MODALIDAD PRESENCIAL

SÍLABO POR COMPETENCIAS

CURSO: CRIPTOGRAFÍA II

DOCENTE: ING BEDER HENRY MEZA VILLANUEVA

SÍLABO DE

CRIPTOGRAFIA II

I. DATOS GENERALES

Línea de Carrera	Seguridad Informática
Semestre Académico	2025-2
Código del Curso	033305353
Créditos	4
Horas Semanales	Hrs. Totales: 6 Teóricas: 2 Practicas: 4
Ciclo	VI
Sección	B
Apellidos y Nombres del Docente	Beder Henry Meza Villanueva
Correo Institucional	bmeza@unjfsc.edu.pe
N° de Celular	989077759

II. SUMILLA Y DESCRIPCIÓN DEL CURSO

El curso de Criptografía II es de carácter teórico-práctico y tiene el propósito de brindar al estudiante la posibilidad de comprender y aplicar las técnicas contemporáneas de sistemas criptográficos.

Introduce al estudiante en los conceptos y elementos fundamentales de la seguridad informática desde las perspectivas siguientes: seguridad lógica y física.

El contenido incluye temas relacionados con la comunicación, la seguridad de la información, seguridad informática, sistemas criptográficos simétricos y asimétricos, aplicaciones de la criptografía.

El curso se desarrollará en 16 semanas, teórico-prácticas, es decir 02 horas de teoría y 04 horas de laboratorio.

III. CAPACIDADES AL FINALIZAR EL CURSO

	CAPACIDAD DE LA UNIDAD DIDÁCTICA	NOMBRE DE LA UNIDAD DIDÁCTICA	SEMANAS
UNIDAD I	Aplica los conceptos y técnicas del Cifrado Simétrico	Fundamentos y Cifrados Simétricos Modernos	**1-4**
UNIDAD II	Aplica los conceptos y técnicas de funciones y protocolos criptográficas	Hashing, Firmas Digitales y Autenticación Moderna	**5-8**
UNIDAD III	Aplica los conceptos y técnicas del Cifrado Asimétrico y Post-cuántica	Criptografía Asimétrica y Post-Cuántica	**9-12**
UNIDAD IV	Aplica los conceptos y técnicas avanzadas en Criptografía	Tendencias Avanzadas en Criptografía	**13-16**

IV. INDICADORES DE CAPACIDADES AL FINALIZAR EL CURSO

NÚMERO	INDICADORES DE CAPACIDAD AL FINALIZAR EL CURSO
1	Introducción a la Criptografía moderna
2	AES y modos de operación seguros (CTR, GCM, XTS)
3	Criptografía ligera (Lightweight Cryptography) para IoT
4	Integrador I
5	Funciones hash seguras
6	Firmas digitales modernas
7	Protocolos de autenticación modernos
8	Integrador II
9	Criptografía de Curvas Elípticas (ECC)
10	Criptografía Post-Cuántica
11	Introducción a Criptografía Multilineal
12	Integrador III
13	Blockchain y Criptografía
14	Criptografía Homomórfica
15	Multi-Party Computation
16	Integrador IV

V.- DESARROLLO DE LAS UNIDADES DIDÁCTICAS:

