Asignatura Sistema de Información y Seguridad **Número** ISM4300

Créditos

3

Horas

45

Horas asignadas fuera de clase

90

Periodo Académico

Por determinarse

Prerrequisitos

—

Correquisitos

—

Horario y lugar de la asignatura

Es un programa *online* y el estudio se basa en materiales disponibles de forma asincrónica. Las únicas actividades presenciales son los webinarios, planeados por el profesor. A continuación, se presentan más detalles sobre los horarios del programa y de la asignatura.

Política de asistencia

La asistencia e implicación por parte del estudiante se mide por la participación en actividades académicas y de evaluación. Por lo tanto, participación en los foros semanales es obligatoria para aprobar la asignatura. Acceder al aula virtual o mandar mensajes a través del email del campus no cuentan como participación en la asignatura.

Política de tardanza

Trabajos o entradas en los foros entregados fuera de plazo no se considerarán y recibirán una nota de suspenso (F).

NOTA: El plagio se define como el uso, sin el debido reconocimiento, de las ideas, frases o mayores unidades del discurso de otro escritor u orador. El plagio incluye la copia de *software* sin autorización y la violación de las leyes de derechos de autor. Estudiantes que plagian recibirán una nota de suspenso en su examen o trabajo.

Nombre y contacto del profesor

Pendiente de aprobación.

Horario de oficina:

El profesor está disponible fuera de las horas de clase para responder a cualquier pregunta o inquietud relacionada con este curso. Los estudiantes pueden ponerse en contacto con su profesor las 24 horas del día, los 7 días de la semana a través del foro Pregúntale al Profesor en Canvas LMS. Los profesores responderán a todas las consultas en un plazo de 48 horas.

Libros y materiales obligatorios

La institución reconoce el uso de libros de texto en el aula como parte de su metodología académica. El libro de texto forma parte del plan de estudio y se utiliza para comunicar con los estudiantes en el aula de forma eficaz. La universidad aportará el material necesario para la asignatura.

Responsabilidades del estudiante

Descripción de la asignatura

La asignatura Seguridad en los Sistemas de Información te proporcionará una perspectiva global de la ciberseguridad en todos sus ámbitos, desde las distintas arquitecturas y los mecanismos de protección hasta las técnicas más avanzadas en *malware*, como *ransomware* o *botnets*, pasando por el estudio de los métodos de cifrado de la información. Todo ello te ayudará a comprender la importancia que tiene hoy en día el mundo de la ciberseguridad, tanto para empresas públicas y privadas como para usuarios, y por qué es una de las grandes apuestas de futuro.

Competencias de la asignatura

Al final de esta asignatura, el estudiante podrá:

- Aprender mecanismos de cifrado simétrico y asimétrico, así como los distintos algoritmos existentes de cada uno de ellos.
- Entender cómo funcionan los ataques a redes, estudiar sus principales amenazas y saber interpretar el tráfico entrante y saliente.
- Analizar las principales arquitecturas de seguridad y los mecanismos de protección.
- Comprender las técnicas de protección de sistemas, estudiar su implantación y determinar la importancia de cada uno de ellos.
- Analizar los patrones de los principales *malware* existentes y el funcionamiento de *botnets* en entornos de redes.

Horario de la Asignatura:

