SÍLABO
Gerencia de la Seguridad de Información

Código	ASUC00381		**Carácter**	Electivo
Prerrequisito	140 créditos aprobados			
Créditos	3			
Horas	**Teóricas**	2	**Prácticas**	2
Año académico	2025			

I. Introducción

Gerencia de la Seguridad de Información es una asignatura electiva de especialidad de la Escuela Académico Profesional de Ingeniería de Sistemas e Informática. Con esta asignatura, se desarrolla, en un nivel logrado, las competencias transversales El Ingeniero y la Sociedad y Gestión de Proyectos, y la competencia específica Uso de Herramientas Modernas. La relevancia de la asignatura reside en gestionar de manera segura la información en las organizaciones, utilizando estándares nacionales e internacionales de seguridad de la información de acuerdo a la realidad de las organizaciones.

Los contenidos generales que la asignatura desarrolla son los siguientes: seguridad de la información. Normas ISO 27001 y 27002. Gestión de Riesgos ISO 27005, metodologías de riesgo: OCTAVE, MAGERIT, NIST800-30 y Risk IT framework. Planeación de continuidad de Negocio BCP/DRP (*Business continuity planning / Disaster recovery planning*). Atención de incidentes de seguridad, NIST800-61. Principios organizacionales básicos como la separación de responsabilidades, mínimo privilegio, *accountability,* y prácticas seguras de gestión de capital humano.

II. Resultado de aprendizaje de la asignatura

Al finalizar la asignatura, el estudiante será capaz de aplicar adecuadamente los elementos que permitan gestionar la seguridad de la información en las organizaciones modernas y complejas de hoy a través de la planificación de riesgos de seguridad de la información, siguiendo las mejores prácticas de la industria.

III. Organización de los aprendizajes

Unidad 1 **Seguridad de la información e introducción a las Normas ISO 27001 y 27002**	**Duración en horas**	16
Resultado de aprendizaje de la unidad	Al finalizar la Unidad, el estudiante será capaz de identificar los conceptos básicos de seguridad de la información y las normas ISO 27001 e ISO 27002	
Ejes temáticos	1. Seguridad de la información 2. Confidencialidad, integridad y disponibilidad 3. ISO 27001 y certificación 4. Controles ISO 27002	

Unidad 2 **Metodologías de riesgo: OCTAVE, MAGERIT, NIST800-30 y Risk IT Framework, gestión de riesgos ISO 27005**	**Duración en horas**	16
Resultado de aprendizaje de la unidad	Al finalizar la Unidad, el estudiante será capaz de identificar los conceptos básicos relacionados con la gestión de riesgos, implementando también un plan de tratamiento de estos en la organización.	
Ejes temáticos	1. Gestión de riesgos en la seguridad de la información 2. ISO 31000 3. ISO 27005 4. MAGERIT 5. OCTVAVE 6. Otros marcos de gestión de riesgos	

Unidad 3 **Planeación de continuidad de negocio BCP/DRP (*Business Continuity Planning / Disaster Recovery Planning*) y atención de incidentes de seguridad, NIST800-61**	**Duración en horas**	16
Resultado de aprendizaje de la unidad	Al finalizar la Unidad, el estudiante será capaz de identificar los conceptos e importancia de la continuidad del negocio y la recuperación ante desastres en las organizaciones, gestionando también incidentes de seguridad.	
Ejes temáticos	1. ¿Qué es la continuidad del negocio? 2. Análisis de impacto del negocio 3. Recuperación ante desastres 4. Proceso de gestión de incidentes y buenas prácticas	

Unidad 4 **Principios organizacionales básicos: separación de responsabilidades, mínimo privilegio, *accountability* y prácticas seguras de gestión de capital humano**	**Duración en horas**	16
Resultado de aprendizaje de la unidad	Al finalizar la Unidad, el estudiante será capaz de aplicar adecuadamente los elementos que permitan gestionar la seguridad de la información, identificando buenas prácticas en los programas de seguridad de información, así como la importancia del capital humano en las organizaciones.	
Ejes temáticos	1. Buenas prácticas en los programas de seguridad de la información 2. Mínimo privilegio, separación de responsabilidades, *accountability* 3. Concientización 4. Entrenamiento 5. Análisis de brechas en el personal	

IV. Metodología

Modalidad Presencial

El desarrollo de la asignatura será mediante la explicación de los conceptos por parte del docente mediante exposiciones teóricas con apoyo audiovisual, se requiere una activa participación de los estudiantes, se hará el tratamiento y exposición de casos y laboratorios en clase, revisión y debate de los controles de lectura asignados y planteamiento de problemas y participación general en su solución.

Se utilizarán las siguientes estrategias:

- aprendizaje colaborativo,
- estudio de casos,
- aprendizaje basado en problemas,
- clase magistral activa.

Modalidad, Semipresencial Blended, A Distancia

El desarrollo de la asignatura se hará mediante la explicación de los conceptos por parte del docente, mediante exposiciones teóricas con el apoyo audiovisual; se requiere, además, una activa participación de los estudiantes, con tratamiento y exposición de casos y laboratorios en clase, revisión y debate de los controles de lectura asignados y el planteamiento de problemas y la participación general en la solución de estos.

Se utilizarán las siguientes estrategias:

- aprendizaje colaborativo,
- estudio de casos,
- aprendizaje basado en problemas,

clase magistral activa.

