UNIVERSIDAD NACIONAL
"JOSÉ FAUSTINO SÁNCHEZ CARRIÓN"
VICERRECTORADO ACADÉMICO

SYLLABUS PARA CLASES VIRTUALES EN LA FIISI - UNJFSC

FACULTAD DE INGENIERÍA INDUSTRIAL, SISTEMAS E INFORMÁTICA

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA

MODALIDAD NO PRESENCIAL

SÍLABO POR COMPETENCIAS

CURSO:

Criptografía I

I. DATOS GENERALES

Línea de Carrera	SEGURIDAD INFORMÁTICA
Semestre Académico	2020-I
Código del Curso	303
Créditos	04
Horas Semanales	Hrs. Totales: 06 Teóricas: 02 Practicas: 04
Ciclo	V
Sección	A
Apellidos y Nombres del Docente	Vergara Quiche, Renzo Iván
Correo Institucional	rvergara@unjfsc.edu.pe
N° De Celular	998996143

II. SUMILLA

La asignatura de Criptografía I corresponde al Área de estudios de Seguridad Informática, el curso de Criptografía I es de carácter teórico-práctico y tiene el propósito de brindar al estudiante la posibilidad de comprender que la comunicación como parte esencial de la humanidad debe acontecer en entornos fiables y seguros, sobre todo en el contexto informático. El contenido incluye temas relacionados con la comunicación y la seguridad de la información, seguridad informática, criptografía, esteganografía, métodos criptográficos y criptoanálisis.

III. CAPACIDADES AL FINALIZAR EL CURSO

	CAPACIDAD DE LA UNIDAD DIDÁCTICA	NOMBRE DE LA UNIDAD DIDÁCTICA	SEMANAS
UNIDAD I	Según las necesidades aplica los conceptos y principios de la comunicación y la seguridad de la información y seguridad informática.	LA COMUNICACIÓN Y LA SEGURIDAD	**1-4**
UNIDAD II	De acuerdo al contexto identifica la criptografía y su evolución y aplica las técnicas criptográficas clásicas.	LA CRIPTOGRAFÍA Y TÉCNICAS CRIPTOGRÁFICAS CLÁSICAS 1	**5-8**
UNIDAD III	De acuerdo al contexto aplica las diferentes técnicas criptográficas clásicas.	TÉCNICAS CRIPTOGRÁFICAS CLÁSICAS 2	**9-12**
UNIDAD IV	De acuerdo al contexto aplica las técnicas de criptoanálisis clásicas.	TÉCNICAS DE CRIPTOANÁLISIS Y CRIPTOSISTEMAS	**13-16**

IV. INDICADORES DE CAPACIDADES AL FINALIZAR EL CURSO

N°	INDICADORES DE CAPACIDAD AL FINALIZAR EL CURSO
1	Detalla el rol de la Comunicación y la seguridad de la información en las organizaciones mediante esquemas y ejemplos.
2	Detalla el rol de la Comunicación y la seguridad informática en las organizaciones mediante esquemas y ejemplos.
3	Identifica los tipos de malware y su gestión precisando ejemplos.
4	Identifica a los hackers y crackers mediante esquemas y ejemplos.
5	Comprende la aplicación de la criptografía en el proceso de comunicación mediante esquemas.
6	Aplica los métodos criptográficos clásicos en el diseño de aplicativos.
7	Aplica los métodos criptográficos clásicos en el diseño de aplicativos.

8	Aplica los métodos criptográficos clásicos en el diseño de aplicativos.
9	Aplica los métodos criptográficos clásicos en el diseño de aplicativos.
10	Aplica los tipos de cifrado por transposición en el diseño de aplicativos.
11	Explica el funcionamiento de las máquinas de cifrado y su funcionamiento mediante esquemas.
12	Identifica la aplicación de la criptografía cuántica como alternativa de solución tecnológica emergente mediante esquemas.
13	Comprende la aplicación del criptoanálisis como una herramienta de descifrado de códigos mediante esquemas.
14	Aplica los métodos de criptoanálisis en el diseño de aplicativos.
15	Comprende la aplicación de los Criptosistemas de cifrado con clave secreta mediante esquemas y ejemplos.
16	Comprende la aplicación de los Criptosistemas de cifrado con clave pública mediante esquemas y ejemplos.

