

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 INGENIERIA INFORMATICA

**MODALIDAD NO PRESENCIAL****SÍLABO POR COMPETENCIAS****CURSO:****Criptografía II**

## I. DATOS GENERALES

|                                 |  |
|---------------------------------|--|
| Línea de Carrera                | Seguridad Informatica  |
| Semestre Académico              | 2020 - I   |
| Código del Curso                | 3305353  |
| Créditos                        | Cuatro (4)   |
| Horas Semanales                 | Hrs. Totales: 4    Teóricas: 2    Practicas: 2                   |
| Ciclo                           | VI   |
| Sección                         | A  |
| Apellidos y Nombres del Docente | CHINGA RAMOS CARLOS ENRIQUE                                      |
| Correo Institucional            | <a href="mailto:cchinga@unjfsc.edu.pe">cchinga@unjfsc.edu.pe</a> |
| N° De Celular                   | 982065304  |

**II. SUMILLA**

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 02 horas de prácticas.

**III. CAPACIDADES AL FINALIZAR EL CURSO**

|            | CAPACIDAD DE LA UNIDAD DIDÁCTICA  | NOMBRE DE LA UNIDAD DIDÁCTICA     | SEMANAS |
|------------|---|-----------------------------------|---------|
| UNIDAD I   | Aplica los conceptos y técnicas de Cifrado Simétrico                      | CIFRADO SIMETRICO                 | 1-4     |
| UNIDAD II  | Aplica los conceptos y técnicas de Cifrado Asimétrico                     | CIFRADO ASIMETRICO                | 5-8     |
| UNIDAD III | Aplica las diferentes técnicas de Seguridad en las Aplicaciones Web       | SEGURIDAD EN LAS APLICACIONES WEB | 9-12    |
| UNIDAD IV  | Identifica los diferentes niveles de Seguridad a nivel del protocolo TCP. | SEGURIDAD A NIVEL DE TCP/IP       | 13-16   |

**IV. INDICADORES DE CAPACIDADES AL FINALIZAR EL CURSO**

| N° | INDICADORES DE CAPACIDAD AL FINALIZAR EL CURSO                           |
|----|--|
| 1  | Identifica los elementos y la importancia de la criptografía.            |
| 2  | Identifica los elementos y la importancia de la criptografía Simétrica.  |
| 3  | Desarrolla aplicaciones haciendo uso de funciones Hash                   |
| 4  | Desarrolla aplicaciones haciendo uso de la criptografía simétrica        |
| 5  | Identifica los elementos y la importancia de la criptografía Asimétrica. |
| 6  | Desarrolla aplicaciones haciendo uso de criptografía Asimétrica.         |
| 7  | Identifica los elementos y la importancia de las Firmas digitales.       |
| 8  | Desarrolla aplicaciones haciendo uso de criptografía Asimétrica.         |
| 9  | Desarrolla aplicaciones Web sin ataques SQL Inyection                    |



|    |   |
|----|---|
| 10 | Desarrolla aplicaciones Web sin Secuencia de Comandos en Sitios cruzados XSS            |
| 11 | Identifica los elementos y la importancia de SSL y TSL                                  |
| 12 | Desarrolla aplicaciones web seguras.  |
| 13 | Identifica los elementos y la importancia de la Seguridad TCP/IP, Fragmentación IP, DoS |
| 14 | Identifica los elementos y la importancia de la Protección a Nivel de red               |
| 15 | Identifica la Protección a Nivel de red   |
| 16 | Identifica los elementos y la importancia de seguridad a nivel de Red.                  |



