



**UNIVERSIDAD NACIONAL DEL CALLAO**  
**FACULTAD DE INGENIERÍA INDUSTRIAL Y DE**  
**SISTEMAS**  
**ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**  
**SÍLABO**



**I. DATOS INFORMATIVOS**

- 1.1. Nombre de la Asignatura : **SEGURIDAD DE INFORMACIÓN**
- 1.2. Código de la Asignatura : SOP1021
- 1.3. Ciclo Académico : X
- 1.4. Créditos : 03
- 1.5. Horas semanales : 04 horas (Teoría: 02 horas / Práctica: 02 horas)
- 1.6. Duración del Ciclo : 17 semanas
- 1.7. Pre Requisito : SOP0708
- 1.8. Tipo de Asignatura : OBLIGATORIO
- 1.9. Semestre Académico : 2022-A

**II. SUMILLA**

Promover en el estudiante la capacidad de análisis de riesgos asociado a la información, el aspecto normativo existente, las buenas prácticas y la forma de gestionar los riesgos para minimizar los daños en una organización.

**III. COMPETENCIA DE ASIGNATURA**

Al concluir el curso el alumno estará en capacidad de:

**Competencia General:**

- Comprende con precisión los fundamentos de la Seguridad de la Información con énfasis en la Ciberseguridad.

**Competencia Específicas:**

- Reconoce con precisión los conceptos básicos de Seguridad de la Información con énfasis en la Ciberseguridad.
- Comprende y valora la realización de una un Sistemas de Gestión de Seguridad de la Información con énfasis en la Ciberseguridad.
- Identifica las diferentes norma y aspectos legales del cumplimiento de controles de Seguridad de la Información en las organizaciones.

**IV. CAPACIDADES.**

- a. Conoce las herramientas (técnicas y legales, procedimientos, métodos) para realizar la auditoria
- b. Identifica los procesos y actividades donde interviene TIC; y sus riesgos y debilidades de tipo técnico y legal, relacionado a la seguridad de la información.
- c. Evalúa cumplimiento de actividades dentro del marco técnico y legal
- d. Analiza y evalúa la magnitud del riesgo o deficiencia de los análisis desarrollados.
- e. Prepara la normatividad de la entidad relacionada a Seguridad de la Información.

## V. PROGRAMACIÓN DE CONTENIDOS

UNIDAD I: INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN				
CAPACIDAD:				
<ul style="list-style-type: none"> <li>➤ Reconoce los conceptos fundamentales de seguridad de la información.</li> <li>➤ Comprende el marco general del Sistema de Gestión de Seguridad de la Información – SGSI.</li> <li>➤ Posee las aptitudes para la implementación del Sistema de Gestión de Seguridad de la Información – SGSI en la entidad.</li> </ul>				
Semana	Actitudes		Estrategias didácticas de Aprendizaje	Horas
	Contenidos Conceptuales	Contenidos Procedimentales		
1	<b>Introducción a la Seguridad de la Información:</b> Conceptos Fundamentales Activos de Información Análisis de Riesgos Controles Estándares y Marco Normativo Introducción al SGSI	<ul style="list-style-type: none"> <li>• Analizan y comentan lecturas</li> <li>• Identifican la aplicación de conceptos a escenarios críticos a Seguridad de la Información.</li> <li>• Resuelven problemas utilizando las etapas del Pensamiento Crítico</li> <li>• Revisa normas y aplica a escenarios dados</li> </ul>	Presentación de casos de estudio	2
			Problematizaciones de situaciones reales. Trabajos prácticos.	2
2	<b>Introducción a la Seguridad de la Información (Continuación):</b> Introducción al SGSI Introducción a la Ciberseguridad y Ciberdefensa Control de Lectura Seleccionada.	<ul style="list-style-type: none"> <li>• Analizan y comentan lecturas</li> <li>• Identifican la aplicación de conceptos a escenarios críticos de SGSI y Ciberseguridad.</li> <li>• Resuelven problemas utilizando las etapas del Pensamiento Crítico</li> <li>• Revisa normas y aplica a escenarios dados</li> </ul>	Presentación de casos de estudio.	2
			Problematizaciones de situaciones reales. Trabajos prácticos.	2
3	<b>Seguridad Digital:</b> Seguridad de la Información en el contexto de la NTP 27001 Gestión de la Seguridad de la Información Implementación del Sistema de Gestión de Seguridad de la Información – SGSI Dominios, Objetivos de Control y Controles Política de Seguridad de la Información	<ul style="list-style-type: none"> <li>• Analizan y comentan lecturas</li> <li>• Identifican la aplicación de conceptos a escenarios críticos relacionados a la Seguridad Digital</li> <li>• Resuelven problemas utilizando las etapas del Pensamiento Crítico</li> <li>• Revisa normas y aplica a escenarios dados</li> </ul>	Presentación de casos de estudio.	2
			Trabajo en equipo para resolver problemas de aplicación. Trabajos prácticos.	2
4	<b>Ciberseguridad:</b> Conceptos Preliminares. Convenio de Budapest.  DL N° 12412 – Ley de Gobierno Digital DU N° 006-2020 – Sistema Nacional de Transformación Digital DU N° 007-2020 – Marco de Confianza Digital	<ul style="list-style-type: none"> <li>• Analizan y comentan lecturas</li> <li>• Identifican la aplicación de conceptos a escenarios críticos relacionados a Ciberseguridad y Ciberdefensa.</li> <li>• Resuelven problemas utilizando las etapas del Pensamiento Crítico</li> <li>• Revisa normas y aplica a escenarios dados</li> </ul>	Presentación de casos de estudio.	2
			Trabajo en equipo para resolver problemas de aplicación. Trabajos prácticos.	2

