1. Datos Generales de la asignatura

Nombre de la asignatura:	Fundamentos De Ciberseguridad
Clave de la asignatura:	CID-2601
SATCA[1]:	(2-3-5)
Carrera:	Ingeniería Informática

2. Presentación

Caracterización de la asignatura
Esta asignatura aporta conocimientos, habilidades y actitudes básicas para la protección de la información y de los sistemas informáticos, mediante el estudio de los principios, amenazas y riesgos asociados a la ciberseguridad.
Intención didáctica
Se desarrolla con un enfoque teórico-práctico, privilegiando el análisis crítico, la investigación documental y actividades prácticas orientadas al desarrollo de competencias profesionales.

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	Santiago Rene de la Torre Lugo Daniel Alfredo Castro Gonzalez	Reunión de Academia de Ingeniería en Informática para la elaboración de Especialidades

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Analiza los fundamentos de la ciberseguridad para identificar amenazas, vulnerabilidades y riesgos en sistemas informáticos, utilizando principios y buenas prácticas de seguridad.

5. Competencias previas

Aplica conceptos de redes de computadoras y sistemas operativos para el análisis de entornos informáticos.

[1] Sistema de Asignación y Transferencia de Créditos Académicos

6. Temario

No.	Temas	Subtemas
1	Introducción a la Ciberseguridad	1.1 Concepto y alcance 1.2 Evolución histórica 1.3 Importancia organizacional 1.4 Dominios de la ciberseguridad 1.5 Continuidad y resiliencia
2	Amenazas, Vulnerabilidades y Riesgos	2.1 Tipos de amenazas 2.2 Vulnerabilidades tecnológicas 2.3 Actores maliciosos 2.4 Análisis de riesgos 2.5 Impacto organizacional
3	Fundamentos de Criptografía	3.1 Principios básicos 3.2 Cifrado simétrico 3.3 Cifrado asimétrico 3.4 Hash y firmas digitales 3.5 Aplicaciones prácticas
4	Concientización en Seguridad	4.1 Cultura de seguridad 4.2 Ingeniería social 4.3 Políticas básicas 4.4 Buenas prácticas 4.5 Responsabilidad del usuario

7. Actividades de aprendizaje de los temas

Nombre de tema Introducción a la Ciberseguridad	
Competencias	Actividades de aprendizaje
Específica(s): Comprende el concepto, alcance e importancia de la ciberseguridad, identificando sus dominios y su relación con la continuidad y resiliencia organizacional. Genéricas: Capacidad de análisis y síntesis; comunicación efectiva; trabajo colaborativo; uso de tecnologías de la información.	• Búsqueda, selección y análisis de información en fuentes académicas y técnicas sobre el concepto, alcance y evolución de la ciberseguridad. • Elaboración de una línea del tiempo que represente los principales hitos históricos de la ciberseguridad. • Discusión grupal sobre la importancia de la ciberseguridad en el contexto organizacional actual. • Análisis de casos reales de incidentes de seguridad y su impacto en la continuidad operativa. • Elaboración de mapas conceptuales que integren los dominios de la ciberseguridad.
Nombre de tema Amenazas, Vulnerabilidades y Riesgos	
Competencias	Actividades de aprendizaje
Específica(s): Analiza los tipos de amenazas, vulnerabilidades y riesgos en sistemas informáticos, valorando su impacto organizacional. Genéricas: Pensamiento crítico; solución de problemas; trabajo en equipo.	• Investigación documental y clasificación de amenazas y actores maliciosos. • Identificación de vulnerabilidades en escenarios simulados de sistemas informáticos. • Desarrollo de ejercicios básicos de análisis de riesgos. • Trabajo colaborativo para evaluar el impacto organizacional de incidentes de seguridad. • Presentación grupal de resultados y conclusiones

Nombre de tema Fundamentos de Criptografía	
Competencias	Actividades de aprendizaje
Específica(s): Aplica los principios básicos de la criptografía para proteger la información. Genéricas: Aplicación del conocimiento; razonamiento lógico; uso de TIC.	• Investigación comparativa de los métodos de cifrado simétrico y asimétrico. • Ejercicios demostrativos del uso de funciones hash y firmas digitales. • Resolución de problemas prácticos relacionados con la confidencialidad e integridad de la información. • Análisis de aplicaciones prácticas de la criptografía en entornos reales.
Nombre de tema Concientización en Seguridad	
Competencias	Actividades de aprendizaje
Específica(s): Reconoce la importancia de la cultura de seguridad y la responsabilidad del usuario en la protección de la información. Genéricas: Responsabilidad social; comunicación efectiva; ética profesional.	• Análisis de técnicas de ingeniería social mediante ejemplos reales. • Diseño de recomendaciones sobre buenas prácticas de seguridad informática. • Elaboración de una propuesta básica de política de seguridad. • Discusión reflexiva sobre el papel del usuario en la ciberseguridad organizacional.

8. Práctica(s)

Práctica 1: Identificación de amenazas, vulnerabilidades y riesgos en un entorno informático simulado. Práctica 2: Aplicación básica de mecanismos criptográficos (hash y cifrado elemental). Práctica 3: Análisis de escenarios de ingeniería social y propuesta de medidas preventivas.

9. Proyecto de asignatura

Nombre del proyecto

Diagnóstico básico de ciberseguridad en un entorno organizacional.

Fundamentación

Se fundamenta en un diagnóstico del contexto organizacional apoyado en un marco teórico y conceptual sobre ciberseguridad, amenazas, vulnerabilidades y buenas prácticas.

Planeación

Definición del problema, objetivos, actividades, recursos necesarios y cronograma de trabajo, con asesoría del docente.

Ejecución

Aplicación de los conocimientos adquiridos para identificar riesgos y proponer acciones de mejora en el entorno seleccionado.

Evaluación

Valoración de resultados, identificación de logros y áreas de mejora, promoviendo la mejora continua y la reflexión crítica.

10. Evaluación por competencias

I**nvestigaciones documentales.**

- Reportes de prácticas.
- Participación individual y grupal.
- Productos del proyecto de asignatura.
- Exposiciones y análisis de casos.

Instrumentos: Rúbricas, listas de cotejo, portafolio de evidencias, autoevaluación y coevaluación.

11. Fuentes de información

Stallings, W. (2023). *Cryptography and Network Security*. Pearson.

- Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security*. Cengage Learning.
- ISO/IEC 27001:2022. Information Security Management Systems.
- NIST. (2024). *Cybersecurity Framework*.