V. DESARROLLO DE LAS UNIDADES DIDÁCTICAS:

UNIDAD DIDÁCTICA I: LA COMUNICACIÓN Y LA SEGURIDAD.

CAPACIDAD DE LA UNIDAD DIDÁCTICA I: Según las necesidades aplica los conceptos y principios de la comunicación y la seguridad de la información y seguridad informática.

SEMANA	CONTENIDOS			ESTRATEGIAS DE LA ENSEÑANZA VIRTUAL	INDICADORES DE LOGRO DE LA CAPACIDAD
	CONCEPTUAL	PROCEDIMENTAL	ACTITUDINAL		
1	La comunicación y la seguridad de la información.	Analiza la importancia de la comunicación y la seguridad de la información para una organización.	Valora el impacto del proceso de la comunicación y la Seguridad de la información en la realidad.	**Expositiva (Docente/Alumno)** • Uso del Google Meet	Detalla el rol de la Comunicación y la seguridad de la información en las organizaciones mediante esquemas y ejemplos.
2	La comunicación y la seguridad informática.	Analiza la importancia de la comunicación y la seguridad informática para una organización.	Valora el impacto del proceso de la comunicación y la Seguridad informática en la realidad.	**Debate dirigido (Discusiones)** • Foros, Chat	Detalla el rol de la Comunicación y la seguridad informática en las organizaciones mediante esquemas y ejemplos.
3	El malware, concepto, tipos, evolución, detección, prevención y eliminación.	Evalúa y analiza los tipos de malware y sus consecuencias.	Propicia el trabajo en equipo para determinar la aplicabilidad del malware.	**Lecturas** • Uso de repositorios digitales	Identifica los tipos de malware y su gestión precisando ejemplos.
4	Los hackers y crackers.	Evalúa y analiza los hacker y los crackers.	Propicia el trabajo en equipo para determinar las características de expertos cibernéticos.	**Lluvia de ideas (Saberes previos)** • Foros, Chat	Identifica a los hackers y crackers mediante esquemas y ejemplos.

EVALUACIÓN DE LA UNIDAD DIDÁCTICA

EVIDENCIA DE CONOCIMIENTOS	EVIDENCIA DE PRODUCTO	EVIDENCIA DE DESEMPEÑO
• Estudios de Casos • Cuestionarios	• Trabajos individuales y/o grupales • Soluciones a Ejercicios propuestos	• Comportamiento en clase virtual y chat

UNIDAD DIDÁCTICA II: LA CRIPTOGRAFÍA Y TÉCNICAS CRIPTOGRÁFICAS CLÁSICAS 1.

CAPACIDAD DE LA UNIDAD DIDÁCTICA II: De acuerdo al contexto identifica la criptografía y su evolución y aplica las técnicas criptográficas clásicas.

