1. Datos Generales de la asignatura

Nombre de la asignatura:	Monitoreo Y Análisis De Incidentes (SOC)
Clave de la asignatura:	CIB-2604
SATCA[1]:	2-3-5
Carrera:	Ingeniería Informática

2. Presentación

Caracterización de la asignatura
Monitorea y responde a incidentes de seguridad
Intención didáctica
Esta asignatura ha sido diseñada para que el estudiante desarrolle la capacidad de gestionar de manera integral la seguridad operativa a través de un Centro de Operaciones de Seguridad (SOC). Se busca fomentar el trabajo colaborativo y el uso de nuevas tecnologías para que el estudiante adquiera conocimientos técnicos, y que desarrolle un pensamiento crítico y analítico. Se integra el conocimiento previo de Seguridad y Legislación Informática para asegurar que todas las acciones de monitoreo y respuesta se realicen bajo un marco ético y legal vigente

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	Zoe Adriana Gonzalez Perez Norma Isela Sanchez Zapata Juan Manuel Hidalgo Martinez	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 eventos e incidentes de seguridad en un SOC.

[1] Sistema de Asignación y Transferencia de Créditos Académicos

5. Competencias previas

Desarrollo e Implementación de Sistemas de Información, Calidad en los Sistemas de Información, Seguridad Informática, Legislación Informática

6. Temario

No.	Temas	Subtemas
1	SOC	1.1 Concepto 1.2 Roles 1.3 Procesos 1.4 Gestión 1.5 Importancia
2	Logs y SIEM	2.1 Logs 2.2 Fuentes 2.3 SIEM 2.4 Correlación 2.5 Alertas
3	Análisis de Tráfico	3.1 Tráfico 3.2 Anomalías 3.3 Eventos 3.4 Ataques 3.5 Herramientas
4	Respuesta a Incidentes	4.1 Clasificación 4.2 Contención 4.3 Recuperación 4.4 Documentación 4.5 Mejora

7. Actividades de aprendizaje de los temas

Nombre de tema SOC	
Competencias	Actividades de aprendizaje
Específica: Comprende la estructura y roles de un SOC para el diseño de estrategias de monitoreo . **Genéricas:** Capacidad de análisis y síntesis, trabajo en equipo y comunicación oral y escrita.	• Investigar en diversas fuentes los roles y procesos de un SOC y presentar un cuadro comparativo . • Realizar un mapa de procesos que ilustre la gestión de incidentes dentro de un centro de operaciones . • Debatir en grupo la importancia del SOC en las organizaciones modernas.
Nombre de tema Logs y SIEM	
Competencias	Actividades de aprendizaje
Específica: Configura y analiza fuentes de logs en sistemas SIEM para la correlación de eventos . **Genéricas:** Habilidades en el uso de tecnologías de información y comunicación.	• Realizar prácticas de configuración de recolección de logs desde diversas fuentes (OS, Network, App). • Configurar reglas de correlación en un SIEM para generar alertas automáticas basadas en eventos específicos . • Analizar casos de estudio sobre falsos positivos y proponer ajustes en las alertas.
Nombre de tema Análisis de Tráfico	
Competencias	Actividades de aprendizaje
Específica: Utiliza herramientas de análisis para identificar anomalías y ataques en el tráfico de red . **Genéricas:** Capacidad de investigación y solución de problemas.	• Utilizar herramientas (como Wireshark o Zeek) para inspeccionar capturas de tráfico (PCAP) en busca de patrones de ataque . • Documentar el hallazgo de anomalías mediante la aplicación del método científico (observación y planteamiento de hipótesis) . • Resolver ejercicios de identificación de protocolos y flujos de tráfico sospechosos.

Nombre de tema Respuesta a Incidentes	
Competencias	Actividades de aprendizaje
Específica: Ejecuta planes de contención, recuperación y documentación ante incidentes de seguridad . **Genéricas:** Compromiso ético y enfoque sustentable.	• Simular un incidente de seguridad para practicar las fases de contención y recuperación en entornos controlados . • Elaborar informes técnicos de incidentes siguiendo estándares de documentación profesional . • Analizar el impacto ambiental y social de las brechas de seguridad masivas.

8. Práctica(s)

Despliegue de un mini-SOC Open Source: Instalación y configuración de un entorno con herramientas como ELK Stack o Wazuh. **Correlación de ataques conocidos:** Generar ataques simulados (Brute force, SQLi) y verificar su detección en el SIEM. **Forense de Red:** Análisis profundo de tráfico malicioso para identificar el origen y alcance de una intrusión. **Simulacro de respuesta (Blue Team vs Red Team):** Ejercicio grupal de defensa y respuesta ante ataques en tiempo real.

9. Proyecto de asignatura

Diseño e implementación de un modelo de monitoreo y respuesta para una organización.
Fundamentación: Realizar un diagnóstico del contexto legal (Legislación Informática) y técnico para definir el alcance del SOC.
Planeación: Diseñar la arquitectura técnica, los recursos requeridos y el cronograma de implementación.
Ejecución: Construcción del modelo, configuración de herramientas y puesta en marcha de las reglas de monitoreo.
Evaluación: Aplicar pruebas de estrés al modelo y presentar un informe de resultados para la mejora continua.

10. Evaluación por competencias

I**nvestigaciones documentales.**

La evaluación será **continua y formativa**, basándose en el desempeño de las actividades:
Portafolio de evidencias: Recopilación de informes de prácticas y reportes de análisis.
Rúbricas de desempeño: Para evaluar la configuración técnica y el uso de terminología científica.
Exámenes prácticos: Resolución de problemas de seguridad en entornos de laboratorio.
Evaluación del proyecto: Presentación de los avances y el entregable final según criterios de calidad.

11. Fuentes de información

NIST. (2024). *Computer Security Incident Handling Guide (Special Publication 800-61)*.
ISO/IEC 27035. (2023). *Information technology — Information security incident management*.
Chantzis, F., et al. (2023). *Practical SIEM: A hands-on guide to log management and correlation*.
Santos, O. (2024). *Orchestrating Security Operations (SOC) and Incident Response*. Cisco Press.