Universidad Nacional de Ingeniería (UNI)
Escuela Profesional de
Ciencia de la Computación
Sílabo 2026-I

1. CURSO

CS3I1. Seguridad en Computación (Obligatorio)

2. INFORMACIÓN GENERAL

2.1 Curso	:	CS3I1. Seguridad en Computación
2.2 Semestre	:	8^{vo} Semestre.
2.3 Créditos	:	3
2.4 Horas	:	1 HT; 4 HP;
2.5 Duración del periodo	:	16 semanas
2.6 Condición	:	Obligatorio
2.7 Modalidad de aprendizaje	:	Presencial
2.8 Prerrequisitos	:	CS231. Redes y Comunicación. (6^{to} Sem)

3. PROFESORES

Atención previa coordinación con el profesor

4. 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 gobiernar sistemas seguros, comprendiendo las responsabilidades éticas y profesionales involucradas en la protección de la información y la infraestructura.

5. 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.

6. RESULTADOS DEL ESTUDIANTE

AG-C11) Uso de Herramientas: Aplica herramientas modernas de computación en la resolución de problemas. (Usage)

AG-C09) Diseño y Desarrollo de Soluciones: Diseña, implementa y evalúa soluciones para problemas complejos de computación. (Usage)

7. TEMAS

Unidad 1: Principios y Mentalidad de Seguridad (6 horas)	
Resultados esperados: AG-C09,AG-C11	
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 Sistemas Operativos (OS)-Protection. • Denegación de Servicio (DoS) y Denegación de Servicio Distribuida (DDoS) Sistemas Operativos (OS)-Protection. • 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 Sistemas Operativos (OS)-Principles,OS-Protection,SE-Construction,SEP-Security. • Consideraciones de optimización entre seguridad, privacidad, rendimiento y otros objetivos de diseño Fundamentos de Desarrollo de Software (SDF)-Practices,SE-Validation,HCI-SystemDesign. • 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 : [PPM15], [Sta17]	

Unidad 2: Fundamentos de Criptografía (8 horas)	
Resultados esperados: AG-C09,AG-C11	
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 Fundamentos Matemáticos y Estadísticos (MSF)-Discrete,MSF-Linear. • Criptografía básica: criptografía de clave simétrica y de clave pública Fundamentos Algorítmicos (AL)-FoundationalDataStructuresAlgorithms,MSF-Discrete. • Criptosistemas clásicos, como cifrados de desplazamiento, sustitución, transposición, libros de códigos y máquinas Fundamentos Matemáticos y Estadísticos (MSF)-Discrete. • Principio de Kerckhoff y uso de bibliotecas evaluadas (vetted) Ingeniería de Software (SE)-Construction.	• 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 : [Sta17]	

Unidad 3: Inyección y Validación de Entrada (8 horas)	
Resultados esperados: AG-C09,AG-C11	
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 Sistemas Operativos (OS)-Protection,SDF-Fundamentals,SE-Validation.	• 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 : [PPM15]	

Unidad 4: Análisis de Malware y Seguridad Avanzada (6 horas)	
Resultados esperados: AG-C09	
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 Ingeniería de Software (SE)-Construction,SE-Validation. • Malware: variedades, creación, ingeniería inversa y defensa contra ellos Fundamentos de los Lenguajes de Programación (FPL)-SystemsExecutionMemoryModel,FPL-LanguageTranslationExecution. • Garantía (assurance): pruebas (incluyendo fuzzing y pruebas de penetración), verificación y validación Sistemas Operativos (OS)-Protection,SDF-Fundamentals,SE-Construction,SE-Validation. • Análisis estático y dinámico Fundamentos de los Lenguajes de Programación (FPL)-ProgramAnalysisAnalyzers,OS-Protection,PDC-Evaluation,SE-Validation. • Compiladores seguros y generación de código seguro Fundamentos de los Lenguajes de Programación (FPL)-RunTimeBehaviorSystems,FPL-LanguageTranslationExecution.	• 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 : [SH12], [Eil05], [Nat20]	