V. DESARROLLO DE LAS UNIDADES DIDÁCTICAS:

| CAPACIDAD DE LA UNIDAD DIDÁCTICA I:  |            |  |   |  |  |   |
|--|------------|--|---|--|--|---|
| SEMANA   | CONTENIDOS |  |   | ESTRATEGIAS DE LA ENSEÑANZA VIRTUAL  | INDICADORES DE LOGRO DE LA CAPACIDAD   |   |
|  | CONCEPTUAL | PROCEDIMENTAL  | ACTITUDINAL   |  |  |   |
| UNIDAD DIDÁCTICA I:  | 1          | Introducción a la Criptografía y a la seguridad de la información.   | Elabora aplicación haciendo uso de la Criptografía. | Discute en equipo los aspectos de la Criptografía  | <b>Expositiva (Docente/Alumno)</b> <ul style="list-style-type: none"> <li>• Uso del Google Meet</li> </ul> <b>Debate dirigido (Discusiones)</b> <ul style="list-style-type: none"> <li>• Foros, Chat</li> </ul> <b>Lecturas</b> <ul style="list-style-type: none"> <li>• Uso de repositorios digitales</li> </ul> <b>Lluvia de ideas (Saberes previos)</b> <ul style="list-style-type: none"> <li>• Foros, Chat</li> </ul> | Aplica los principios de la Criptografía.           |
|  | 2          | Criptografía Simétrica – Diferentes Algoritmos y sus Aplicaciones.   | Elabora aplicaciones con Criptografía Simétrica     | Reflexiona acerca de la criptografía simétrica   |  | Aplica los principios de la Criptografía Simétrica. |
|  | 3          | Funciones Hash y sus Aplicaciones.   | Elabora aplicaciones con funciones Hash             | Reflexiona acerca de las funciones Hash  |  | Aplica los principios de la Criptografía.           |
|  | 4          | Proyecto de Seguridad simétrica  | Elabora, analiza un caso aplicativo                 | Valora el uso de la Criptografía Simétrica   |  | Discute los resultados del Proyecto de Seguridad.   |
| <b>EVALUACIÓN DE LA UNIDAD DIDÁCTICA</b>   |            |  |   |  |  |   |
| <b>EVIDENCIA DE CONOCIMIENTOS</b>  |            | <b>EVIDENCIA DE PRODUCTO</b>   |   | <b>EVIDENCIA DE DESEMPEÑO</b>  |  |   |
| <ul style="list-style-type: none"> <li>• Estudios de Casos</li> <li>• Cuestionarios</li> </ul> |            | <ul style="list-style-type: none"> <li>• Trabajos individuales y/o grupales</li> <li>• Soluciones a Ejercicios propuestos</li> </ul> |   | <ul style="list-style-type: none"> <li>• Comportamiento en clase virtual y chat</li> </ul> |  |   |



| <b>CAPACIDAD DE LA UNIDAD DIDÁCTICA II:</b>  |                   |  |  |  |  |   |
|--|-------------------|--|--|--|--|---|
| <b>SEMANA</b>  | <b>CONTENIDOS</b> |  |  | <b>ESTRATEGIAS DE LA ENSEÑANZA VIRTUAL</b>   | <b>INDICADORES DE LOGRO DE LA CAPACIDAD</b>  |   |
|  | <b>CONCEPTUAL</b> | <b>PROCEDIMENTAL</b>   | <b>ACTITUDINAL</b>                                   |  |  |   |
| <b>UNIDAD DIDÁCTICA II:</b>  | 1                 | Introducción a la Clave Publica.   | Elabora aplicación haciendo uso Clave Publica.       | Valora el uso de la Clave Publica  | <b>Expositiva (Docente/Alumno)</b> <ul style="list-style-type: none"> <li>• Uso del Google Meet</li> </ul> <b>Debate dirigido (Discusiones)</b> <ul style="list-style-type: none"> <li>• Foros, Chat</li> </ul> <b>Lecturas</b> <ul style="list-style-type: none"> <li>• Uso de repositorios digitales</li> </ul> <b>Lluvia de ideas (Saberes previos)</b> <ul style="list-style-type: none"> <li>• Foros, Chat</li> </ul> | Aplica los principios de la Clave Publica.                      |
|  | 2                 | Algoritmos de clave Publica  | Elabora aplicaciones con algoritmos de Clave Publica | Reflexiona acerca de los algoritmos de clave publica                                       |  | Aplica los principios de los algoritmos de cla. publica.        |
|  | 3                 | Firmas Digitales   | Elabora aplicaciones con Firma Digital               | Reflexiona acerca de las firmas digitales  |  | Aplica los principios de las firmas digitales.                  |
|  | 4                 | Proyecto de Clave Publica  | Elabora, analiza un caso aplicativo                  | Valora el uso de la Criptografía Asimétrica  |  | Discute los resultados del Proyecto de Criptografía Asimétrica. |
| <b>EVALUACIÓN DE LA UNIDAD DIDÁCTICA</b>   |                   |  |  |  |  |   |
| <b>EVIDENCIA DE CONOCIMIENTOS</b>  |                   | <b>EVIDENCIA DE PRODUCTO</b>   |  | <b>EVIDENCIA DE DESEMPEÑO</b>  |  |   |
| <ul style="list-style-type: none"> <li>• Estudios de Casos</li> <li>• Cuestionarios</li> </ul> |                   | <ul style="list-style-type: none"> <li>• Trabajos individuales y/o grupales</li> <li>• Soluciones a Ejercicios propuestos</li> </ul> |  | <ul style="list-style-type: none"> <li>• Comportamiento en clase virtual y chat</li> </ul> |  |   |



