



UNIVERSIDAD NACIONAL
JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

FACULTAD DE INGENIERIA INDUSTRIAL, SISTEMAS E INFORMATICA
ESCUELA PROFESIONAL DE INGENIERIA INFORMÁTICA

SILABO
ASIGNATURA: CRIPTOGRAFÍA I

I. DATOS GENERALES

- 1.1. Código de la Asignatura : 303
- 1.2. Escuela Académico Profesional : Ingeniería Informática
- 1.3. Departamento Académico : Ingeniería de Sistemas e Informática
- 1.4. Ciclo : V
- 1.5. Créditos : 4.0
- 1.6. Plan de Estudios : 05
- 1.7. Condición : Obligatorio
- 1.8. Horas Semanales : 06
 - Horas Teóricas : 02
 - Horas de Práctica : 04
- 1.9. Pre-requisito : 151, 254
- 1.10. Semestre Académico : 2018-1
- 1.11. Docente : Ing. CIP Renzo I. Vergara Quiche
 - Colegiatura : CIP N° 89998
 - Correo Electrónico : renzovergaraq@hotmail.com

II. SUMILLA Y DESCRIPCIÓN DEL CURSO

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.

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

III. CAPACIDADES AL TERMINAR EL CURSO

	CAPACIDAD DE LA UNIDAD DIDACTICA	NOMBRE DE LA UNIDAD DIDACTICA	SEMANAS
UNIDAD I	Aplica los conceptos y principios de la comunicación y la seguridad de la información y seguridad informática.	LA COMUNICACIÓN Y LA SEGURIDAD	1,2,3,4



UNIVERSIDAD NACIONAL
JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

FACULTAD DE INGENIERIA INDUSTRIAL, SISTEMAS E INFORMATICA
ESCUELA PROFESIONAL DE INGENIERIA INFORMÁTICA

UNIDAD II	Identifica los conceptos de criptografía y esteganografía y su evolución y tendencias a través del tiempo.	INTRODUCCIÓN A LA CRIPTOGRAFÍA Y ESTEGANOGRAFÍA	5,6,7,8
UNIDAD III	Aplica las diferentes técnicas criptográficas de cifrado clásico por sustitución y por transposición.	MÉTODOS CRIPTOGRÁFICOS	9,10,11,12
UNIDAD IV	Aplica las diferentes técnicas de criptoanálisis clásicas y técnicas de codificación clásicas.	CRIPTOANÁLISIS	13,14,15,16

IV. DESARROLLO DE LAS UNIDADES DIDÁCTICAS

UNIDAD I: LA COMUNICACIÓN Y LA SEGURIDAD

PRIMERA SEMANA

La comunicación y la seguridad de la información

SEGUNDA SEMANA

La comunicación y la seguridad informática

TERCERA SEMANA

Control de acceso, sistema seguro, control de acceso al sistema, control de acceso a datos

CUARTA SEMANA

Código malicioso: virus, gusanos, troyanos, bombas lógicas, trap doors, otros

UNIDAD II: INTRODUCCIÓN A LA CRIPTOGRAFÍA Y ESTEGANOGRAFÍA

QUINTA SEMANA

La criptografía, historia, evolución, tendencias



UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

FACULTAD DE INGENIERIA INDUSTRIAL, SISTEMAS E INFORMATICA ESCUELA PROFESIONAL DE INGENIERIA INFORMÁTICA

SEXTA SEMANA

La esteganografía, historia, evolución, tendencias, comparación con la criptografía

SÉPTIMA SEMANA

Métodos criptográficos clásicos por sustitución 1

OCTAVA SEMANA.

Métodos criptográficos clásicos por sustitución 2

UNIDAD III: MÉTODOS CRIPTOGRÁFICOS

NOVENA SEMANA

Métodos criptográficos clásicos por sustitución 3

DÉCIMA SEMANA

Métodos criptográficos clásicos por transposición 1

DÉCIMA PRIMERA SEMANA

Métodos criptográficos clásicos por transposición 2

DÉCIMA SEGUNDA SEMANA

Métodos criptográficos clásicos por transposición 3

UNIDAD IV: CRIPTOANÁLISIS

DÉCIMO TERCERA SEMANA

Métodos de criptoanálisis clásico 1

DÉCIMO CUARTA SEMANA

Métodos de criptoanálisis clásico 2

DÉCIMO QUINTA SEMANA

Métodos de codificación 1

DÉCIMO SEXTA SEMANA

Métodos de codificación 2

V. MATERIALES EDUCATIVOS Y OTROS RECURSOS DIDÁCTICOS

1.- MEDIOS ESCRITOS.

- Libros
- Revistas

2.- MEDIOS VISUALES Y ELECTRÓNICOS.

- Pizarrón
- Videos
- Proyector Multimedia



UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

FACULTAD DE INGENIERIA INDUSTRIAL, SISTEMAS E INFORMATICA
ESCUELA PROFESIONAL DE INGENIERIA INFORMÁTICA

2.- MEDIOS INFORMÁTICOS.

- Internet

VI. EVALUACIÓN

1.- CALIFICACIÓN.

Sistema de calificación: Escala vigesimal (0-20)

2.- EVALUACIÓN DE LOS RESULTADOS DE LAS UNIDADES DIDÁCTICAS.

Evaluación mensual por cada unidad didáctica: Todas las unidades didácticas serán evaluadas en las tres componentes con un puntaje del 0 al 20, obteniéndose tres (03) notas:

ECn: Evaluación de Conocimientos **WECn:** Peso para la evaluación de Conocimiento= 0,30

EPn: Evaluación de Producto **WPCn:** Peso para la evaluación de Producto= 0,35

EDn: Evaluación de Desempeño **WEDn:** Peso para la evaluación de conocimiento= 0,35

PMn: Promedio del Módulo **PMn:** Promedio del Módulo, con un decimal sin redondeo.

A las notas anteriores se les aplicarán los pesos indicados en la siguiente tabla:

UNIDA DIDÁCTICA	EVIDENCIA DE CONOCIMIENTOS (30%)	EVIDENCIA DE PRODUCTO (35%)	EVIDENCIA DE DESEMPEÑO (35%)
I	EC ₁	EP ₁	ED ₁
II	EC ₂	EP ₂	ED ₂
III	EC ₃	EP ₃	ED ₃
IV	EC ₄	EP ₄	ED ₄

Promedio del Módulo $PMn = (ECn \times WECn + EPn \times WPCn + EDn \times WEDn)$

Donde el PROMEDIO FINAL: $(PM1 + PM2 + PM3 + PM4)/4$

VII. BIBLIOGRAFÍA Y REFERENCIAS WEB

UNIDAD DIDACTICA I: LA COMUNICACIÓN Y LA SEGURIDAD

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

UNIDAD DIDACTICA II: INTRODUCCIÓN A LA CRIPTOGRAFÍA Y ESTEGANOGRAFÍA

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



UNIVERSIDAD NACIONAL

JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

FACULTAD DE INGENIERIA INDUSTRIAL, SISTEMAS E INFORMATICA
ESCUELA PROFESIONAL DE INGENIERIA INFORMÁTICA

UNIDAD DIDACTICA III: MÉTODOS CRIPTOGRÁFICOS

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

UNIDAD DIDACTICA IV: CRIPTOANÁLISIS

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