SEMANA	CONTENIDO	
Semana 1	Objetivos específicos	· Breve repaso histórico a la ciberseguridad. Analizar cómo se han «profesionalizado» los ataques a través de bandas de ciberdelincuencia, lo que ha conllevado un auge sin precedentes del ciberterrorismo y el ciberespionaje. · Presentar los primeros conceptos sobre seguridad informática, sus procedimientos y sus métodos. Definir las diferencias entre marketing estratégico y operacional. · Analizar brevemente sus objetivos, necesidades y formas de actuación.
	Temas	Tema 1. Una perspectiva global de la seguridad 1.1. Introducción y objetivos 1.2. La seguridad informática: perspectiva histórica 1.3. ¿Qué se entiende por seguridad? 1.4. Otros conceptos importantes 1.5. Cuaderno de ejercicios
	Actividades	Lectura, estudio, y comprensión de los materiales de la asignatura, incluyendo webinarios y la participación obligatoria en los foros, interacción con el profesor y los demás estudiantes. Las actividades interactivas de esta unidad son: · Clase de presentación de la asignatura y del tema 1. · Test del tema 1.
	Lectura adicional y actividades fuera del horario de clase	El profesor puede asignar actividades fuera del aula que figurarán en la calificación final del estudiante (p. ej. proyectos, casos prácticos, presentaciones, etc.). Estas actividades se comunicarán y se especificarán al estudiante a lo largo de la asignatura. Fuera de clase: 6 horas
Semana 2	Objetivos específicos	· Estudiar métodos clásicos de cifrado, que son aquellos utilizados desde prácticamente la invención de la escritura hasta la aparición de los ordenadores y los microprocesadores. · Usar técnicas de sustitución y transposición de los caracteres del texto «en claro».
	Temas	Tema 2. Criptografía y criptoanálisis clásicos 2.1. Introducción y objetivos 2.2. Historia de la criptografía 2.3. Cifradores de sustitución 2.4. Caso de estudio: la máquina Enigma

SEMANA	CONTENIDO	
		2.5. Cuaderno de ejercicios
	Actividades	Lectura, estudio, y comprensión de los materiales de la asignatura, incluyendo webinarios y la participación obligatoria en los foros, interacción con el profesor y los demás estudiantes. Las actividades interactivas de esta unidad son: · Clase del tema 2 · Test del tema 2 · Inicio foro temático 1
	Lectura adicional y actividades fuera del horario de clase	El profesor puede asignar actividades fuera del aula que figurarán en la calificación final del estudiante (p. ej. proyectos, casos prácticos, presentaciones, etc.). Estas actividades se comunicarán y se especificarán al estudiante a lo largo de la asignatura. Fuera de clase: 6 horas
Semana 3	Objetivos específicos	· Identificar los tipos de algoritmos criptográficos simétricos y sus características principales. · Asentar conceptos como «privacidad», «integridad», «autenticación» o «no repudio».
	Temas	Tema 3. Criptografía simétrica 3.1. Introducción y objetivos 3.2. Terminología básica 3.3. Cifrado simétrico 3.4. Modos de operación 3.5. El nuevo estándar AES 3.6. Cifrado en flujo 3.7. Criptoanálisis 3.8. Cuaderno de ejercicios
	Actividades	Lectura, estudio, y comprensión de los materiales de la asignatura, incluyendo webinarios y la participación obligatoria en los foros, interacción con el profesor y los demás estudiantes. Las actividades interactivas de esta unidad son: · Clase del tema 3 · Test del tema 3 · Inicio del laboratorio «Delitos informáticos en fuentes abiertas» · Inicio foro laboratorio
	Lectura adicional y	El profesor puede asignar actividades fuera del aula que figurarán en la calificación final del estudiante (p. ej.

SEMANA	CONTENIDO	
	actividades fuera del horario de clase	proyectos, casos prácticos, presentaciones, etc.). Estas actividades se comunicarán y se especificarán al estudiante a lo largo de la asignatura. Fuera de clase: 6 horas
Semana 4	Objetivos específicos	· Entender que, junto con la explosión de Internet, la criptografía de clave pública ha sido un pilar fundamental en el desarrollo del comercio electrónico, la banca online y, en general, cualquier otra área telemática que necesite seguridad en su definición y operación. · Conocer los nuevos mecanismos, como la firma o los certificados digitales, que solucionan los eternos problemas del establecimiento y la distribución de claves, o de la confidencialidad y la autenticación.
	Temas	Tema 4. Criptografía asimétrica 4.1. Introducción y objetivos 4.2. Orígenes de la criptografía de clave pública 4.3. Conceptos básicos y funcionamiento 4.4. El algoritmo RSA 4.5. Certificados digitales 4.6. Almacenamiento y gestión de claves 4.7. Resumen 4.8. Cuaderno de ejercicio
	Actividades	Lectura, estudio, y comprensión de los materiales de la asignatura, incluyendo webinarios y la participación obligatoria en los foros, interacción con el profesor y los demás estudiantes. Las actividades interactivas de esta unidad son: · Clase del tema 4 · Test del tema 4
	Lectura adicional y actividades fuera del horario de clase	El profesor puede asignar actividades fuera del aula que figurarán en la calificación final del estudiante (p. ej. proyectos, casos prácticos, presentaciones, etc.). Estas actividades se comunicarán y se especificarán al estudiante a lo largo de la asignatura. Fuera de clase: 6 horas
Semana 5	Objetivos específicos	· Identificar los principales ataques que tienen como objetivo una red. · Aprender a monitorizar el tráfico de toda una red con *sniffers*, capaces de detectar comportamientos anómalos.
	Temas	Tema 5. Ataques en redes