**Referencias**

- Ver sección IX Fuentes Bibliográficas

**UNIDAD II: SEGURIDAD DE LA INFORMACIÓN EN EL MARCO DE LA NTP ISO 27002**

**SEGURIDAD EN REDES Y SEGURIDAD EN SISTEMAS OPERATIVOS**

**CAPACIDAD:**

- Reconoce los conceptos fundamentales de seguridad de la información, NTP 27001, NTP 27002.
- Comprende el marco general Xde la Seguridad en Redes y Sistemas Operativos.
- Posee las aptitudes para la implementación de controles de Seguridad en Redes y Sistemas Operativos.

Semana	Actitudes		Estrategias didácticas de Aprendizaje	Horas
	Contenidos Conceptuales	Contenidos Procedimentales		
5	<b>Seguridad de la Información y la NTP ISO 27002:</b> Norma ISO/IEC NTP 27001 Norma ISO/IEC NTP 27002 Conceptos relacionados al SGSI Componentes del SGSI Establecimiento de un SGSI Política de Seguridad Gestión de Riesgos Identificación y Tasación de Activos de Información Monitoreo Interno Auditorías Internas Práctica Calificada		<ul style="list-style-type: none"> <li>• Analizan y comentan lecturas relacionadas a la Seguridad de la Información en el marco de la NTP ISO 27002</li> <li>• Identifican la aplicación de conceptos a escenarios críticos de la NTP ISO 27002</li> <li>• Resuelven problemas utilizando las etapas del Pensamiento Crítico</li> <li>• Revisa normas y aplica a escenarios dados</li> </ul>	Presentación de casos de estudio. 2
				Trabajo en equipo para resolver problemas de aplicación. Trabajos prácticos. 2
6	<b>Seguridad en Redes:</b> Protocolos TC/IP Protocolos de Seguridad Herramientas de Seguridad Proactivas Redes SCADA		<ul style="list-style-type: none"> <li>• Analizan y comentan lecturas relacionadas a la Seguridad en Redes.</li> <li>• conceptos a escenarios críticos de Seguridad en Redes</li> <li>• Resuelven problemas utilizando las etapas del Pensamiento Crítico</li> <li>• Revisa normas y aplica a escenarios dados</li> </ul>	Presentación de casos de estudio. 2
				Trabajo en equipo para resolver problemas de aplicación. Trabajos prácticos. 2
7	<b>Seguridad en Sistemas Operativos:</b> Sistema Operativo Windows Sistema Operativo Linux Sistema Operativo para Móviles Sistemas Virtualizados		<ul style="list-style-type: none"> <li>• Analizan y comentan lecturas relacionadas a la Seguridad en Sistemas Operativos</li> <li>• Identifican la aplicación de conceptos a escenarios críticos de Seguridad de Sistemas Operativos</li> <li>• Resuelven problemas utilizando las etapas del Pensamiento Crítico</li> <li>• Revisa normas y aplica a escenarios dados</li> </ul>	Presentación de casos de estudio. 2
				Trabajo en equipo para resolver problemas de aplicación. Trabajos prácticos. 2
8	Presentación de primera parte del Sistema de Gestión de Seguridad de la Información (de acuerdo al Índice). EXAMEN PARCIAL			

