

# SÍLABO

## Seguridad de la Información Corporativa

<b>Código</b>	ASUC00769	<b>Carácter</b>	Electivo	
<b>Prerrequisito</b>	140 créditos aprobados			
<b>Créditos</b>	3			
<b>Horas</b>	<b>Teóricas</b>	2	<b>Prácticas</b>	2
<b>Año académico</b>	2025-00			

### 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**

<b>Unidad 1</b> <b>Introducción a la seguridad de la información</b>		<b>Duración en horas</b>	16
<b>Resultado de aprendizaje de la unidad</b>	Al finalizar la Unidad, el estudiante será capaz de identificar los conceptos básicos de seguridad de la información: ciberespacio, confidencialidad, integridad, disponibilidad, riesgo, etc.		
<b>Ejes temáticos</b>	<ol style="list-style-type: none"> <li>1. La seguridad de la información</li> <li>2. El ciberespacio</li> <li>3. La confidencialidad</li> <li>4. La integridad</li> <li>5. La disponibilidad</li> <li>6. Diferencia de la seguridad de la información con la ciberseguridad</li> <li>7. Riesgos de la seguridad de la información</li> <li>8. Ataques relevantes</li> </ol>		

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

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

<b>Unidad 4</b> <b>Criptografía y seguridad de aplicaciones</b>		<b>Duración en horas</b>	16
<b>Resultado de aprendizaje de la unidad</b>	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.		
<b>Ejes temáticos</b>	<ol style="list-style-type: none"> <li>1. Introducción a la criptografía</li> <li>2. Criptografía asimétrica</li> <li>3. Criptografía simétrica</li> <li>4. Desarrollo seguro</li> <li>5. OWASP TOP 10</li> <li>6. Cloud computing</li> </ol>		

#### **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/ <b>Prueba objetiva</b>	<b>0 %</b>	
Consolidado 1 <b>C1</b>	1	Semana 4	- Evaluación teórico-práctica/ <b>Prueba de desarrollo</b>	30 %	<b>20 %</b>
	2	Semana 7	- Ejercicios desarrollados en clase/ <b>Rúbrica de evaluación</b>	30 %	
			- <b>Actividades de trabajo autónomo en línea</b>	40 %	
Evaluación parcial <b>EP</b>	1 y 2	Semana 8	- Evaluación teórico-práctica/ <b>Prueba de desarrollo</b>	<b>20 %</b>	
Consolidado 2 <b>C2</b>	3	Semana 12	- Evaluación teórico-práctica/ <b>Prueba de desarrollo</b>	30 %	<b>20 %</b>
	4	Semana 15	- Ejercicios desarrollados en clase/ <b>Rúbrica de evaluación</b>	30 %	
			- <b>Actividades de trabajo autónomo en línea</b>	40 %	
Evaluación final <b>EF</b>	Todas las unidades	Semana 16	- Evaluación teórico-práctica/ <b>Prueba de desarrollo</b>	<b>40 %</b>	
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 / <b>Prueba objetiva</b>	<b>0 %</b>	
Consolidado 1 <b>C1</b>	1	Semana 1 - 3	- Actividades virtuales	15 %	<b>20 %</b>
			- Ejercicios desarrollados en clase/ <b>Rúbrica de evaluación</b>	85 %	
Evaluación parcial <b>EP</b>	1 y 2	Semana 4	- Evaluación teórico-práctica/ <b>Prueba de desarrollo</b>	<b>20 %</b>	
Consolidado 2 <b>C2</b>	3	Semana 5 - 7	- Actividades virtuales	15 %	<b>20 %</b>
			- Ejercicios desarrollados en clase/ <b>Rúbrica de evaluación</b>	85 %	
Evaluación final <b>EF</b>	Todas las unidades	Semana 8	- Evaluación teórico-práctica/ <b>Prueba de desarrollo</b>	<b>40 %</b>	
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/ <b>Prueba objetiva</b>	<b>0 %</b>
Consolidado 1 <b>C1</b>	1	Semana 2	- Ejercicios desarrollados en clase/ <b>Rúbrica de evaluación</b>	<b>20 %</b>
Evaluación parcial <b>EP</b>	1 y 2	Semana 4	- Evaluación teórico-práctica/ <b>Prueba de desarrollo</b>	<b>20 %</b>
Consolidado 2 <b>C2</b>	3	Semana 6	- Ejercicios desarrollados en clase/ <b>Rúbrica de evaluación</b>	<b>20 %</b>
Evaluación final <b>EF</b>	Todas las unidades	Semana 8	- Evaluación teórico-práctica/ <b>Prueba de desarrollo</b>	<b>40 %</b>
Evaluación sustitutoria *	Todas las unidades	Fecha posterior a la evaluación final	- <b>Aplica</b>	

\* 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>