UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

FACULTAD DE CIENCIAS MATEMÁTICAS

SÍLABO

1. INFORMACIÓN GENERAL

1.1 Curso	:	Seguridad en Computación
1.2 Código	:	CS3I1
1.3 Programa Académico	:	Computación Científica
1.4 Créditos	:	5
1.5 Prerrequisitos	:	CS210. Algoritmos y Estructuras de Datos. (4^{to} Sem)
1.6 Tipo de curso	:	Electivo
1.7 Área de Estudios	:	Estudios Generales
1.8 Número de Semanas	:	16
1.9 Horas por semana	:	3 HT; 4 HP;
1.10 Ciclo	:	I
1.11 Modalidad de aprendizaje	:	Presencial
1.12 Periodo Académico	:	2026-I
1.13 Inicio del semestre	:	
1.14 Fin del semestre	:	

2. PROFESORES

Atención previa coordinación con el profesor

3. INTRODUCCIÓN AL CURSO

En un mundo cada vez más digital, la seguridad ya no es una característica opcional sino un requisito fundamental. Este curso proporciona una introducción completa a los principios y prácticas de la ciberseguridad, cubriendo desde los fundamentos teóricos hasta la codificación segura y la informática forense digital. Los estudiantes adquirirán las habilidades necesarias para diseñar, implementar y gobernar sistemas seguros, comprendiendo las responsabilidades éticas y profesionales involucradas en la protección de la información y la infraestructura.

4. OBJETIVOS

- Comprender los principios fundamentales y las bases matemáticas de la seguridad.
- Aplicar técnicas de codificación segura y métodos criptográficos al software.
- Analizar vulnerabilidades del sistema y realizar investigaciones forenses.
- Evaluar la gobernanza de seguridad y la ética profesional en ciberseguridad.

5. RESULTADOS DEL ESTUDIANTE

ABET-3) Habilidad para desarrollar y llevar a cabo experimentos o probar hipótesis, analizar e interpretar datos y utilizar el juicio científico para obtener conclusiones. (Usage)

ABET-2) Habilidad para formular o diseñar un sistema, proceso, procedimiento o programa para el propósito previsto. (Usage)

6. TEMAS

Unidad 1: Principios y Mentalidad de Seguridad (6 horas)	
Resultados esperados: ABET-2,ABET-3	
Temas	**Aprendizaje esperado (*Learning Outcomes*)**
▪ Desarrollar una mentalidad de seguridad que incorpore conceptos transversales: confidencialidad, integridad, disponibilidad, evaluación de riesgos, pensamiento sistémico, pensamiento adversarial, pensamiento centrado en el humano. ▪ Vulnerabilidades, amenazas, superficies de ataque y vectores de ataque Protección y Seguridad. ▪ Denegación de Servicio (DoS) y Denegación de Servicio Distribuida (DDoS) Protección y Seguridad. ▪ Principios y prácticas de protección, por ejemplo, privilegio mínimo, diseño abierto, valores predeterminados seguros ante fallos, defensa en profundidad y confianza cero; y cómo pueden implementarse Principios del Sistema Operativo, Protección y Seguridad, Prácticas de Codificación, Construcción a Escala y Proceso, Delitos y Ataques Informáticos, Leyes, Políticas y Responsabilidad en Seguridad. ▪ Consideraciones de optimización entre seguridad, privacidad, rendimiento y otros objetivos de diseño Diseño de Sistemas, Prácticas de Desarrollo de Software, Pruebas de Rendimiento y Evaluación Comparativa, Herramientas y Análisis de Pruebas, Conceptos de verificación y validación, Planificación y Tipos de Pruebas, Prácticas Avanzadas de Pruebas. ▪ Conceptos de confianza (trust) y confiabilidad (trustworthiness).	▪ Evaluar un sistema para posibles ataques que pueda lanzar un adversario [Evaluar] ▪ Diseñar y desarrollar enfoques para proteger un sistema de un conjunto de amenazas identificadas [Diseñar] ▪ Describir cómo se puede evitar el daño a la privacidad del usuario [Describir] ▪ Desarrollar un sistema que incorpore varios principios de seguridad y privacidad [Crear]
Lecturas : [**Pfleeger2015**], [**Stallings2017**]	