**Referencias**

- Ver sección IX Fuentes Bibliográficas

**UNIDAD III: LEY DE PROTECCIÓN DE DATOS PERSONALES**

**SEGURIDAD EN EL SOFTWARE Y BASES DE DATOS**

<b>CAPACIDAD:</b>				
<ul style="list-style-type: none"> <li>➤ Reconoce los conceptos fundamentales de la seguridad en la Ley de Protección de Datos Personal.</li> <li>➤ Comprende el marco general de la Seguridad en Redes y Sistemas Operativos.</li> <li>➤ Posee las aptitudes para la implementación de controles de Seguridad en Redes y Sistemas Operativos.</li> </ul>				
Semana	Actitudes		Estrategias didácticas de Aprendizaje	Horas
	<ul style="list-style-type: none"> <li>• Entiende los conceptos del Gobierno de TI y la Ley de Protección de Datos Personales, así como la Seguridad en el Software y Base de Datos.</li> <li>• Demuestra actitudes innovadoras, críticas y de solidaridad para trabajar en equipos.</li> </ul>			
	Contenidos Conceptuales	Contenidos Procedimentales		
9	<b>Ley de Protección de Datos Personales:</b> Gobierno de TI y Gestión de TI Ley N° - Ley de Protección de Datos Personales. Ley de Transparencia y Acceso a la Información Pública.	<ul style="list-style-type: none"> <li>• Analizan y comentan lecturas relacionadas al Gobierno y Gestión de TI.</li> <li>• Identifican la aplicación de conceptos a escenarios críticos de Protección de Datos Personales.</li> <li>• Resuelven problemas utilizando las etapas del Pensamiento Crítico</li> <li>• Revisa normas y aplica a escenarios dados</li> </ul>	Presentación de casos de estudio.	2
			Trabajo en equipo para resolver problemas de aplicación. Trabajos prácticos.	2
10	<b>Seguridad en el Software:</b> Seguridad en el Ciclo de Vida de Software. Análisis de Malware.	<ul style="list-style-type: none"> <li>• Analizan y comentan lecturas relacionadas a la Seguridad en el Software.</li> <li>• Identifican la aplicación de conceptos a escenarios críticos de Seguridad en el Software.</li> <li>• Resuelven problemas utilizando las etapas del Pensamiento Crítico</li> <li>• Revisa normas y aplica a escenarios dados</li> </ul>	Presentación de casos de estudio.	2
			Trabajo en equipo para resolver problemas de aplicación. Trabajos prácticos.	2
11	<b>Seguridad en Bases de Datos:</b> Seguridad en el Ciclo de Vida de Base de Datos. Control de Lectura Seleccionada	<ul style="list-style-type: none"> <li>• Analizan y comentan lecturas relacionadas a la Seguridad de Base de Datos.</li> <li>• Identifican la aplicación de conceptos a escenarios críticos de Seguridad de Base de Datos.</li> <li>• Resuelven problemas utilizando las etapas del Pensamiento Crítico</li> <li>• Revisa normas y aplica a escenarios dados</li> </ul>	Presentación de casos de estudio.	2
			Trabajo en equipo para resolver problemas de aplicación. Trabajos prácticos.	2
<b>Referencias</b>				
<ul style="list-style-type: none"> <li>• Ver sección IX Fuentes Bibliográficas</li> </ul>				
<b>UNIDAD IV: ETHICAL HACKING Y PENETRATION TESTING</b>				
<b>CAPACIDAD:</b>				
<ul style="list-style-type: none"> <li>➤ Reconoce los conceptos fundamentales del Ethical Hacking y Penetration Testing.</li> <li>➤ Comprende el marco general del Ethical Hacking y Penetration Testing.</li> <li>➤ Posee las aptitudes para la implementación de Ethical Hacking y Penetration Testing.</li> </ul>				
Semana	Actitudes		Estrategias didácticas de Aprendizaje	Horas
	<ul style="list-style-type: none"> <li>• Entiende los conceptos de Ethical Hacking y Penetration Testing.</li> <li>• Demuestra actitudes innovadoras, críticas y de solidaridad</li> </ul>			