SEMANA	CONTENIDO	
		5.1. Introducción y objetivos 5.2. Amenazas y ataques de una red 5.3. Enumeración 5.4. Interceptación de tráfico: *sniffers* 5.5. Ataques de denegación de servicio 5.6. Ataques de envenenamiento ARP 5.7. Cuaderno de ejercicios
	Actividades	Lectura, estudio, y comprensión de los materiales de la asignatura, incluyendo webinarios y la participación obligatoria en los foros, interacción con el profesor y los demás estudiantes. Las actividades interactivas de esta unidad son: · Clase del tema 5 · Test del tema 5 · Foro temático 2
	Lectura adicional y actividades fuera del horario de clase	El profesor puede asignar actividades fuera del aula que figurarán en la calificación final del estudiante (p. ej. proyectos, casos prácticos, presentaciones, etc.). Estas actividades se comunicarán y se especificarán al estudiante a lo largo de la asignatura. Fuera de clase: 6 horas
Semana 6	Objetivos específicos	· Definir SSL como una capa de seguridad independiente que posibilita la transmisión de datos críticos sobre Internet. · Reconocer las VPN y los NAT como dos de los grandes problemas del sistema de direccionamiento de IPv4 y para la protección de dispositivos de almacenamiento seguro que guardan información confidencial. · Valorar la aparición de IPv6 debido a la escasez de direccionamientos IP.
	Temas	Tema 6. Arquitecturas de seguridad 6.1. Introducción y objetivos 6.2. Arquitecturas de seguridad tradicionales 6.3. *Secure socket layer* (SSL) 6.4. Protocolo SSH 6.5. Redes privadas virtuales (VPN) 6.6. Mecanismos de protección de unidades de almacenamiento externo 6.7. Mecanismos de protección *hardware* 6.8. Cuaderno de ejercicios

SEMANA	CONTENIDO	
	Actividades	Lectura, estudio, y comprensión de los materiales de la asignatura, incluyendo webinarios y la participación obligatoria en los foros, interacción con el profesor y los demás estudiantes. Las actividades interactivas de esta unidad son: · Clase del tema 6 · Test del tema 6
	Lectura adicional y actividades fuera del horario de clase	El profesor puede asignar actividades fuera del aula que figurarán en la calificación final del estudiante (p. ej. proyectos, casos prácticos, presentaciones, etc.). Estas actividades se comunicarán y se especificarán al estudiante a lo largo de la asignatura. Fuera de clase: 6 horas
Semana 7	Objetivos específicos	· Garantizar que los usuarios, las aplicaciones y los servidores tienen los privilegios correctos de acceso a los recursos y supervisar su implementación a través de monitorización y auditoría. · Identificar los recursos que deben ser protegidos y los privilegios que deben restringirse. · Conocer los diferentes mecanismos de control y protección que pueden emplearse en los sistemas de información.
	Temas	Tema 7. Técnicas de protección de sistemas 7.1. Introducción y objetivos 7.2. Seguridad en operaciones 7.3. Recursos y controles 7.4. Monitorización 7.5 Sistemas de detección de intrusión
	Actividades	Lectura, estudio, y comprensión de los materiales de la asignatura, incluyendo webinarios y la participación obligatoria en los foros, interacción con el profesor y los demás estudiantes. Las actividades interactivas de esta unidad son: · Clase del tema 7 · Entrega del laboratorio «Delitos informáticos en fuentes abiertas» · Fin foro laboratorio
	Lectura adicional y actividades	El profesor puede asignar actividades fuera del aula que figurarán en la calificación final del estudiante (p. ej. proyectos, casos prácticos, presentaciones, etc.). Estas

