



# UNIVERSIDAD NACIONAL

JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

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

## SILABO

### ASIGNATURA: CRIPTOGRAFÍA II

#### I. DATOS GENERALES

1.1. Código de la Asignatura	: 353
1.2. Escuela Académico Profesional	: Ingeniería Informática
1.3. Departamento Académico	: Ingeniería de Sistemas e Informática
1.4. Ciclo	: VI
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	: 303
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 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. 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 prácticas.

#### III. CAPACIDADES AL TERMINAR EL CURSO

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



**UNIVERSIDAD NACIONAL**  
**JOSÉ FAUSTINO SÁNCHEZ CARRIÓN**

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

<b>UNIDAD II</b>	Aplica las diferentes técnicas criptográficas contemporáneas de cifrado simétricas.	CRITOSISTEMAS SIMÉTRICOS	5,6,7,8
<b>UNIDAD III</b>	Aplica las diferentes técnicas criptográficas contemporáneas de cifrado asimétricas.	CRITOSISTEMAS ASIMÉTRICOS	9,10,11,12
<b>UNIDAD IV</b>	Identifica las diferentes aplicaciones de la criptografía en el campo real y su beneficio para la humanidad.	APLICACIONES DE LA CRIPTOGRAFÍA	13,14,15,16

#### **IV. DESARROLLO DE LAS UNIDADES DIDÁCTICAS**

##### **UNIDAD I: LA COMUNICACIÓN, LA SEGURIDAD Y CRIPTOGRAFÍA**

###### **PRIMERA SEMANA**

La comunicación y la seguridad de la información

###### **SEGUNDA SEMANA**

La comunicación y la seguridad informática

###### **TERCERA SEMANA**

Principales métodos criptográficos clásicos por sustitución

###### **CUARTA SEMANA**

Principales métodos criptográficos clásicos por transposición

##### **UNIDAD II: CRIPTOSISTEMAS SIMÉTRICOS**

###### **QUINTA SEMANA**

Principales métodos de criptoanálisis clásicos



# UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

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

## **SEXTA SEMANA**

Criptosistemas, definición, clasificación, evolución

## **SÉPTIMA SEMANA**

Criptosistemas simétricos 1

## **OCTAVA SEMANA.**

Criptosistemas simétricos 2

## **UNIDAD III: CRIPTOSISTEMAS ASIMÉTRICOS**

### **NOVENA SEMANA**

Criptosistemas asimétricos de cifrado en bloque 1

### **DÉCIMA SEMANA**

Criptosistemas asimétricos de cifrado en bloque 2

### **DÉCIMA PRIMERA SEMANA**

Criptosistemas asimétricos de cifrado en flujo 1

### **DÉCIMA SEGUNDA SEMANA**

Criptosistemas asimétricos de cifrado en flujo 2

## **UNIDAD IV: APLICACIONES DE LA CRIPTOGRAFÍA**

### **DÉCIMO TERCERA SEMANA**

Firma electrónica, certificado electrónico

### **DÉCIMO CUARTA SEMANA**

PC Cards y Smart cards

### **DÉCIMO QUINTA SEMANA**

Criptografía Cuántica

### **DÉCIMO SEXTA SEMANA**

Las matemáticas y la criptografía

## **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 **WECn:** 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%)
<b>I</b>	EC <sub>1</sub>	EP <sub>1</sub>	ED <sub>1</sub>
<b>II</b>	EC <sub>2</sub>	EP <sub>2</sub>	ED <sub>2</sub>
<b>III</b>	EC <sub>3</sub>	EP <sub>3</sub>	ED <sub>3</sub>
<b>IV</b>	EC <sub>4</sub>	EP <sub>4</sub>	ED <sub>4</sub>

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

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

## VII. BIBLIOGRAFÍA Y REFERENCIAS WEB

### UNIDAD DIDACTICA I: LA COMUNICACIÓN, LA SEGURIDAD Y CRIPTOGRAFÍA

- <http://www.intypedia.com>

### UNIDAD DIDACTICA II: CRIPTOSISTEMAS SIMÉTRICOS

- <http://www.intypedia.com>



**UNIVERSIDAD NACIONAL**  
**JOSÉ FAUSTINO SÁNCHEZ CARRIÓN**

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

**UNIDAD DIDACTICA III: CRIPTOSISTEMAS ASIMÉTRICOS**

- <http://www.intypedia.com>

**UNIDAD DIDACTICA IV: APLICACIONES DE LA CRIPTOGRAFÍA**

- <http://www.intypedia.com>