Cifrado Simétrico	***CAPACIDAD DE LA UNIDAD DIDÁCTICA I:*** Aplica los conceptos y técnicas del Cifrado Simétrico					
	Semana	Contenidos			Estrategia didáctica	Indicadores de logro de la capacidad
		Cognitivos	Procedimental	Actitudinal		
	1	Introducción. Rol en la sociedad digital, NIST, IETF, estándares ISO	Elabora una aplicación haciendo uso de la criptografía.	Discute en equipo los aspectos de la Criptografía	Diapositivas Uso de Proyector Uso de Pizarra	Identifica los elementos y la importancia de la criptografía
	2	AES y modos de operación seguros (CTR, GCM, XTS). Aplicaciones en almacenamiento y comunicaciones seguras	Elabora aplicaciones con Cifrado de Flujo.	Reflexiona acerca del Cifrado de Flujo.		Identifica los elementos y la importancia del Cifrado Simétrico.
	3	Criptografía ligera (Lightweight Cryptography) para IoT .	Elabora aplicaciones con Cifrado DES	Reflexiona acerca del Cifrado DES		Identifica los elementos y la importancia del Cifrado DES
	4	Proyecto de Seguridad simétrica	Elabora, analiza un caso aplicativo	Valora el uso de la Criptografía Simétrica		Desarrolla aplicaciones haciendo uso de cifrado simétrico
Unidad Didáctica I :		**EVALUACIÓN DE LA UNIDAD DIDÁCTICA**				
		EVIDENCIA DE CONOCIMIENTOS	**EVIDENCIA DE PRODUCTO**		**EVIDENCIA DE DESEMPEÑO**	
		Estudios de casos, cuestionario	Trabajos individuales y/o grupales, solución a ejercicios propuestos		Comportamiento en clases virtuales y chat	

	UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN	FACULTAD DE INGENIERÍA INDUSTRIAL, SISTEMAS E INFORMÁTICA	
Código: FIISI-SI-16			Versión: 01
PROCESO: PLANIFICACIÓN			

Funciones y Protocolos Criptográficos	***CAPACIDAD DE LA UNIDAD DIDÁCTICA II:*** Aplica los conceptos y técnicas de funciones y protocolos criptográficas					
	Semana	Contenidos			Estrategia didáctica	Indicadores de logro de la capacidad
		Cognitivos	Procedimental	Actitudinal		
	5	Funciones hash seguras (SHA-3, BLAKE3) y KDFs (Argon2, scrypt).	Elabora aplicaciones con Cifrado AES	Reflexiona acerca del Cifrado AES	Diapositivas Uso de Proyector Uso de Pizarra	Identifica los elementos y la importancia del Cifrado AES
	6	Firmas digitales modernas: ECDSA, EdDSA (Ed25519).	Elabora aplicaciones haciendo uso de las Funciones Hash	Reflexiona acerca de las funciones Hash		Identifica los elementos y la importancia de la Cifrado Hash
	7	Protocolos de autenticación modernos: PAKE (Password-Authenticated Key Exchange), OPAQUE	Elabora aplicaciones haciendo uso Protocolo de Diffie-Hellman	Reflexiona acerca del protocolo de Diffie-Hellman		Identifica los elementos y la importancia del Protocolo de Diffie-Hellman
	8	Proyecto de Funciones Criptografías y Protocolo	Elabora, analiza un caso aplicativo	Valora el uso de Funciones Criptografías y Protocolo.		Desarrolla aplicaciones haciendo uso de funciones criptográficas y protocolo
Unidad Didáctica II:		**EVALUACIÓN DE LA UNIDAD DIDÁCTICA**				
		EVIDENCIA DE CONOCIMIENTOS	**EVIDENCIA DE PRODUCTO**		**EVIDENCIA DE DESEMPEÑO**	
		Estudios de casos, cuestionario	Trabajos individuales y/o grupales, solución a ejercicios propuestos		Comportamiento en clases virtuales y chat	

	UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN	FACULTAD DE INGENIERÍA INDUSTRIAL, SISTEMAS E INFORMÁTICA	
Código: FIISI-SI-16			Versión: 01
PROCESO: PLANIFICACIÓN			

