1. Datos Generales de la asignatura

Nombre de la asignatura:	Seguridad en Sistemas Operativos
Clave de la asignatura:	CIB-2603
SATCA[1]:	2-3-5
Carrera:	Ingeniería Informática

2. Presentación

Caracterización de la asignatura
Aplica principios de seguridad en sistemas operativos Windows y Linux mediante la identificación de amenazas, la gestión de privilegios y la configuración segura del sistema
Intención didáctica
Que el estudiante aplique principios y mecanismos de seguridad en sistemas operativos Windows y Linux, mediante la identificación de amenazas, la gestión de privilegios, la configuración segura del sistema y la protección de endpoints, con el fin de prevenir, identificar y mitigar riesgos de seguridad en entornos informáticos. Durante el desarrollo de la asignatura, el estudiante analiza vulnerabilidades, utiliza herramientas especializadas para su detección y mitigación, y aplica buenas prácticas de seguridad, fortaleciendo competencias técnicas, analíticas y éticas propias del campo de la ciberseguridad. El enfoque de la materia es teórico–práctico, promoviendo el aprendizaje significativo a través de prácticas de laboratorio, estudios de caso y un proyecto integrador, que simulan situaciones reales del entorno profesional.

[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
Villa Montemorelos, Dgo., a 20 de abril de 2026	Velia Zúñiga Meraz Octaviano Sergio Meraz Carranza	Reunión de Academia de Ingeniería en Informática para la elaboración de Especialidades

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Identifica, evalúa y mitiga vulnerabilidades en sistemas y endpoints mediante metodologías y herramientas especializadas.

5. Competencias previas

Sistemas operativos I, Sistemas operativos II

6. Temario

No.	Temas	Subtemas
1	Seguridad en Sistemas Operativos	1.1 Amenazas 1.2 Windows 1.3 Linux 1.4 Privilegios mínimos 1.5 Configuración segura
2	Gestión de Vulnerabilidades	2.1 Identificación 2.2 Evaluación 2.3 Escaneo 2.4 Parches 2.5 Mitigación
3	Malware y Endpoints	3.1 Tipos 3.2 Infección 3.3 Antimalware 3.4 Protección 3.5 Respuesta
		4.1 IAM 4.2 Autenticación

4	Identidades y Accesos	4.3 Autorización 4.4 Credenciales 4.5 Buenas prácticas

7. Actividades de aprendizaje de los temas

Seguridad en Sistemas Operativos	
Competencias	Actividades de aprendizaje
Aplica principios de seguridad en sistemas operativos Windows y Linux mediante la identificación de amenazas, la gestión de privilegios y la configuración segura del sistema.	Investigar y analizar diferentes tipos de amenazas que afectan a los sistemas operativos actuales. Comparar mecanismos de seguridad en Windows y Linux mediante cuadros comparativos. Realizar configuraciones de privilegios mínimos en entornos de prueba. Ejecutar prácticas guiadas de hardening básico en sistemas operativos. Participar en discusiones grupales sobre fallas comunes de configuración y sus implicaciones. Elaborar reportes técnicos utilizando terminología científico-tecnológica adecuada.
Gestión de Vulnerabilidades	
Competencias	Actividades de aprendizaje
Identifica, evalúa y mitiga vulnerabilidades en sistemas y endpoints mediante metodologías y herramientas especializadas.	Investigar conceptos y metodologías de gestión de vulnerabilidades. Analizar casos reales de explotación de vulnerabilidades. Utilizar herramientas de escaneo de vulnerabilidades en entornos controlados. Interpretar reportes de escaneo y priorizar vulnerabilidades. Diseñar planes básicos de aplicación de

	parches y mitigación. Trabajar en equipo para la resolución de problemas de seguridad simulados.
Malware y Endpoints	
Competencias	Actividades de aprendizaje
Analiza y responde ante incidentes de malware en equipos finales mediante el uso de herramientas antimalware y estrategias de protección	Clasificar los diferentes tipos de malware y sus vectores de infección. Analizar el comportamiento de código malicioso en entornos aislados. Configurar y evaluar soluciones antimalware. Simular incidentes y aplicar procedimientos de respuesta básica. Elaborar informes técnicos de incidentes de seguridad. Reflexionar sobre buenas prácticas de protección de endpoints
Identidades y accesos	
Competencias	Actividades de aprendizaje
Gestiona de forma segura identidades y accesos utilizando principios de autenticación, autorización y buenas prácticas de seguridad	Investigar modelos de gestión de identidades y accesos (IAM). Analizar mecanismos de autenticación y autorización. Configurar credenciales seguras en sistemas de prueba. Evaluar riesgos asociados a una mala gestión de accesos. Desarrollar políticas básicas de control de acceso. Integrar conocimientos mediante actividades prácticas interdisciplinarias

8. Práctica(s)

Configuración segura y evaluación de seguridad en un endpoint.

- Configuración de un sistema operativo aplicando principios de hardening.
- Escaneo de vulnerabilidades y aplicación de medidas de mitigación.
- Instalación y configuración de soluciones antimalware.
- Implementación de políticas básicas de autenticación y control de acceso.

Competencias desarrolladas

- Aplicación práctica de técnicas de seguridad.
- Trabajo colaborativo.
- Uso adecuado de herramientas tecnológicas.
- Análisis y solución de problemas reales del entorno profesional.

9. Proyecto de asignatura

Implementación de un esquema integral de seguridad para endpoints en una organización.

El proyecto se fundamenta en la necesidad actual de proteger sistemas operativos y dispositivos finales frente a amenazas, vulnerabilidades y accesos no autorizados, considerando el contexto tecnológico y organizacional.

Para llevar a cabo la planeación se requiere:

- Diagnóstico de seguridad de una organización simulada.
- Definición de objetivos y alcance del proyecto.
- Selección de herramientas y recursos.
- Elaboración de un cronograma de actividades.

La ejecución

- Implementación de configuraciones seguras.
- Gestión de vulnerabilidades.
- Protección contra malware.
- Administración de identidades y accesos.

La evaluación

- Presentación del proyecto.
- Evidencias técnicas documentadas.
- Autoevaluación y coevaluación.
- Retroalimentación orientada a la mejora continua.

10. Evaluación por competencias

La evaluación será continua, formativa y sumativa, basada en evidencias de desempeño.

- Estrategias e instrumentos
- Investigaciones documentales.

- Reportes técnicos.
- Prácticas de laboratorio.
- Proyecto integrador.
- Listas de cotejo y rúbricas.
- Observación del desempeño.
- Participación individual y grupal.

11. Fuentes de información

Stallings, W. (2023). Operating System Security. Pearson.

NIST. (2022). Guide to Operating System Security.

Scarfone, K., & Mell, P. (2023). Managing Security Vulnerabilities. NIST.

Behl, A. (2022). Cybersecurity and Cyberwar. Oxford University Press.

Documentación oficial de Microsoft Security y Linux Security.

Artículos científicos y técnicos especializados en seguridad informática.

Recursos digitales y normativas vigentes en ciberseguridad