		para trabajar en equipos.			
		Contenidos Conceptuales	Contenidos Procedimentales		
12	<b>Ethical Hacking y Penetration Testing:</b> Reconocimiento Activo y Pasivo Escaneo	<ul style="list-style-type: none"> <li>Analizan y comentan lecturas relacionadas al Ethical Hacking y Penetration Testing.</li> <li>Identifican la aplicación de conceptos a escenarios críticos de Ethical Hacking y Penetration Testing.</li> <li>Resuelven problemas utilizando las etapas del Pensamiento Crítico</li> <li>Revisa normas y aplica a escenarios dados</li> </ul>	Presentación de casos de estudio.	2	
			Trabajo en equipo para resolver problemas de aplicación. Trabajos prácticos.	2	
13	<b>Ethical Hacking y Penetration Testing:</b> Obtener Acceso. Mantener Acceso. Cubrir los pasos. Práctica Calificada	<ul style="list-style-type: none"> <li>Analizan y comentan lecturas relacionadas a Ethical Hacking y Penetration Testing.</li> <li>Identifican la aplicación de conceptos a escenarios críticos de Ethical Hacking y Penetration Testing..</li> <li>Resuelven problemas utilizando las etapas del Pensamiento Crítico</li> <li>Revisa normas y aplica a escenarios dados</li> </ul>	Presentación de casos de estudio.	2	
			Trabajo en equipo para resolver problemas de aplicación. Trabajos prácticos.	2	
14	<b>Seguridad de Nuevas Tecnologías:</b> Seguridad en Internet Seguridad del Cloud Seguridad en Móviles	<ul style="list-style-type: none"> <li>Analizan y comentan lecturas relacionadas a los Controles de Seguridad de Nuevas Tecnologías.</li> <li>Identifican la aplicación de conceptos a escenarios críticos de Seguridad de Nuevas Tecnologías.</li> <li>Resuelven problemas utilizando las etapas del Pensamiento Crítico</li> <li>Revisa normas y aplica a escenarios dados</li> </ul>	Presentación de casos de estudio.	2	
			Trabajo en equipo para resolver problemas de aplicación. Trabajos prácticos.	2	
15	<b>Tecnologías de Seguridad:</b> Tecnologías de seguridad de la Información y seguridad informática	<ul style="list-style-type: none"> <li>Analizan y comentan lecturas relacionadas a las Tecnologías de Seguridad.</li> <li>Identifican la aplicación de conceptos a escenarios críticos de Tecnologías e Seguridad.</li> <li>Resuelven problemas utilizando las etapas del Pensamiento Crítico</li> <li>Revisa normas y aplica a escenarios dados</li> </ul>	Presentación de casos de estudio.	2	
			Trabajo en equipo para resolver problemas de aplicación. Trabajos prácticos.	2	
16	Presentación del Sistema de Gestión de Seguridad de la Información (de acuerdo al Índice). EXAMEN FINAL				
17	ENTREGA DE NOTAS				
<b>Referencias</b> Ver sección IX Fuentes Bibliográficas					

## VI. METODOLOGÍA

### 6.1. Estrategias centradas en la enseñanza

- a. Clase magistral
- b. Exposición problemática. deductiva e inductiva de la teoría.
- c. Se propicia y estimula la intuición de los alumnos en clase.
- d. Aplicación de la teoría en casos reales de su profesión.
- e. Demostración de resultados. Teoremas importantes.

### 6.2. Estrategias centradas en el aprendizaje

- a. Dinámica de Grupos para la solución de las guías de práctica.
- b. Se promueve la investigación por medio de Trabajos asignados.
- c. Exposición dialogada y discusión de soluciones de problemas.
- d. Manejo del software. Foro

## VII. RECURSOS PARA EL APRENDIZAJE

- a. Pizarra, pizarra, plumones.
- b. Separatas del curso.
- c. Equipos informáticos
- d. Multimedia.