Cifrado Asimétrico	***CAPACIDAD DE LA UNIDAD DIDÁCTICA III:*** Aplica los conceptos y técnicas del Cifrado Asimétrico					
	Semana	Contenidos			Estrategia didáctica	Indicadores de logro de la capacidad
		Cognitivos	Procedimental	Actitudinal		
	9	Criptografía de Curvas Elípticas (ECC): Curve25519, secp256k1, usos en blockchain	Elabora una aplicación haciendo uso de RSA.	Valora el uso de las apps web con RSA	Diapositivas Uso de Proyector Uso de Pizarra	Identifica los elementos y la importancia del Cifrado Asimétrico - RSA
	10	Criptografía Post-Cuántica (PQC) – Algoritmos ganadores de NIST 2022-2024	Elabora aplicaciones haciendo uso de Certificado Digital	Reflexiona acerca de los Certificados digitales		Identifica los elementos y la importancia de Certificado Digital
	11	Introducción a Criptografía Multilineal, Lattice-based y Code-based	Elabora aplicaciones haciendo uso de Blockchain	Reflexiona acerca del Blockchain		Identifica los elementos y la importancia B*lockchain*
	12	Proyecto de Seguridad Cifrado Asimétrico	Elabora, analiza un caso aplicativo	Valora el Cifrado asimétrico		Desarrolla aplicaciones haciendo uso de cifrado asimétrico.
Unidad Didáctica III :		**EVALUACIÓN DE LA UNIDAD DIDÁCTICA**				
		EVIDENCIA DE CONOCIMIENTO	**EVIDENCIA DE PRODUCTO**		**EVIDENCIA DE DESEMPEÑO**	
		Estudios de casos, cuestionario	Trabajos individuales y/o grupales, solución a ejercicios propuestos		Comportamiento en clases virtuales y chat	

	UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN	FACULTAD DE INGENIERÍA INDUSTRIAL, SISTEMAS E INFORMÁTICA	
Código: FIISI-SI-16			Versión: 01
PROCESO: PLANIFICACIÓN			

: Seguridad en las aplicaciones web	***CAPACIDAD DE LA UNIDAD DIDÁCTICA IV:*** Aplica los conceptos y técnicas de las aplicaciones web					
	Semana	Contenidos			Estrategia didáctica	Indicadores de logro de la capacidad
		Cognitivos	Procedimental	Actitudinal		
	13	Blockchain y Criptografía: Merkle Trees, zk-SNARKs, zk-STARKs, pruebas de conocimiento cero	Elabora aplicaciones haciendo uso de Sesiones y Cookies	Valora el uso de Sesiones y Cookies	Diapositivas Uso de Proyector Uso de Pizarra	dentifica lo elementos y la importancia de la seguridad de las AppWeb, Sesión y Cookies
	14	Criptografía Homomórfica (HE): Fully Homomorphic Encryption (FHE) y aplicaciones en privacidad	Elabora aplicaciones con protección a ataques injection	Valora la protección de ataques injection		Identifica lo elementos y la importancia de los ataques SQL Injection y XSS
	15	Multi-Party Computation (MPC) y aplicaciones en finanzas descentralizadas (DeFi).	Realiza un mapa mental en relación a la Seguridad en Red	Valora el uso de la seguridad ea nivel TCP/IP		Identifica los elementos y la importancia de la Protección a Nivel de red
	16	Proyecto de Seguridad de aplicaciones web	Elabora, analiza un caso aplicativo	Valora el uso de la Seguridad de las aplicaciones web		Desarrolla de aplicaciones web seguras
Unidad Didáctica IV :		**EVALUACIÓN DE LA UNIDAD DIDÁCTICA**				
		EVIDENCIA DE CONOCIMIENTOS	**EVIDENCIA DE PRODUCTO**		**EVIDENCIA DE DESEMPEÑO**	
		Estudios de casos, cuestionario	Trabajos individuales y/o grupales, solución a ejercicios propuestos		Comportamiento en clases virtuales y chat	

VI. MATERIALES EDUCATIVOS Y OTROS RECURSOS DIDÁCTICOS

Los materiales educativos y recursos didácticos que se utilizaran en el desarrollo del presente curso:

1. MEDIOS ESCRITOS

- Materiales convencionales como separatas, guías de prácticas y pizarra
- Material de apoyo del curso.