| <b>CAPACIDAD DE LA UNIDAD DIDÁCTICA III:</b>  |                   |   |   |  |  |  |
|---|-------------------|---|---|--|--|--|
| <b>SEMANA</b>   | <b>CONTENIDOS</b> |   |   | <b>ESTRATEGIAS DE LA ENSEÑANZA VIRTUAL</b>   | <b>INDICADORES DE LOGRO DE LA CAPACIDAD</b>  |  |
|   | <b>CONCEPTUAL</b> | <b>PROCEDIMENTAL</b>  | <b>ACTITUDINAL</b>                                    |  |  |  |
| <b>UNIDAD DIDÁCTICA III:</b>  | 1                 | Introducción a la Seguridad de las aplicaciones web.  | Elabora aplicación haciendo uso seguridad de app web. | Valora el uso de las apps web  | <b>Expositiva (Docente/Alumno)</b><br><ul style="list-style-type: none"><li>• Uso del Google Meet</li> </ul> <b>Debate dirigido (Discusiones)</b><br><ul style="list-style-type: none"><li>• Foros, Chat</li> </ul> <b>Lecturas</b><br><ul style="list-style-type: none"><li>• Uso de repositorios digitales</li> </ul> <b>Lluvia de ideas (Saberes previos)</b><br><ul style="list-style-type: none"><li>• Foros, Chat</li> </ul> |  |
|   | 2                 | Gestión de sesiones y Secuencia de Comandos en Sitios cruzados.   | Elabora aplicaciones con secuencia de comandos y XSS  | Reflexiona acerca de las aplicaciones con XSS  |  | Aplica los principios de la seguridad en las apps w. |
|   | 3                 | SSL y TLS   | Elabora aplicaciones con SSL y TLS                    | Reflexiona acerca de las SSL y TLS   |  | Aplica los principios aplicaciones con XSS.          |
|   | 4                 | Proyecto de Seguridad Aplicaciones web  | Elabora, analiza un caso aplicativo                   | Valora el uso de la Seguridad en las Apps web  |  | Aplica los principios de las firmas digitales.       |
| <b>EVALUACIÓN DE LA UNIDAD DIDÁCTICA</b>  |                   |   |   |  |  |  |
| <b>EVIDENCIA DE CONOCIMIENTOS</b>   |                   | <b>EVIDENCIA DE PRODUCTO</b>  |   | <b>EVIDENCIA DE DESEMPEÑO</b>  |  |  |
| <ul style="list-style-type: none"><li>• Estudios de Casos</li><li>• Cuestionarios</li></ul> |                   | <ul style="list-style-type: none"><li>• Trabajos individuales y/o grupales</li><li>• Soluciones a Ejercicios propuestos</li></ul> |   | <ul style="list-style-type: none"><li>• Comportamiento en clase virtual y chat</li></ul> |  |  |



