Universidad Nacional de Ingeniería (UNI)
Escuela Profesional de
Ciberseguridad
Sílabo 2024-II

1. CURSO

CY211. Seguridad de Datos (Obligatorio)

2. INFORMACIÓN GENERAL

2.1 Curso	:	CY211. Seguridad de Datos
2.2 Semestre	:	8^{vo} Semestre.
2.3 Créditos	:	3
2.4 horas	:	2 HT; 2 HP;
2.5 Duración del periodo	:	16 semanas
2.6 Condición	:	Obligatorio
2.7 Modalidad de aprendizaje	:	Presencial
2.8 Prerrequisitos	:	CS3I1. Seguridad en Computación. (7^{mo} Sem)

3. PROFESORES

Atención previa coordinación con el profesor

4. INTRODUCCIÓN AL CURSO

Este curso introduce los fundamentos de la seguridad de datos, cruciales para la ciberseguridad. Cubre criptografía, control de acceso, forensia digital, almacenamiento seguro y privacidad, preparando a los estudiantes para analizar amenazas y proteger información sensible.

5. OBJETIVOS

- Dominar los principios de la criptografía y su aplicación en la protección de datos.
- Comprender técnicas de control de acceso y almacenamiento seguro para proteger datos.
- Analizar vulnerabilidades y aplicar prácticas para la seguridad de la información.

6. RESULTADOS DEL ESTUDIANTE

1) Analizar un problema computacional complejo y aplicar los principios computacionales y otras disciplinas relevantes para identificar soluciones. (Assessment)

6) Aplicar principios y prácticas de seguridad para mantener las operaciones en presencia de riesgos y amenazas. (Usage)

7. TEMAS

Unidad 1: Criptografía (12 horas)	
Resultados esperados: 1,6	
Temas	**Objetivos de Aprendizaje (*Learning Outcomes*)**
• Conceptos básicos – Cifrado/descifrado, autenticación del remitente, integridad de datos, no repudio – Clasificación de ataques (solo texto cifrado, texto sin formato conocido, texto sin formato elegido, texto cifrado elegido) – Clave secreta (simétrica), criptografía y criptografía de clave pública (asimétrica) – Seguridad teórica de la información (libreta de un solo uso, teorema de Shannon) – Seguridad computacional • Conceptos avanzados – Protocolos avanzados ∗ Pruebas y protocolos de conocimiento cero ∗ Intercambio de secretos ∗ Compromiso ∗ Transferencia ajena ∗ Computación multipartita segura – Desarrollos recientes avanzados: cifrado totalmente homomórfico, ofuscación, criptografía cuántica y esquema KLJN • Antecedentes matemáticos – Aritmética modular – Teoremas de Fermat y Euler – Raíces primitivas, problema de registros discretos – Prueba de primalidad, factorización de números enteros grandes – Curvas elípticas, celosías y problemas de celosías duras. – Álgebra abstracta, campos finitos. – Teoría de la información. • Cifrados históricos – Cifrado por desplazamiento, cifrado afín, cifrado por sustitución, cifrado Vigenere, ROT-13 – Cifrado Hill, máquina Enigma y otros. • Cifrados simétricos (clave privada) – Cifrados de bloque B y cifrados de flujo (permutaciones pseudoaleatorias, generadores pseudoaleatorios) – Redes Feistel, Estándar de cifrado de datos (DES) – Estándar de cifrado avanzado (AES) – Modos de funcionamiento de cifrados en bloque – Ataque diferencial, ataque lineal.	• Describa el propósito de la criptografía y enumere las formas en que se utiliza en las comunicaciones de datos [Usar] • Describa los siguientes términos: cifrado, criptoanálisis, algoritmo criptográfico y criptología, y describa los dos métodos básicos (cifrados) para transformar texto sin formato en texto cifrado [Usar] • Explique cómo la infraestructura de clave pública admite la firma y el cifrado digitales y analice las limitaciones/vulnerabilidades [Usar] • Discutir los peligros de inventar sus propios métodos criptográficos [Usar] • Describir qué protocolos, herramientas y técnicas criptográficas son apropiados para una situación determinada [Usar] • Explicar los objetivos de la seguridad de datos de un extremo a otro [Usar]

