

SÍLABO

Seguridad de la Información Corporativa

Código	ASUC00769	Carácter	Electivo	
Prerrequisito	140 créditos aprobados			
Créditos	3			
Horas	Teóricas	2	Prácticas	2
Año académico	2024			

I. Introducción

Seguridad de la Información Corporativa es una asignatura electiva de especialidad, que se ubica en el noveno período de la Escuela Académico Profesional de Ingeniería de Sistemas e Informática. Tiene como requisito haber aprobado 140 créditos. Desarrolla, a nivel logrado, las competencias específicas Análisis de Problemas y Uso de Herramientas Modernas. La relevancia de la asignatura reside en emplear diferentes modelos de seguridad asociados al manejo de confidencialidad, integridad y disponibilidad, en el marco global de los diferentes estándares de seguridad en TI.

Los contenidos generales que la asignatura desarrolla son los siguientes: Introducción a la seguridad de la información; sistemas de control de acceso; arquitecturas de seguridad y sus modelos; seguridad en las operaciones; criptografía y sus aplicaciones; seguridad perimetral; seguridad por contenidos; seguridad en el ciclo de vida de las aplicaciones; seguridad de entornos físicos; ciberseguridad y tecnologías de seguridad.

II. Resultado de aprendizaje de la asignatura

Al finalizar la asignatura, el estudiante será capaz de aplicar mecanismos de protección para defender a las organizaciones de los diferentes riesgos informáticos que puedan alterar o dañar los recursos informáticos, siguiendo las técnicas de seguridad y las mejores prácticas de la industria relacionadas con seguridad informática.

III. Organización de los aprendizajes

Unidad 1 Introducción a la seguridad de la información		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: ciberespacio, confidencialidad, integridad, disponibilidad, riesgo, etc.		
Ejes temáticos	<ol style="list-style-type: none"> 1. La seguridad de la información 2. El ciberespacio 3. La confidencialidad 4. La integridad 5. La disponibilidad 6. Diferencia de la seguridad de la información con la ciberseguridad 7. Riesgos de la seguridad de la información 8. Ataques relevantes 		

Unidad 2 Sistemas de control de acceso		Duración en horas	16
Resultado de aprendizaje de la unidad	Al finalizar la Unidad, el estudiante será capaz de identificar las amenazas y vulnerabilidades relacionadas a la seguridad de la información y la ciberseguridad.		
Ejes temáticos	<ol style="list-style-type: none"> 1. Necesidades de la organización 2. Métodos de control de acceso 3. Tecnologías de control de acceso 4. Auditoría 		

Unidad 3 Arquitecturas de seguridad y Seguridad en las operaciones		Duración en horas	16
Resultado de aprendizaje de la unidad	Al finalizar la Unidad, el estudiante será capaz de identificar las técnicas y herramientas para establecer una estrategia de seguridad en la organización.		
Ejes temáticos	<ol style="list-style-type: none"> 1. Frameworks de seguridad 2. Identificación de controles existentes 3. Controles físicos 4. Controles lógicos 5. Controles administrativos 6. Uso de herramientas de seguridad 		

Unidad 4 Criptografía y seguridad de aplicaciones		Duración en horas	16
Resultado de aprendizaje de la unidad	Al finalizar la Unidad, el estudiante será capaz de aplicar mecanismos de protección para la defensa de las organizaciones de los diferentes riesgos informáticos, identificando las técnicas y herramientas para auditar redes y sistemas, ya que son utilizadas por los ciberdelincuentes.		
Ejes temáticos	<ol style="list-style-type: none"> 1. Introducción a la criptografía 2. Criptografía asimétrica 3. Criptografía simétrica 4. Desarrollo seguro 5. OWASP TOP 10 6. Cloud computing 		

IV. Metodología

El desarrollo de la asignatura será mediante la explicación de los conceptos por parte del docente, mediante exposiciones teóricas con apoyo audiovisual; sin embargo, se requiere 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 planteamiento de problemas y participación general en la solución de estos.

Modalidad Presencial- Virtual

Se utilizarán las siguientes estrategias:

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

Modalidad Semipresencial-Blended

Se utilizarán las siguientes estrategias:

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

Modalidad A Distancia

Se utilizarán las siguientes estrategias:

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

V. Evaluación
Modalidad Presencial-Virtual

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 4	- Evaluación teórico-práctica/ Prueba de desarrollo	30 %	20 %
	2	Semana 7	- Ejercicios desarrollados en clase/ Rúbrica de evaluación	30 %	
			- Actividades de trabajo autónomo en línea	40 %	
Evaluación parcial EP	1 y 2	Semana 8	- Evaluación teórico-práctica/ Prueba de desarrollo	20 %	
Consolidado 2 C2	3	Semana 12	- Evaluación teórico-práctica/ Prueba de desarrollo	30 %	20 %
	4	Semana 15	- Ejercicios desarrollados en clase/ Rúbrica de evaluación	30 %	
			- Actividades de trabajo autónomo en línea	40 %	
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 %
			- Ejercicios desarrollados en clase/ Rúbrica de evaluación	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 %
			- Ejercicios desarrollados en clase/ Rúbrica de evaluación	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

Gómez, A. (2011). *Enciclopedia de la seguridad informática*. (2.ª ed.). Rama. <https://at1z.short.gy/0DwE1Q>

International Organization for Standardization (2013). *ISO/IEC 27002 Information technology – Code of Practice for Information Security Management*. (2.ª ed.). ISO/IEC. <https://at1z.short.gy/OOeKIH>

Complementaria

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

Harris, S. (2019). *CISSP® All-in-One Exam Guide Eighth edition*. McGraw Hill.

Messier, R. (2019). *CEH v10 Certified Ethical Hacker Study Guide*. Sybex

VII. Recursos digitales

Kali Linux 2021. [software]. <https://www.kali.org/get-kali/#kali-virtual-machines>

Virtual Box. [software]. <https://www.virtualbox.org>

The Leading Cybersecurity Professional Development Platform. (2021). <https://www.cybrary.it>

Un informático en el lado del mal. [Blog] <https://www.elladodelmal.com>

Una al día. [Blog]Hispacec <https://unaaldia.hispasec.com>