Unidad 2: Fundamentos de Criptografía (8 horas)	
Resultados esperados: ABET-2,ABET-3	
Temas	**Aprendizaje esperado (*Learning Outcomes*)**
▪ Diferencias entre las vistas algorítmica, aplicada y matemática de la criptografía. ▪ Preliminares matemáticos: aritmética modular, algoritmo euclidiano, independencia probabilística, conceptos básicos de álgebra lineal, teoría de números, campos finitos, complejidad, análisis asintótico Matemáticas Discretas, álgebra Lineal. ▪ Criptografía básica: criptografía de clave simétrica y de clave pública Estructuras de Datos Fundamentales, Algoritmos Fundamentales, Algoritmos Avanzados, Matemáticas Discretas. ▪ Criptosistemas clásicos, como cifrados de desplazamiento, sustitución, transposición, libros de códigos y máquinas Matemáticas Discretas. ▪ Principio de Kerckhoff y uso de bibliotecas evaluadas (vetted) Prácticas de Codificación, Construcción a Escala y Proceso.	▪ Explicar el papel de la criptografía en el soporte de la seguridad y la privacidad [Explicar] ▪ Discutir los riesgos de inventar los propios métodos criptográficos [Debatir] ▪ Discutir la importancia de los números primos en criptografía y explicar su uso en algoritmos criptográficos [Debatir] ▪ Implementar y criptoanalizar cifrados clásicos [Implementar]
Lecturas : [**Stallings2017**]	

Unidad 3: Inyección y Validación de Entrada (8 horas)	
Resultados esperados: ABET-2,ABET-3	
Temas	**Aprendizaje esperado (*Learning Outcomes*)**
▪ Vulnerabilidades y debilidades comunes. ▪ Inyección SQL y otros ataques de inyección. ▪ Técnicas de cross-site scripting y mitigaciones. ▪ Validación de entrada y sanitización de datos Protección y Seguridad, Conceptos y Construcciones Básicas de Programación, Prácticas de Programación: Pruebas, Depuración y Documentación, Pruebas de Rendimiento y Evaluación Comparativa, Herramientas y Análisis de Pruebas, Conceptos de verificación y validación, Planificación y Tipos de Pruebas, Prácticas Avanzadas de Pruebas.	▪ Identificar problemas subyacentes en ejemplos dados de una enumeración de debilidades comunes y explicar cómo pueden evitarse [Analizar] ▪ Aplicar técnicas de validación de entrada y sanitización de datos para mejorar la seguridad de un programa [Aplicar] ▪ Evaluar y prevenir ataques de inyección SQL en una aplicación de base de datos [Evaluar] ▪ Evaluar y prevenir ataques de cross-site scripting contra un sitio web [Evaluar] ▪ Construir un programa que pruebe todos los errores de manejo de entrada [Crear]
Lecturas : [**Pfleeger2015**]	

Unidad 4: Análisis de Malware y Seguridad Avanzada (6 horas)	
Resultados esperados: ABET-2	
Temas	**Aprendizaje esperado (*Learning Outcomes*)**
▪ Técnicas de seguridad ofensiva como defensa. ▪ Técnicas de detección de malware asistidas por IA. ▪ Ransomware: creación, prevención y mitigación. ▪ Uso seguro de componentes de terceros Prácticas de Codificación, Construcción a Escala y Proceso, Pruebas de Rendimiento y Evaluación Comparativa, Herramientas y Análisis de Pruebas, Conceptos de verificación y validación, Planificación y Tipos de Pruebas, Prácticas Avanzadas de Pruebas. ▪ Malware: variedades, creación, ingeniería inversa y defensa contra ellos Traducción y Ejecución de Lenguajes, Modelo de Ejecución y Memoria de Sistemas. ▪ Garantía (assurance): pruebas (incluyendo fuzzing y pruebas de penetración), verificación y validación Protección y Seguridad, Conceptos y Construcciones Básicas de Programación, Prácticas de Programación: Pruebas, Depuración y Documentación, Prácticas de Codificación, Construcción a Escala y Proceso, Pruebas de Rendimiento y Evaluación Comparativa, Herramientas y Análisis de Pruebas, Conceptos de verificación y validación, Planificación y Tipos de Pruebas, Prácticas Avanzadas de Pruebas. ▪ Análisis estático y dinámico Análisis de Programas y Analizadores, Protección y Seguridad, Evaluación, Pruebas de Rendimiento y Evaluación Comparativa, Herramientas y Análisis de Pruebas, Conceptos de verificación y validación, Planificación y Tipos de Pruebas, Prácticas Avanzadas de Pruebas. ▪ Compiladores seguros y generación de código seguro Traducción y Ejecución de Lenguajes, Comportamiento en Tiempo de Ejecución y Sistemas.	▪ Describir diferentes tipos de software malicioso [Describir] ▪ Explicar los riesgos del mal uso de interfaces con código de terceros y cómo usar correctamente el código de terceros [Explicar] ▪ Discutir la necesidad de actualizar el software para corregir vulnerabilidades de seguridad y la gestión del ciclo de vida de la corrección [Debatir] ▪ Aplicar herramientas estáticas y dinámicas para identificar fallos de programación [Aplicar] ▪ Evaluar un sistema para detectar la existencia de malware y eliminarlo [Evaluar] ▪ Implementar técnicas preventivas para reducir la ocurrencia de ransomware [Implementar]
Lecturas : [**SikorskiHonig2012**], [**Eilam2005**], [**NIST800-53**]	