Unidad 2: Integridad y autenticación de datos (12 horas)	
Resultados esperados: 1,6	
Temas	**Objetivos de Aprendizaje (*Learning Outcomes*)**
• Fuerza de autenticación – Autenticación multifactor – Fichas criptográficas – Dispositivos criptográficos – Autenticación biométrica – Contraseñas de un solo uso – Autenticación basada en conocimientos • Técnicas de ataque a contraseñas – Ataque de diccionario – Ataque de fuerza bruta – Ataque a la mesa arcoiris – Phishing e ingeniería social – Ataque basado en malware – Araña – Análisis fuera de línea – Herramientas para descifrar contraseñas • Técnicas de almacenamiento de contraseñas – Funciones hash criptográficas (SHA-256, SHA-3, resistencia a colisiones) – Salazón – Recuento de iteraciones – Derivación de clave basada en contraseña • Integridad de datos – Códigos de autenticación de mensajes (HMAC, CBC-MAC) – Firmas digitales – Cifrado autenticado – árboles de hachís	• Explicar los conceptos de autenticación, autorización, control de acceso e integridad de datos [Usar] • Explicar las diversas técnicas de autenticación y sus fortalezas y debilidades [Usar] • Explicar los distintos ataques posibles a las contraseñas [Usar]
Lecturas : [**owasp2017authentication**]	

Unidad 3: Forense digital (8 horas)	
Resultados esperados: 1,6	
Temas	**Objetivos de Aprendizaje (*Learning Outcomes*)**
• Introducción – Definición – Límites y tipos de herramientas (código abierto versus código cerrado) • Cuestiones legales – Derecho a la privacidad – Cuarta y Quinta Enmiendas – Protección de claves de cifrado según la Quinta Enmienda – Tipos de autoridad legal (consentimiento del propietario, orden de registro, FISA, Título III (escuchas telefónicas), abandono, circunstancias exigentes, a simple vista, etc.) – Protección contra procesos legales (por ejemplo, información del suscriptor del ISP mediante citación, datos transaccionales del servidor de correo electrónico de una orden judicial 2703(d), contenido completo mediante orden de registro, etc.) – Solicitud legal de preservación de evidencia digital (por ejemplo, a través de una carta de preservación 2703(f)) – Declaraciones juradas, testimonios y declaraciones • Herramientas forenses digitales – Tipos – Herramientas centradas en artefactos frente a herramientas todo en uno – Requisitos – Limitaciones • Proceso de investigación – Alertas – Identificación de evidencia – Recopilación y conservación de pruebas. – Cronogramas, informes, cadena de custodia – Autenticación de pruebas • Adquisición y preservación de pruebas – Desconexión versus clasificación – Bloqueo de escritura – Medios de destino preparados forensemente – Procedimientos de imagen – Adquisición de evidencia volátil – Análisis forense en vivo – Cadena de custodia • Análisis de pruebas	• Explicar los conceptos de autenticación, autorización, control de acceso e integridad de datos [Usar] • Describir qué es una investigación digital, las fuentes de evidencia digital y las limitaciones de la ciencia forense [Usar] • Compare y contraste una variedad de herramientas forenses [Usar] • Explicar las diversas técnicas de autenticación y sus fortalezas y debilidades [Usar] • Explicar los distintos ataques posibles a las contraseñas [Usar]

Unidad 4: Seguridad del almacenamiento de información (8 horas)	
Resultados esperados: 1,6	
Temas	**Objetivos de Aprendizaje (*Learning Outcomes*)**
• Disco y cifrado de archivos – Cifrado a nivel de hardware versus el de software. • Borrado de datos – Sobrescritura, desmagnetización – Métodos de destrucción física. – remanencia de la memoria • Enmascaramiento de datos – Enmascaramiento de datos para pruebas. – Enmascaramiento de datos para ofuscación – Enmascaramiento de datos para privacidad • Seguridad de la base de datos – Acceso/autenticación, auditoría – Paradigmas de integración de aplicaciones • Ley de Seguridad de Datos – Este tema presenta los aspectos legales de la seguridad de los datos, las leyes y las políticas que los rigen (por ejemplo, HIPAA). También proporciona una introducción a otros temas relacionados con la ley en el área de conocimiento de Seguridad Organizacional.	• Describir las diversas técnicas para el borrado de datos [Usar]
Lecturas : [**ferguson2003practical**]	

Unidad 5: Privacidad de datos (8 horas)	
Resultados esperados: 1,6	
Temas	**Objetivos de Aprendizaje (*Learning Outcomes*)**
• Descripción general – Definiciones (Brandeis, Solove) – Legales (HIPAA, FERPA, GLBA) – Recopilación de datos – Agregación de datos – Difusión de datos – Invasiones de privacidad – Ingeniería social – Medios de comunicación social	• Describir las diversas técnicas para el borrado de datos [Usar]
Lecturas : [**solove2008understanding**]	

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