SEMANA	CONTENIDO	
	fuera del horario de clase	actividades se comunicarán y se especificarán al estudiante a lo largo de la asignatura. Fuera de clase: 6 horas
Semana 8:	Objetivos específicos	· Garantizar que los usuarios, las aplicaciones y los servidores tienen los privilegios correctos de acceso a los recursos y supervisar su implementación a través de monitorización y auditoría. · Identificar los recursos que deben ser protegidos y los privilegios que deben restringirse. · Conocer los diferentes mecanismos de control y protección que pueden emplearse en los sistemas de información. Estudiar los diferentes mecanismos de control y protección que pueden llevarse a cabo sobre los sistemas de información.
	Temas	Tema 7. Técnicas de protección de sistemas (continuación) 7.6 IDS de host 7.7. IDS de red 7.8. IDS basados en firmas 7.9. Sistemas señuelos 7.10. Cuaderno de ejercicios
	Actividades	Lectura, estudio, y comprensión de los materiales de la asignatura, incluyendo webinarios y la participación obligatoria en los foros, interacción con el profesor y los demás estudiantes. Las actividades interactivas de esta unidad son: · Clase del tema 7 · Test del tema 7 · Resolución del laboratorio «Delitos informáticos en fuentes abiertas»
	Lectura adicional y actividades fuera del horario de clase	El profesor puede asignar actividades fuera del aula que figurarán en la calificación final del estudiante (p. ej. proyectos, casos prácticos, presentaciones, etc.). Estas actividades se comunicarán y se especificarán al estudiante a lo largo de la asignatura. Fuera de clase: 6 horas
Semana 9:	Objetivos específicos	· Reconocer el verdadero alcance del spam. · Aprender a detectar el spam. · Conocer las nuevas técnicas del mundo del cibercrimen especializado en robar credenciales bancarias. · Aprender cómo ha resurgido el spam de la mano de los ciberdelincuentes y de una nueva tecnología: las *botnets*.

SEMANA	CONTENIDO	
	Temas	Tema 8. *Botnets* y *spam* 8.1. Introducción y objetivos 8.2. Proceso del *spam* 8.3. Envío del *spam* 8.4. Refinamiento de las listas de direcciones de correo 8.5. Técnicas de protección frente a *spam* 8.6. Servicios *antispam* ofrecidos por terceros 8.7. Casos de estudio 8.8. *Spam* exótico 8.9. Cuaderno de ejercicios
	Actividades	Lectura, estudio, y comprensión de los materiales de la asignatura, incluyendo webinarios y la participación obligatoria en los foros, interacción con el profesor y los demás estudiantes. Las actividades interactivas de esta unidad son: · Clase del tema 8 · Test del tema 8 · Inicio actividad «Vectores de ataque» · Inicio foro actividad
	Lectura adicional y actividades fuera del horario de clase	El profesor puede asignar actividades fuera del aula que figurarán en la calificación final del estudiante (p. ej. proyectos, casos prácticos, presentaciones, etc.). Estas actividades se comunicarán y se especificarán al estudiante a lo largo de la asignatura. Fuera de clase: 6 horas
Semana 10:	Objetivos específicos	· Estudiar las principales técnicas de ataque de las aplicaciones web. · Analizar cada técnica, comenzando con las de reconocimiento y extracción de información.
	Temas	Tema 9. Ataques a aplicaciones web 9.1. Introducción y objetivos 9.2. Recopilación de información 9.3. Técnicas de ataque 9.4. Herramientas 9.5. Cuaderno de ejercicios
	Actividades	Lectura, estudio, y comprensión de los materiales de la asignatura, incluyendo webinarios y la participación obligatoria en los foros, interacción con el profesor y los