Unidad 5: Análisis de Amenazas e Ingeniería de Seguridad (8 horas)	
Resultados esperados: AG-C09,AG-C11	
Temas	**Aprendizaje esperado (*Learning Outcomes*)**
• Objetivos de la ingeniería de seguridad: construir sistemas que permanezcan confiables a pesar de errores, accidentes o adversarios maliciosos Ingeniería de Software (SE)-Construction,SE-Validation,SEP-Security. • Análisis de problemas y análisis situacional para abordar la seguridad del sistema Ingeniería de Software (SE)-Validation. • Análisis de seguridad, que cubre análisis de requisitos de seguridad; análisis de controles de seguridad; análisis de amenazas; y análisis de vulnerabilidades Fundamentos de los Lenguajes de Programación (FPL)-ProgramAnalysisAnalyzers,PDC-Evaluation. • Dominios de ataque de seguridad y superficies de ataque, por ejemplo, comunicaciones y redes, hardware, físico, ingeniería social, software y cadena de suministro Redes y Comunicaciones (NC)-Security. • 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 Redes y Comunicaciones (NC)-Security,OS-Protection,SE-Validation.	• 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 : [And20]	

Unidad 6: Técnicas de Informática Forense (6 horas)	
Resultados esperados: AG-C09,AG-C11	
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 Redes y Comunicaciones (NC)-Security. • Ataques a la informática forense y prevención de tales ataques.	• Explicar qué es una investigación digital y cómo se puede implementar Sociedad, ética y la Profesión (SEP)-Security [Explicar] • Diseñar e implementar software para apoyar la informática forense [Diseñar] • Extraer datos de un disco duro para cumplir con la ley Sociedad, ética y la Profesión (SEP)-Security [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. Desarrollo de Plataformas Especializadas (SPD)-MobilePlatforms,SPD-WebPlatforms [Aplicar] • Capturar y analizar tráfico de red. Redes y Comunicaciones (NC)-Security [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 : [PPM15]	

Unidad 7: Gobierno, Gestión y Política de Seguridad (6 horas)	
Resultados esperados: AG-C09,AG-C11	
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 Ingeniería de Software (SE)-Validation. • 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 : [And20]	

Unidad 8: Ética, Ley y Sociedad en Seguridad (6 horas)	
Resultados esperados: AG-C09,AG-C11	
Temas	**Aprendizaje esperado (*Learning Outcomes*)**
• Impactos sociales de las fallas en seguridad y privacidad Sociedad, ética y la Profesión (SEP)-Context,SEP-Privacy,SEP-Security. • Aplicabilidad de leyes y regulaciones sobre seguridad y privacidad Sociedad, ética y la Profesión (SEP)-Security. • Consideraciones éticas profesionales al diseñar sistemas seguros y mantener la privacidad; hacking ético Sociedad, ética y la Profesión (SEP)-ProfessionalEthics,SEP-Privacy,SEP-Security. • Implicaciones de seguridad y privacidad de actores maliciosos de IA/aprendizaje automático, por ejemplo, identificación de deep fakes Inteligencia Artificial (AI)-IntroductionFundamentalIssues,AI-MachineLearning,SEP-Privacy,SEP-Security. • Impactos sociales de los dispositivos del Internet de las Cosas (IoT) y otras tecnologías emergentes en la seguridad y la privacidad Sociedad, ética y la Profesión (SEP)-Privacy,SEP-Security.	• 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 : [And20], [PPM15]	

8. PLAN DE TRABAJO

8.1 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.

8.2 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.

8.3 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.

9. SISTEMA DE EVALUACIÓN

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

10. BIBLIOGRAFÍA BÁSICA

[Eil05] Eldad Eilam. *Reversing: Secrets of Reverse Engineering*. Indianapolis, IN: Wiley, 2005.

[SH12] Michael Sikorski and Andrew Honig. *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*. San Francisco, CA: No Starch Press, 2012.

[PPM15] Charles P. Pfleeger, Shari Lawrence Pfleeger, and Jonathan Margulies. *Security in Computing*. 5th. Prentice Hall, 2015.

[Sta17] William Stallings. *Computer Security: Principles and Practice*. 4th. Pearson, 2017.

[And20] Ross Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 3rd. Wiley, 2020.

[Nat20] National Institute of Standards and Technology. *Security and Privacy Controls for Information Systems and Organizations*. Tech. rep. NIST SP 800-53 Rev. 5. Disponible en: `https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final`. Gaithersburg, MD: National Institute of Standards and Technology, 2020.