SEMANA	CONTENIDOS			ESTRATEGIAS DE LA ENSEÑANZA VIRTUAL	INDICADORES DE LOGRO DE LA CAPACIDAD
	CONCEPTUAL	PROCEDIMENTAL	ACTITUDINAL		
5	La criptografía, historia, elementos, tendencias, diferencia con la esteganografía.	Identifica y analiza los elementos de la criptografía y estenografía.	Acrecienta el interés de conocer la criptografía y su relación con la esteganografía.	**Expositiva (Docente/Alumno)** • Uso del Google Meet	Comprende la aplicación de la criptografía en el proceso de comunicación mediante esquemas.
6	Métodos criptográficos clásicos: el cifrado de cesar, cifrado, cifrado ROT13, cifrado ROT47.	Identifica y analiza la estructura y funcionamiento de los métodos criptográficos.	Propicia el trabajo individual y en equipo para realizar los métodos criptográficos.	**Debate dirigido (Discusiones)** • Foros, Chat	Aplica los métodos criptográficos clásicos en el diseño de aplicativos.
7	Métodos criptográficos clásicos: la escítala, cifrado atbash, cifrado polybios.	Identifica y analiza la estructura y funcionamiento de los métodos criptográficos.	Propicia el trabajo individual y en equipo para realizar los métodos criptográficos.	**Lecturas** • Uso de repositorios digitales	Aplica los métodos criptográficos clásicos en el diseño de aplicativos.
8	Métodos criptográficos clásicos: cifrado de Vigenere, cifrado de Alberti.	Identifica y analiza la estructura y funcionamiento de los métodos criptográficos.	Propicia el trabajo individual y en equipo para realizar los métodos criptográficos.	**Lluvia de ideas (Saberes previos)** • Foros, Chat	Aplica los métodos criptográficos clásicos en el diseño de aplicativos.

EVALUACIÓN DE LA UNIDAD DIDÁCTICA		
EVIDENCIA DE CONOCIMIENTOS	**EVIDENCIA DE PRODUCTO**	**EVIDENCIA DE DESEMPEÑO**
• Estudios de Casos • Cuestionarios	• Trabajos individuales y/o grupales • Soluciones a Ejercicios propuestos	• Comportamiento en clase virtual y chat

UNIDAD DIDÁCTICA III: TÉCNICAS CRIPTOGRÁFICAS CLÁSICAS 2.

CAPACIDAD DE LA UNIDAD DIDÁCTICA III: De acuerdo al contexto aplica las diferentes técnicas criptográficas clásicas.

SEMANA	CONTENIDOS			ESTRATEGIAS DE LA ENSEÑANZA VIRTUAL	INDICADORES DE LOGRO DE LA CAPACIDAD
	CONCEPTUAL	PROCEDIMENTAL	ACTITUDINAL		
9	Métodos criptográficos clásicos: cifrado de Playfair, cifrado de Hill.	Identifica y analiza la estructura y funcionamiento de los métodos criptográficos.	Propicia el trabajo individual y en equipo para realizar los métodos criptográficos.	**Expositiva (Docente/Alumno)** • Uso del Google Meet	Aplica los métodos criptográficos clásicos en el diseño de aplicativos.
10	Métodos criptográficos clásicos: transposición por grupos, transposición por series, transposición por columnas/filas.	Identifica y analiza la estructura y funcionamiento de los métodos criptográficos.	Propicia el trabajo individual y en equipo para realizar los métodos criptográficos.	**Debate dirigido (Discusiones)** • Foros, Chat	Aplica los tipos de cifrado por transposición en el diseño de aplicativos.
11	Métodos criptográficos clásicos: cifrado ADFGVX, Enigma, cifrado purpura, cifras Tipex, cifras SIGABA.	Identifica y analiza la estructura y funcionamiento de los métodos criptográficos.	Propicia el trabajo individual y en equipo para comprender el funcionamiento de las máquinas de cifrado.	**Lecturas** • Uso de repositorios digitales	Explica el funcionamiento de las máquinas de cifrado y su funcionamiento mediante esquemas.
12	Introducción a la criptografía cuántica.	Analiza el funcionamiento de la criptografía cuántica.	Propicia el trabajo individual y en equipo para para comprender el funcionamiento de la criptografía cuántica.	**Lluvia de ideas (Saberes previos)** • Foros, Chat	Identifica la aplicación de la criptografía cuántica como alternativa de solución tecnológica emergente mediante esquemas.