Unidad 5: Análisis de Amenazas e Ingeniería de Seguridad (8 horas)	
Resultados esperados: ABET-2,ABET-3	
Temas	**Aprendizaje esperado (*Learning Outcomes*)**
▪ Objetivos de la ingeniería de seguridad: construir sistemas que permanezcan confiables a pesar de errores, accidentes o adversarios maliciosos Prácticas de Codificación, Construcción a Escala y Proceso, Pruebas de Rendimiento y Evaluación Comparativa, Herramientas y Análisis de Pruebas, Conceptos de verificación y validación, Planificación y Tipos de Pruebas, Prácticas Avanzadas de Pruebas, Delitos y Ataques Informáticos, Leyes, Políticas y Responsabilidad en Seguridad. ▪ Análisis de problemas y análisis situacional para abordar la seguridad del sistema Pruebas de Rendimiento y Evaluación Comparativa, Herramientas y Análisis de Pruebas, Conceptos de verificación y validación, Planificación y Tipos de Pruebas, Prácticas Avanzadas de Pruebas. ▪ Análisis de seguridad, que cubre análisis de requisitos de seguridad; análisis de controles de seguridad; análisis de amenazas; y análisis de vulnerabilidades Análisis de Programas y Analizadores, Evaluación. ▪ Dominios de ataque de seguridad y superficies de ataque, por ejemplo, comunicaciones y redes, hardware, físico, ingeniería social, software y cadena de suministro Seguridad de Red. ▪ Modos, técnicas y tácticas de ataque de seguridad, por ejemplo, abuso de autenticación; fuerza bruta; manipulación de búfer; inyección de código; inserción de contenido; denegación de servicio; escucha; omisión de función; suplantación; ataque de integridad; intercepción; phishing; análisis de protocolo; abuso de privilegio; suplantación (spoofing); e inyección de tráfico Seguridad de Red, Protección y Seguridad, Pruebas de Rendimiento y Evaluación Comparativa, Herramientas y Análisis de Pruebas, Conceptos de verificación y validación, Planificación y Tipos de Pruebas, Prácticas Avanzadas de Pruebas.	▪ Crear un modelo de amenazas para un sistema o diseño de sistema [Crear] ▪ Aplicar análisis situacional para desarrollar soluciones seguras bajo un escenario especificado [Aplicar] ▪ Identificar y mitigar vulnerabilidades y debilidades de seguridad en un sistema [Analizar]
Lecturas : [**Anderson2020**]	

Unidad 6: Técnicas de Informática Forense (6 horas)	
Resultados esperados: ABET-2,ABET-3	
Temas	**Aprendizaje esperado (*Learning Outcomes*)**
▪ Principios y metodologías básicas para la informática forense. ▪ Diseño de sistemas para informática forense. ▪ Informática forense en diferentes situaciones: sistemas operativos, sistemas de archivos, informática forense de aplicaciones, informática forense web, informática forense de red, informática forense de dispositivos móviles, uso de auditoría de bases de datos Seguridad de Red. ▪ Ataques a la informática forense y prevención de tales ataques.	▪ Explicar qué es una investigación digital y cómo se puede implementar Delitos y Ataques Informáticos, Leyes, Políticas y Responsabilidad en Seguridad [Explicar] ▪ Diseñar e implementar software para apoyar la informática forense [Diseñar] ▪ Extraer datos de un disco duro para cumplir con la ley Delitos y Ataques Informáticos, Leyes, Políticas y Responsabilidad en Seguridad [Extraer] ▪ Recuperar datos basados en un término de búsqueda dado desde un sistema del que se ha hecho una imagen (imaged) [Analizar] ▪ Reconstruir datos y eventos a partir de un historial de aplicación, o un artefacto web, o una base de datos en la nube, o un dispositivo móvil. Plataformas Móviles: Capacidades y Computación Asíncrona, Plataformas Móviles: Arquitectura y Restricciones, Plataformas Móviles: Fundamentos del Desarrollo, Arquitectura Cloud y Gestión de Datos, Frontend, Frameworks y Estándares Web [Aplicar] ▪ Capturar y analizar tráfico de red. Seguridad de Red [Analizar] ▪ Desarrollar enfoques para abordar los desafíos asociados con la informática forense de dispositivos móviles [Crear] ▪ Aplicar herramientas de informática forense para investigar violaciones de seguridad [Aplicar] ▪ Identificar y mitigar métodos anti-forenses [Analizar]
Lecturas : [**Pfleeger2015**]	