SEMANA	CONTENIDO	
		demás estudiantes. Las actividades interactivas de esta unidad son: · Clase del tema 9 · Test del tema 9.
	Lectura adicional y actividades fuera del horario de clase	El profesor puede asignar actividades fuera del aula que figurarán en la calificación final del estudiante (p. ej. proyectos, casos prácticos, presentaciones, etc.). Estas actividades se comunicarán y se especificarán al estudiante a lo largo de la asignatura. Fuera de clase: 6 horas
Semana 11:	Objetivos específicos	· Estudiar el *software* malicioso o *malware*. · Definir con precisión sus objetivos y valorar su crecimiento exponencial en los últimos años. · Conocer los principales tipos de *malware* existentes y aprender a clasificarlos en función de algunos parámetros como capacidad de propagación o autorreplicación. · Identificar los troyanos de última generación, en especial aquellos destinados a robar credenciales de autenticación. · Analizar las motivaciones para escribir *malware*, cómo se emplea para robar dinero o cómo incluso se paga por él. · Estudiar posibles soluciones y contramedidas efectivas para evitar ser víctima de un *malware*.
	Temas	Tema 10. *Malware* y código malicioso 10.1. Introducción y objetivos 10.2. ¿Qué es el *malware*? 10.3. Tipos de *malware* 10.4. Virus 10.5. Criptovirus 10.6. Gusanos 10.7. *Adware* 10.8. *Spyware* 10.9. *Hoaxes* 10.10. *Phishing* 10.11. Troyanos 10.12. La economía del *malware* 10.13. Posibles soluciones 10.14. Cuaderno de ejercicios
	Actividades	Lectura, estudio, y comprensión de los materiales de la asignatura, incluyendo webinarios y la participación

SEMANA	CONTENIDO	
		obligatoria en los foros, interacción con el profesor y los demás estudiantes. Las actividades interactivas de esta unidad son: · Clase del tema 10. · Test del tema 10. · Inicio foro temático 3
	Lectura adicional y actividades fuera del horario de clase	El profesor puede asignar actividades fuera del aula que figurarán en la calificación final del estudiante (p. ej. proyectos, casos prácticos, presentaciones, etc.). Estas actividades se comunicarán y se especificarán al estudiante a lo largo de la asignatura. Fuera de clase: 6 horas
Semana 12:	Objetivos específicos	· Valorar la relevancia que tiene el desarrollo de código seguro en el mundo de la ciberseguridad. · Identificar los principios de seguridad básicos. · Conocer qué acciones pueden llevarse a cabo para gestionar el fallo en aplicaciones. · Analizar los errores más frecuentes a la hora de desarrollar código con criptografía.
	Temas	Tema 11. Desarrollo de código seguro 11.1. Introducción y objetivos 11.2. Principios de seguridad básicos: D^3 11.3. Gestión del fallo 11.4. Enemigo público número uno: el desbordamiento de búfer 11.5. «Chapuzas» criptográficas 11.6. Cuaderno de ejercicios
	Actividades	Lectura, estudio, y comprensión de los materiales de la asignatura, incluyendo webinarios y la participación obligatoria en los foros, interacción con el profesor y los demás estudiantes. Las actividades interactivas de esta unidad son: · Clase del tema 11. · Test del tema 11.
	Lectura adicional y actividades fuera del horario de clase	El profesor puede asignar actividades fuera del aula que figurarán en la calificación final del estudiante (p. ej. proyectos, casos prácticos, presentaciones, etc.). Estas actividades se comunicarán y se especificarán al estudiante a lo largo de la asignatura. Fuera de clase: 6 horas