EVALUACIÓN DE LA UNIDAD DIDÁCTICA		
EVIDENCIA DE CONOCIMIENTOS	**EVIDENCIA DE PRODUCTO**	**EVIDENCIA DE DESEMPEÑO**
• Estudios de Casos • Cuestionarios	• Trabajos individuales y/o grupales • Soluciones a Ejercicios propuestos	• Comportamiento en clase virtual y chat

UNIDAD DIDÁCTICA IV: TÉCNICAS DE CRIPTOANÁLISIS Y CRIPTOSISTEMAS.

CAPACIDAD DE LA UNIDAD DIDÁCTICA IV: De acuerdo al contexto aplica las técnicas de criptoanálisis clásicas.

SEMANA	CONTENIDOS			ESTRATEGIAS DE LA ENSEÑANZA VIRTUAL	INDICADORES DE LOGRO DE LA CAPACIDAD
	CONCEPTUAL	PROCEDIMENTAL	ACTITUDINAL		
13	El Criptoanálisis, historia, tendencias, tipos de ataque criptoanalítico.	Identifica y analiza la estructura y funcionamiento de los métodos criptográficos.	Propicia el trabajo individual y en equipo para realizar los métodos criptográficos.	**Expositiva (Docente/Alumno)** • Uso del Google Meet	Comprende la aplicación del criptoanálisis como una herramienta de descifrado de códigos mediante esquemas.
14	Métodos de criptoanálisis clásico: método de fuerza bruta, método de frecuencia, método de Kasiski, método de índice de coincidencia.	Identifica y analiza la estructura y funcionamiento de los métodos criptográficos.	Propicia el trabajo individual y en equipo para realizar los métodos criptográficos.	**Debate dirigido (Discusiones)** • Foros, Chat	Aplica los métodos de criptoanálisis en el diseño de aplicativos.
15	Introducción a los Criptosistemas de cifrado con clave secreta.	Analiza el funcionamiento de la criptografía cuántica.	Propicia el trabajo individual y en equipo para para comprender el funcionamiento de la criptografía cuántica.	**Lecturas** • Uso de repositorios digitales	Comprende la aplicación de los Criptosistemas de cifrado con clave secreta mediante esquemas y ejemplos.
16	Introducción a los Criptosistemas de cifrado con clave pública.	Analiza el funcionamiento de la criptografía cuántica.	Propicia el trabajo individual y en equipo para para comprender el funcionamiento de la criptografía cuántica.	**Lluvia de ideas (Saberes previos)** • Foros, Chat	Comprende la aplicación de los Criptosistemas de cifrado con clave pública mediante esquemas y ejemplos.

EVALUACIÓN DE LA UNIDAD DIDÁCTICA		
EVIDENCIA DE CONOCIMIENTOS	**EVIDENCIA DE PRODUCTO**	**EVIDENCIA DE DESEMPEÑO**
• Estudios de Casos • Cuestionarios	• Trabajos individuales y/o grupales • Soluciones a Ejercicios propuestos	• Comportamiento en clase virtual y chat

VI. MATERIALES EDUCATIVOS Y OTROS RECURSOS DIDÁCTICOS

Se utilizarán todos los materiales y recursos requeridos de acuerdo a la naturaleza de los temas programados. Básicamente serán:

1. **MEDIOS Y PLATAFORMAS VIRTUALES**
   - Casos prácticos
   - Pizarra interactiva
   - Google Meet
   - Repositorios de datos

2. **MEDIOS INFORMATICOS:**
   - Computadora
   - Tablet
   - Celulares
   - Internet.

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.

2. 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 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.

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)

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

VIII. BIBLIOGRAFÍA

8.1. Fuentes Bibliográficas

- Lucena López M. J. (2001) Criptografía y Seguridad en Computadores

8.2. Fuentes Electrónicas

- http://www.criptored.upm.es
- https://www.khanacademy.org/math/applied-math/cryptography/crypt/v/intro-to-cryptography

Huacho……..2020

Universidad Nacional
"José Faustino Sánchez Carrión"

……

Vergara Quiche, Renzo Iván
DCU348