2. MEDIOS VISUALES Y ELECTRÓNICOS

- Materiales audiovisuales como videos
- Presentaciones multimedia, animaciones y simulaciones interactivas.
- Servicios telemáticos: sitios web, correo electrónico, chats, foros.

3. MEDIOS INFORMÁTICOS

- Laptop con conexión a internet
- Programas informáticos (CD u on-line) educativos
- Uso de plataformas virtual con fines educativos

VII. EVALUACIÓN

La Evaluación es inherente al proceso de enseñanza aprendizaje y será continua y permanente. Los criterios de evaluación son de conocimiento, de desempeño y de producto.

1. Evidencias de Conocimiento.

La Evaluación será a través de pruebas escritas y orales para el análisis y autoevaluación. En cuanto al primer caso, medir la competencia a nivel interpretativo, argumentativo y propositivo, para ello debemos ver como identifica (describe, ejemplifica, relaciona, reconoce, explica, etc.); y la forma en que argumenta (plantea una afirmación, describe las refutaciones en contra de dicha afirmación, expone sus argumentos contra las refutaciones y llega a conclusiones) y la forma en que propone a través de establecer estrategias, valoraciones, generalizaciones, formulación de hipótesis, respuesta a situaciones, etc.

En cuanto a la autoevaluación permite que el estudiante reconozca sus debilidades y fortalezas para corregir o mejorar.

Las evaluaciones de este nivel serán de respuestas simples y otras con preguntas abiertas para su argumentación.

1. EVIDENCIA DE CONOCIMIENTO		**PORCENTAJE**	**PONDERACION**	**INSTRUMENTOS**
UNIDAD I	Evaluación escrita de 50 preguntas, utilizando plataforma para el manejo de saberes de los métodos de investigación.	5%	0.05	Cuestionario
UNIDAD II	Evaluación escrita de 50 preguntas, utilizando plataforma para el manejo de saberes de los proyectos de investigación en tecnología.	7%	0.07	Cuestionario
UNIDAD III	Evaluación escrita de 50 preguntas, utilizando plataforma para el manejo de saberes de la investigación en ingeniería	8%	0.08	Cuestionario
UNIDAD IV	Evaluación escrita de 50 preguntas, utilizando plataforma para el manejo de saberes de los informes científicos. Se incluirán en la evaluación mínimo dos videos.	10%	0.1	Cuestionario/videos
Total Evidencia de Conocimiento		**30%**	**0.3**	

2. Evidencia de Producto.

Están implicadas en las finalidades de la competencia, por tanto, no es simplemente la entrega del producto, sino que tiene que ver con el campo de acción y los requerimientos del contexto de aplicación.

La evaluación de producto de evidencia en la entrega oportuna de sus trabajos parciales y el trabajo final.

Además, se tendrá en cuenta la asistencia como componente del desempeño, el 30% de inasistencia inhabilita el derecho a la evaluación.

2. EVIDENCIA DEL PRODUCTO	**PORCENTAJE**	**PONDERACION**	**INSTRUMENTOS**
1. Presentación del primer avance del proyecto formativo.	5%	0.05	Trabajo impreso de acuerdo al formato establecido
2. Contenido de forma y fondo	15%	0.15	
3. Aportes hechos al trabajo	15%	0.15	
Total Evidencia del Producto	**35%**	**0.35**	

3. Evidencia de Desempeño.

Esta evidencia pone en acción recursos cognitivos, recursos procedimentales y recursos afectivos; todo ello en una integración que evidencia un saber hacer reflexivo; en tanto, se puede verbalizar

lo que se hace, fundamentar teóricamente la práctica y evidenciar un pensamiento estratégico, dado en la observación en torno a cómo se actúa en situaciones impredecibles.
La evaluación de desempeño se evalúa ponderando como el estudiante se hace investigador aplicando los procedimientos y técnicas en el desarrollo de las clases a través de su asistencia y participación asertiva.