## VIII. EVALUACIÓN

La evaluación es un componente del proceso formativo que implica el recojo de información sobre los rendimientos y desempeños del estudiante. Permite el análisis para mejorar el proceso de enseñanza – aprendizaje. Se evalúa antes, durante y al finalizar el proceso.

**Antes:** evaluación inicial, para recoger los saberes que posee el estudiante para asumir la asignatura y se aplica con una prueba de entrada cuyo resultado no interviene en el cálculo de la calificación de la asignatura.

**Durante:** se evalúa el desempeño del estudiante en el cumplimiento de tareas académicas de manera procesal que originan la nota de proceso.

**Final:** evalúa los productos del aprendizaje, al finalizar una o más unidades de aprendizaje, usándose la prueba escrita como instrumento de medición (Examen Parcial y Examen Final).

El proceso de evaluación consta dos exámenes, parcial (E.P) y final (E.F) Asimismo, las tareas (NT) y Prácticas y Controles (PC), y el Sistema de Gestión de Seguridad de la Información (SGSI).

La nota final (NF) del curso se obtiene como sigue:

$$\text{NOTA FINAL (NF)} = (3*\text{EP} + 1*\text{NT} + 3*\text{EF} + 2*\text{SGSI} + 1*\text{PC})/10$$

La Nota Final (NF) obtenida debe ser mayor o igual a 11 para considerarse APROBADO.

## IX. FUENTES BIBLIOGRÁFICAS.

- Muñoz Razo, Carlos **Auditoría en Sistemas Computacionales**, Prentice Hall 2002
- Piattini, Mario y Del Peso, Emilio **Auditoría Informática: Un enfoque práctico 2ª Edición** Editorial AlfaOmega 2001
- Normas de Control Interno de la Contraloría General de la República. Contraloría General de la República. 1998.
- Normas de la SeGDI sobre sistemas, seguridad y sistemas de información Oficina Nacional de Gobierno Electrónico e Informática. 2003
- Auditoría Informática. A.J. Thomas, Editorial Paraninfo, España,
- MAGU, NAGU Contraloría General de la República
- COBIT Control Objectives for Information and Related technology, information system Audit and Control foundation Rolling Meadows II
- IT Audit Framework (ITAF™): A Professional Practices Framework for IT Audit, 4th Edition
- DIRECCION GENERAL DE MODERNIZACION ADMINISTRATIVA, PROCEDIMIENTOS E IMPULSO DE LA ADMINISTRACION ELECTRONICA. (2012). Metodología de análisis y gestión de riesgos de los sistemas de información versión 3.0. España: Ministerio de Hacienda y Administraciones Públicas.

- GORDON, A. (2015). Official (ISC)2 Guide to the CISSP CBK, Fourth Edition. USA: (ISC)2 Press.
- HARRIS, S. (2013). CISSP All-In-One Exam Guide, 6th Edition. USA: McGraw-Hill.
- INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. (2016). CISM Review Manual. Chicago: ISACA.
- INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (2013). Information technology – Code of Practice for Information Security Management – INTERNATIONAL STANDARD ISO/IEC 27002:2013. Geneva: ISO.
- GREENWALD G. (2014). Snowden: Sin un lugar para esconderse. Barcelona: Ediciones B.
- INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. (2016). CISA Review Manual. Chicago: ISACA.
- INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. (2012) COBIT 5 Un marco de negocio para el Gobierno y la Gestión de la TI en la Empresa. USA: ISACA.
- INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. (2012). COBIT 5 Procesos catalizadores. USA: ISACA
- Recursos de Seguridad de la Información. <http://www.isaca.org> - <http://www.sans.org> - <http://www.intypedia.com/> - <http://www.welivesecurity.com/la-es>
- Metodología de Análisis y Gestión de Riesgos de los sistemas de información, MAGERIT versión 3.0. <https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/>
- Norma Técnica Peruana NTP ISO 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información. INDECOPI, 2007. <http://www.bvindicopi.gob.pe/normas/isoiec17799.pdf>
- Norma Técnica Peruana NTP ISO 27001:2014. Tecnología de la Información Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisito Requisitos. 2ª Edición. <http://portal.indecopi.gob.pe/cidalerta/buscadocdet.aspx?id=21374>