SEMANA	CONTENIDO	
Semana 13:	Objetivos específicos	· Definir en qué consiste el análisis forense y determinar su ámbito de actuación. · Identificar las etapas del análisis forense y valorar la importancia de la fase de recolección de evidencias. · Conocer las técnicas antiforenses más comunes.
	Temas	Tema 12. Análisis forense 12.1. Introducción y objetivos 12.2. ¿Qué es un análisis forense? 12.3. Recolección de evidencias 12.4. Análisis de las evidencias 12.5. Técnicas antiforenses 12.6. Caso de estudio práctico 12.7. Cuaderno de ejercicios
	Actividades	Lectura, estudio, y comprensión de los materiales de la asignatura, incluyendo webinarios y la participación obligatoria en los foros, interacción con el profesor y los demás estudiantes. Las actividades interactivas de esta unidad son: · Clase del tema 12 · Entrega de la actividad «Vectores de ataque» · Fin foro actividad · Test del tema 12
	Lectura adicional y actividades fuera del horario de clase	El profesor puede asignar actividades fuera del aula que figurarán en la calificación final del estudiante (p. ej. proyectos, casos prácticos, presentaciones, etc.). Estas actividades se comunicarán y se especificarán al estudiante a lo largo de la asignatura. Fuera de clase: 6 horas
Semana 14:	Objetivos específicos	-
	Temas	-
	Actividades	Lectura, estudio, y comprensión de los materiales de la asignatura, incluyendo webinarios y la participación obligatoria en los foros, interacción con el profesor y los demás estudiantes. Las actividades interactivas de esta unidad son: · Resolución de la actividad «Vectores de ataque» · Repaso

SEMANA	CONTENIDO	
	Lectura adicional y actividades fuera del horario de clase	El profesor puede asignar actividades fuera del aula que figurarán en la calificación final del estudiante (p. ej. proyectos, casos prácticos, presentaciones, etc.). Estas actividades se comunicarán y se especificarán al estudiante a lo largo de la asignatura. Fuera de clase: 6 horas
Semana 15:	Objetivos específicos	-
	Temas	-
	Actividades	Lectura, estudio, y comprensión de los materiales de la asignatura, incluyendo webinarios y la participación obligatoria en los foros, interacción con el profesor y los demás estudiantes. Las actividades interactivas de esta unidad son: · Examen final (respuesta abierta).
	Lectura adicional y actividades fuera del horario de clase	El profesor puede asignar actividades fuera del aula que figurarán en la calificación final del estudiante (p. ej. proyectos, casos prácticos, presentaciones, etc.). Estas actividades se comunicarán y se especificarán al estudiante a lo largo de la asignatura. Fuera de clase: 6 horas

Metodología

A la hora de desarrollar estrategias metodológicas, es conveniente comentarlas entre profesores y estudiantes en un entorno abierto y de apoyo para asegurarse de que los estudiantes tomen la responsabilidad por su implementación y por lograr los objetivos de la asignatura.

Las siguientes estrategias pueden utilizarse en esta asignatura:

- Un repaso de las preguntas al final de cada capítulo.
- Comprobación de comprensión de lectura.
- Análisis de lecturas asignadas.
- Discusiones en grupo.
- Discusiones individuales y en grupo.
- Preparación de reportes.
- Creación de un plan de enseñanza.
- Llevar a cabo una microclase.

Criterios y métodos de evaluación de estudiantes

Letra	Valor numérico	GPA
A	97 – 100%	4,0
A-	90 - 96%	3,7
B+	87 – 89%	3,3
B	80 – 86%	3,0
B-	78 – 79%	2,7
C+	75 – 77%	2,3
C	70 – 74%	2,0
C-	67 – 69%	1,7
D+	63 – 66%	1,3
D	57 – 62%	1,0
F	< 57%	0,0
I	-	Incomplete*
TR	-	Transfer Credit**
W	-	Withdrawal**
WP	-	Withdraw Passing**
WF	0	Withdraw Failing

* Nota no se calcula como parte del CGPA del estudiante, pero las horas de crédito se incluyen en el total de créditos intentados.

** Nota no se calcula como parte del CGPA del estudiante, y las horas de crédito no se incluyen en el total de créditos intentados.

CALIFICACIONES APROBATORIAS

Para programas de ASSOCIATE Y BACHELOR'S, la nota aprobatoria es de C (2,0) o más.

Para programas de MÁSTER, la nota aprobatoria es de B (3,0) o más.

Distribución de calificaciones

Evaluación de la asignatura	Peso
Foros	15%
Evaluación de actividades interactivas (a través de los foros)	35%
Examen de cada tema	20%
Examen Final (respuesta abierta)	30%
Total	**100%**

Última revisión del syllabus: MAYO 2022