3. EVIDENCIA DEL DESEMPEÑO	PORCENTAJE	PONDERACION	INSTRUME
1. Presentación oportuna del trabajo	5%	0.05	Responsabil en la entre avances d proyectos formativos
2. Formular un procedimiento para hacer el mejor planteamiento de la solución posibles.	15%	0.15	
3. Discriminar las soluciones posibles y propone una solución la que permite resolver el problema.	15%	0.15	
Total Evidencia del Desempeño	**35%**	**0.35**	

VARIABLES	PONDERACIONES	UNIDADES DIDÁCTICAS DENOMINADAS MÓDULOS
Evaluación de Conocimiento	**30 %**	El ciclo académico comprende 4
Evaluación de Producto	**35%**	
Evaluación de Desempeño	**35 %**	

Siendo el promedio final (PF), el promedio simple de los promedios ponderados de cada módulo (PM1, PM2, PM3, PM4)

$$PF = \frac{PM1 + PM2 + PM3 + PM4}{4}$$

CRONOGRAMA ACADEMICO

EVALUACIONES DEL SEMESTRE ACADÉMICO	DEL	AL
Módulo I	28/04/2025	02/05/2025
Módulo II - I PARCIAL (Plan por Objetivos)	26/05/2025	30/05/2025
Módulo III	23/06/2025	27/06/2025
Módulo IV - II PARCIAL (Plan por objetivos)	21/07/2025	25/07/2025
Examen Sustitutorio (Plan por Objetivos)	25/07/2025	
INGRESO DE NOTAS AL SISTEMA	**DEL**	**AL**
Módulo I	05/05/2025	11/05/2025
Módulo II - I PARCIAL (Plan por objetivos)	02/06/2025	08/06/2025
Módulo III	30/06/2025	06/07/2025
Módulo IV - II PARCIAL (Plan por objetivos)	28/07/2025	03/082025
FINALIZAR Y GENERAR ACTA POR EL DOCENTE RESPONSABLE DEL CURSO A CARGO	**28/07/2025**	**03/08/2025**
IMPRESIÓN Y FIRMA DE ACTAS POR PARTE DE: ORAA Y DOCENTE DE CURSO	**30/07/2025**	**04/08/2025**
Al finalizar cada Módulo y/o Parcial el Director de Escuela Profesional Informa al Decano el incumplimiento de los docentes sobre el ingreso de notas al sistema, en sus dos modalidades.		
Inicio y término de clases	**07/04/2025**	**25/07/2025**

VIII. BIBLIOGRAFÍA Y REFERENCIAS WEB

UNIDAD DIDACTICA I:

- **García, A. (2011).** Seguridad Informática.
- **Christof Paar, Jan Pelzl. (2010).** Understanding Cryptography
- **Katz, J. and Lindell, Y. (2014).** *Introduction to Modern Cryptography, Second Edition*. Hoboken: CRC Press.

UNIDAD DIDACTICA II:

- **García, A. (2011).** Seguridad Informática.
- **Christof Paar, Jan Pelzl. (2010).** Understanding Cryptography
- **Katz, J. and Lindell, Y. (2014).** *Introduction to Modern Cryptography, Second Edition*. Hoboken: CRC Press.

UNIDAD DIDACTICA III:

- **García, A. (2011).** Seguridad Informática.
- **Christof Paar, Jan Pelzl. (2010).** Understanding Cryptography
- **Katz, J. and Lindell, Y. (2014).** *Introduction to Modern Cryptography, Second Edition*. Hoboken: CRC Press.

UNIDAD DIDACTICA IV:

- **García, A. (2011).** Seguridad Informática.
- **Christof Paar, Jan Pelzl. (2010).** Understanding Cryptography
- **Katz, J. and Lindell, Y. (2014).** *Introduction to Modern Cryptography, Second Edition*. Hoboken: CRC Press.

Huacho, setiembre, 2025

Ing. Beder Henry Meza Villanueva
Docente auxiliar