuración de una VPN y segmentación de red mediante VLANs.

9. Proyecto de asignatura

Diseño e implementación de una solución integral de seguridad para una red de datos en un contexto real o simulado.

- **Fundamentación:** Análisis del contexto organizacional y diagnóstico de riesgos de seguridad, sustentado en un marco teórico, conceptual y normativo.
- **Planeación:** Definición de objetivos, alcance, actividades, recursos necesarios y cronograma del proyecto con asesoría docente.
- **Ejecución:** Implementación de las soluciones propuestas (hardening, firewall, IDS/IPS, VPN y segmentación).
- **Evaluación:** Valoración de resultados, logros y áreas de mejora, fomentando la metacognición y la mejora continua.

10. Evaluación por competencias

I**nvestigaciones documentales.**
La evaluación será continua y formativa, considerando evidencias de desempeño tales como:

- Reportes de investigaciones documentales.
- Prácticas de laboratorio y configuraciones implementadas.
- Participación en actividades colaborativas y discusiones.
- Desarrollo, presentación y reporte final del proyecto de asignatura.

Se emplearán rúbricas, listas de cotejo y observación directa para constatar el logro de las competencias específicas y genéricas.

11. Fuentes de información

- Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach*. Pearson.
- Stallings, W. (2020). *Network Security Essentials*. Pearson.
- Cisco Networking Academy. (2023). *Network Security Fundamentals*.
- Scarfone, K., & Hoffman, P. (NIST). *Guidelines on Firewalls and Firewall Policy*.
- Documentación técnica y recursos digitales actualizados relacionados con seguridad de redes, citados conforme a la norma APA vigente.