| <b>CAPACIDAD DE LA UNIDAD DIDÁCTICA IV:</b>  |                   |  |   |  |  |  |
|--|-------------------|--|---|--|--|--|
| <b>SEMANA</b>  | <b>CONTENIDOS</b> |  |   | <b>ESTRATEGIAS DE LA ENSEÑANZA VIRTUAL</b>   | <b>INDICADORES DE LOGRO DE LA CAPACIDAD</b>  |  |
|  | <b>CONCEPTUAL</b> | <b>PROCEDIMENTAL</b>   | <b>ACTITUDINAL</b>  |  |  |  |
| <b>UNIDAD DIDÁCTICA IV:</b>  | 1                 | Introducción a la Seguridad TCP/IP, Fragmentación IP, DoS.   | Realiza un mapa mental en relación a la Seguridad en Red. | Valora el uso de la seguridad en las apps web  | <b>Expositiva (Docente/Alumno)</b> <ul style="list-style-type: none"> <li>• Uso del Google Meet</li> </ul> <b>Debate dirigido (Discusiones)</b> <ul style="list-style-type: none"> <li>• Foros, Chat</li> </ul> <b>Lecturas</b> <ul style="list-style-type: none"> <li>• Uso de repositorios digitales</li> </ul> <b>Lluvia de ideas (Saberes previos)</b> <ul style="list-style-type: none"> <li>• Foros, Chat</li> </ul> |  |
|  | 2                 | Protección a Nivel de red/ Protección a Nivel de Transporte.   | Secuencia de comandos y XSS                               | Reflexiona acerca de las aplicaciones con XSS  |  | Aplica los principios de la seguridad en las apps w. |
|  | 3                 | Políticas, Normas de la Seguridad de la Información  | Elabora aplicaciones con SSL y TLS                        | Reflexiona acerca de las SSL y TLS   |  | Aplica los principios aplicaciones con XSS.          |
|  | 4                 | Proyecto de Seguridad de Red   | Elabora, analiza un caso aplicativo                       | Valora el uso de la Seguridad en las Apps web  |  | Aplica los principios de las firmas digitales.       |
| <b>EVALUACIÓN DE LA UNIDAD DIDÁCTICA</b>   |                   |  |   |  |  |  |
| <b>EVIDENCIA DE CONOCIMIENTOS</b>  |                   | <b>EVIDENCIA DE PRODUCTO</b>   |   | <b>EVIDENCIA DE DESEMPEÑO</b>  |  |  |
| <ul style="list-style-type: none"> <li>• Estudios de Casos</li> <li>• Cuestionarios</li> </ul> |                   | <ul style="list-style-type: none"> <li>• Trabajos individuales y/o grupales</li> <li>• Soluciones a Ejercicios propuestos</li> </ul> |   | <ul style="list-style-type: none"> <li>• Comportamiento en clase virtual y chat</li> </ul> |  |  |



**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<br>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

- García, A. (2011). Seguridad Informática.
- Raya. Seguridad de una Red NetWare. (5ta. Ed.) Alfaomega.
- Piattini, M. y De Peso, E. (2001). AUDITORIA INFORMATICA – Un enfoque práctico. RA-MA Editorial
- Katz, J. and Lindell, Y. (2014). *Introduction to Modern Cryptography, Second Edition*. Hoboken: CRC Press

### 8.2. Fuentes Electrónicas

- Norma Técnica Peruana NTP ISO 27001:2014. Tecnología de la Información Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición. <http://portal.indecopi.gob.pe/cidalerta/buscadocdet.aspx?id=21374>.
- Recursos de Seguridad de la Información.
- <http://www.intypedia.com>

Huacho Julio del 2020



*Universidad Nacional  
"José Faustino Sánchez Carrión"*

.....  
**Chinga Ramos Carlos Enrique**  
**DCU986**