Unidad 7: Gobierno, Gestión y Política de Seguridad (6 horas)	
Resultados esperados: ABET-2,ABET-3	
Temas	**Aprendizaje esperado (*Learning Outcomes*)**
▪ Proteger activos críticos de amenazas. ▪ Gobierno de seguridad (security governance): objetivos organizacionales y evaluación general de riesgos. ▪ Gestión de seguridad (security management): lograr y mantener niveles apropiados de confidencialidad, integridad, disponibilidad, responsabilidad (accountability), autenticidad y confiabilidad Pruebas de Rendimiento y Evaluación Comparativa, Herramientas y Análisis de Pruebas, Conceptos de verificación y validación, Planificación y Tipos de Pruebas, Prácticas Avanzadas de Pruebas. ▪ Política de seguridad (security policy): políticas organizacionales, políticas específicas de temas, políticas específicas de sistemas.	▪ Describir activos críticos y cómo pueden protegerse [Describir] ▪ Diferenciar entre gobierno de seguridad, gestión y controles, dando ejemplos de cada uno [Diferenciar] ▪ Describir un control técnico e implementarlo para mitigar amenazas específicas [Describir]
Lecturas : [**Anderson2020**]	

Unidad 8: Ética, Ley y Sociedad en Seguridad (6 horas)	
Resultados esperados: ABET-2,ABET-3	
Temas	**Aprendizaje esperado (*Learning Outcomes*)**
▪ Impactos sociales de las fallas en seguridad y privacidad Equidad Digital y Accesibilidad, Impacto Social e IA, Libertades Civiles y Expresión, Datos, Vigilancia y Tecnología de Privacidad, Fundamentos Filosóficos y Legislación de Privacidad, Delitos y Ataques Informáticos, Leyes, Políticas y Responsabilidad en Seguridad. ▪ Aplicabilidad de leyes y regulaciones sobre seguridad y privacidad Delitos y Ataques Informáticos, Leyes, Políticas y Responsabilidad en Seguridad. ▪ Consideraciones éticas profesionales al diseñar sistemas seguros y mantener la privacidad; hacking ético Libertades Civiles y Expresión, Datos, Vigilancia y Tecnología de Privacidad, Fundamentos Filosóficos y Legislación de Privacidad, Códigos de Ética y Responsabilidad Legal, Responsabilidad Profesional y Política Pública, Valores, Naturaleza y Actualización Profesional, Disidencia Ética y Contexto Cultural, Ética en el Lugar de Trabajo, Delitos y Ataques Informáticos, Leyes, Políticas y Responsabilidad en Seguridad. ▪ Implicaciones de seguridad y privacidad de actores maliciosos de IA/aprendizaje automático, por ejemplo, identificación de deep fakes Formulación del Aprendizaje Automático y Evaluación, Aprendizaje Profundo, RL y Ética, Introducción a la IA: Conceptos y Comportamiento Inteligente, Características del Problema y Naturaleza de los Agentes, Fundamentos de Aprendizaje Automático, Aprendizaje Automático: Datos, Representaciones y Evaluación, Redes Neuronales y Ética, Libertades Civiles y Expresión, Datos, Vigilancia y Tecnología de Privacidad, Fundamentos Filosóficos y Legislación de Privacidad, Delitos y Ataques Informáticos, Leyes, Políticas y Responsabilidad en Seguridad. ▪ Impactos sociales de los dispositivos del Internet de las Cosas (IoT) y otras tecnologías emergentes en la seguridad y la privacidad Libertades Civiles y Expresión, Datos, Vigilancia y Tecnología de Privacidad, Fundamentos Filosóficos y Legislación de Privacidad, Delitos y Ataques Informáticos, Leyes, Políticas y Responsabilidad en Seguridad.	▪ Calcular el impacto de una falla de seguridad en un sistema dado [Calcular] ▪ Construir un sistema que se ajuste a las leyes de seguridad [Crear] ▪ Aplicar un conjunto de regulaciones de privacidad para diseñar un sistema que proteja la privacidad [Aplicar] ▪ Evaluar las ramificaciones legales de un sistema que no se ajusta a las leyes y regulaciones aplicables [Evaluar]
Lecturas : [**Anderson2020**], [**Pfleeger2015**]	

7. PLAN DE TRABAJO

7.1 Metodología

Se fomenta la participación individual y en equipo para exponer sus ideas, motivándolos con puntos adicionales en las diferentes etapas de la evaluación del curso.

7.2 Sesiones Teóricas

Las sesiones de teoría se llevan a cabo en clases magistrales donde se realizarán actividades que propicien un aprendizaje activo, con dinámicas que permitan a los estudiantes interiorizar los conceptos.

7.3 Sesiones Prácticas

Las sesiones prácticas se llevan en clase donde se desarrollan una serie de ejercicios y/o conceptos prácticos mediante planteamiento de problemas, la resolución de problemas, ejercicios puntuales y/o en contextos aplicativos.

8. SISTEMA DE EVALUACIÓN

********* EVALUATION MISSING ********

9. BIBLIOGRAFÍA BÁSICA