-

V. Evaluación

Modalidad Presencial

Rubros	Unidad por evaluar	Fecha	Entregable / Instrumento	Peso parcial	Peso total
Evaluación de entrada	Prerrequisito	Primera sesión	Evaluación individual teórica/ **Prueba objetiva**	**0 %**	
Consolidado 1 **C1**	1	Semana 1 - 4	Evaluación teórico-práctica/ **Prueba de desarrollo**	40 %	**20%**
	2	Semana 5 - 7	Ejercicios desarrollados en clase/ **Rúbrica de evaluación**	60 %	
Evaluación parcial **EP**	1 y 2	Semana 8	Evaluación teórico-práctica/ **Prueba de desarrollo**	**20 %**	
Consolidado 2 **C2**	3	Semana 9 - 12	- Evaluación teórico-práctica/ **Prueba de desarrollo**	40 %	**20 %**
	4	Semana 13- 15	Ejercicios desarrollados en clase/ **Rúbrica de evaluación**	60 %	
Evaluación final **EF**	Todas las unidades	Semana 16	Evaluación teórico-práctica/ **Prueba de desarrollo**	**40 %**	
Evaluación sustitutoria*	Todas las unidades	Fecha posterior a la evaluación final	**Aplica**		

* Reemplaza la nota más baja obtenida en los rubros anteriores.

Modalidad Semipresencial - Blended

Rubros	Unidad por evaluar	Fecha	Entregable/Instrumento	Peso parcial	Peso Total
Evaluación de entrada	Prerrequisito	Primera sesión	- Evaluación individual teórica/ **Prueba objetiva**	**0 %**	
Consolidado 1 **C1**	1	Semana 1-3	- Actividades virtuales	15 %	**20 %**
			- Evaluación teórico-práctica/ **Prueba de desarrollo**	85 %	
Evaluación parcial **EP**	1 y 2	Semana 4	- Evaluación teórico-práctica/ **Prueba de desarrollo**	**20 %**	
Consolidado 2 **C2**	3	Semana 5-7	- Actividades virtuales	15 %	**20 %**
			- Evaluación teórico-práctica/ **Prueba de desarrollo**	85 %	
Evaluación final **EF**	Todas las unidades	Semana 8	- Evaluación teórico-práctica/ **Prueba de desarrollo**	**40 %**	
Evaluación sustitutoria *	Todas las unidades	Fecha posterior a la evaluación final	**Aplica**		

* **Reemplaza la nota más baja obtenida en los rubros anteriores.**

Modalidad A Distancia

Rubros	Unidad por evaluar	Fecha	Entregable / Instrumento	Peso
Evaluación de entrada	Prerrequisito	Primera sesión	Evaluación individual teórica/ **Prueba objetiva**	**0 %**
Consolidado 1 **C1**	1	Semana 2	Ejercicios desarrollados en clase/ **Rúbrica de evaluación**	**20 %**
Evaluación parcial **EP**	1 y 2	Semana 4	Evaluación teórico-práctica/ **Prueba de desarrollo**	**20 %**
Consolidado 2 **C2**	3	Semana 6	Ejercicios desarrollados en clase/ **Rúbrica de evaluación**	**20 %**
Evaluación final **EF**	Todas las unidades	Semana 8	Evaluación teórico-práctica/ **Prueba de desarrollo**	**40 %**
Evaluación sustitutoria*	Todas las unidades	Fecha posterior a la evaluación final	**Aplica**	

* Reemplaza la nota más baja obtenida en los rubros anteriores.

Fórmula para obtener el promedio:

PF = C1 (20 %) + EP (20 %) + C2 (20 %) + EF (40 %)

VI. Bibliografía

Básica

ISACA (2016). *CISM: review manual* (15. a ed.). ISACA. https://bit.ly/3s075aG

Taylor, L. (2013). *FISMA compliance handbook* (2a ed.). Syngress. https://bit.ly/441fmYU

Complementaria

Gregory, H. (2018). *CISM Certified Information Security Manager All-in-One Exam Guide*. McGraw Hill.

Gómez, A. (2011). *Enciclopedia de la seguridad informática*. AlfaoMega – Rama.

ISACA (2014). *Certified Information Security Manager - CISM. Review Manual.* (13.a ed.). ISACA.

International Organization for Standardization (ISO). (2013). *ISO/IEC 27002:2013 Information technology – Code of Practice for Information Security Management*. Recuperado de https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:en

VII. Recursos digitales

INCIBE- Instituto Nacional de Ciberseguridad. (2022). https://www.incibe.es/

ManageEngine LATAM. (2022). Webinar: Actualización de ISO/IEC 27002: seguridad a un nivel superior [video]. YouTube. shorturl.at/fGTW4

Neuro Hacking. (2022). Cambios en ISO 27001:2022 por Alberto Alexander, Eficiencia Gerencial y Productividad [video]. YouTube. shorturl.at/oqvX7

The Leading Cybersecurity Professional Development Platform. (2022). https://www.cybrary.it

Un informático en el lado del mal. (2022). https://www.elladodelmal.com

Una al día. (2022). Hispasec https://unaaldia.hispasec.com

Firmado por
FELIPE NESTOR GUTARRA MEZA

O = UNIVERSIDAD CONTINENTAL SOCIEDAD ANONIMA CERRADA
T = DECANO
Date: 03/03/2025 09:39