

1. DATOS BÁSICOS

Asignatura	Seguridad Informática
Titulación	Grado de Ingeniería Informática
Escuela/ Facultad	Escuela de Arquitectura, Ingeniería y Diseño
Curso	4º
ECTS	6
Carácter	Optativa
Idioma/s	Español
Modalidad	Presencial/Online
Semestre	S8
Curso académico	2022/2023
Docente coordinador	Oscar Cabanillas Nuñez

2. PRESENTACIÓN

“Seguridad Informática” es una asignatura optativa de 6 créditos ECTS dentro del área de Computación formada por 42 créditos ECTS siendo 6 créditos optativos. En una era digital como la actual, en la que empresas y personas poseen información importante o clasificada en sus dispositivos digitales, se hace de vital importancia conocer los riesgos existentes, ya sea en forma de ataques informáticos, espionajes o actos delictivos de los cuales se puede ser víctima, así como de las herramientas existentes para detectar los, prevenirlos y contrarrestarlos.

Esta asignatura resume la percepción que un individuo debe tener en cuanto a la seguridad informática y al tratamiento de datos sensibles. Para ello, se realiza un acercamiento a través de las recomendaciones de la Agencia de Protección de Datos y la LOPD/GDD de cómo se debe tratar la información por parte de una organización.

Una vez analizada la importancia que lleva intrínsecamente ligada la información, se pasa a realizar una observación de la seguridad informática desde un punto de vista estructural, atendiendo a definir las amenazas y mecanismos de defensa en entornos de seguridad perimetral y lógica, haciendo hincapié en la necesidad de establecer políticas de seguridad. Finalmente se realiza un acercamiento más práctico hacia la seguridad en red y la aplicación de mecanismos de criptografía para robustecer el uso de ciertas aplicaciones. El estudiante del Grado en Informática aprovechará los conocimientos obtenidos en asignaturas previas para llevar a cabo el análisis de vulnerabilidades en un sistema y plantear modelos y soluciones de seguridad.

3. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

Competencias básicas:

- CB4: Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.

- CB5: Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.

Competencias Generales de la profesión:

- CG3: Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan.

Competencias transversales:

- CT10: Iniciativa y espíritu emprendedor: Capacidad para acometer con resolución acciones difíciles o azarosas. Capacidad para anticipar problemas, proponer mejoras y perseverar en su consecución. Preferencia por asumir y llevar a cabo actividades.
- CT14: Innovación/Creatividad: Capacidad para proponer y elaborar soluciones nuevas y originales que añaden valor a problemas planteados, incluso de ámbitos diferentes al propio del problema.
- CT16: Toma de decisiones: Capacidad para realizar una elección entre las alternativas o formas existentes para resolver eficazmente diferentes situaciones o problemas.
- CT18: Utilización de las tecnologías de la información y las comunicaciones (TIC): Capacidad para utilizar eficazmente las tecnologías de la información y las comunicaciones como herramienta para la búsqueda, procesamiento y almacenamiento de la información, así como para el desarrollo de habilidades comunicativas.

Competencias específicas:

- CE18: Conocimiento y aplicación de las características, funcionalidades y estructura de las bases de datos, que permitan su adecuado uso, y el diseño y el análisis e implementación de aplicaciones basadas en ellos.
- CE21: Conocimiento y aplicación de los principios fundamentales y técnicas básicas de los sistemas inteligentes y su aplicación práctica.
- CE23: Capacidad para diseñar y evaluar interfaces persona computador que garanticen la accesibilidad y usabilidad a los sistemas, servicios y aplicaciones informáticas.
- CE26: Capacidad para conocer los fundamentos teóricos de los lenguajes de programación y las técnicas de procesamiento léxico, sintáctico y semántico asociadas, y saber aplicarlas para la creación, diseño y procesamiento de lenguajes.
- CE28: Capacidad para conocer los fundamentos, paradigmas y técnicas propias de los sistemas inteligentes y analizar, diseñar y construir sistemas, servicios y aplicaciones informáticas que utilicen dichas técnicas en cualquier ámbito de aplicación.
- CE29: Capacidad para adquirir, obtener, formalizar y representar el conocimiento humano en una formacomputable para la resolución de problemas mediante un sistema informático en cualquier ámbito de aplicación, particularmente los relacionados con aspectos de computación, percepción y actuación en ambientes o entornos inteligentes.
- CE30: Capacidad para desarrollar y evaluar sistemas interactivos y de presentación de información compleja y su aplicación a la resolución de problemas de diseño de interacción persona computadora.
- CE31: Capacidad para conocer y desarrollar técnicas de aprendizaje computacional y diseñar e implementar aplicaciones y sistemas que las utilicen, incluyendo las dedicadas a extracción automática de información y conocimiento a partir de grandes volúmenes de datos

Resultados de aprendizaje:

- RA1: Conocer la normativa relativa a protección de datos.
- RA2: Comprender los conceptos de seguridad informática.
- RA3: Implementar mecanismos de seguridad en redes.
- RA4: Utilizar técnicas y mecanismos de criptografía.
- RA5: Aplicar técnicas de análisis forense.

En la tabla inferior se muestra la relación entre las competencias que se desarrollan en la asignatura y los resultados de aprendizaje que se persiguen:

Competencias	Resultados de aprendizaje
CB5, CG3, CT10, CT14, CT16, CT18, CE18	RA1: Conocer la normativa relativa a protección de datos.
CB5, CG3, CT10, CT14, CT16, CT18, CE23	RA2: Comprender los conceptos de seguridad informática.
CB5, CG3, CT10, CT14, CT16, CT18, CE26, CE28, CE29, CE30, CE31	RA3: Implementar mecanismos de seguridad en redes.
CB5, CG3, CT10, CT14, CT16, CT18, CE21, CE26, CE28, CE29, CE30, CE31	RA4: Utilizar técnicas y mecanismos de criptografía.
CB5, CG3, CT10, CT14, CT16, CT18, CE26, CE28, CE29, CE30, CE31	RA5: Aplicar técnicas de análisis forense.

4. CONTENIDOS

- Normativa y protección de datos.
 - a. Información personal y sus riesgos.
 - B. Normativas en Protección de Datos.
 - c. LOPD
 - d. Reglamento General de Protección de Datos.
 - e. Guías de Cumplimiento.
- Seguridad Física y Lógica.
 - Introducción a la Seguridad Informática
 - Seguridad Perimetral
 - Seguridad Lógica
- Seguridad en Redes.
 - Introducción al Pentesting
 - Seguridad en Redes
 - Seguridad Redes WIFI
 - Ejemplo de Ataque Man in the Middle
- Criptografía.
 - Introducción a la criptografía
 - Cifrados de clase simétrica
 - HTTPS y SSL/TLS
- Análisis Forense.
 - Metodología
 - Adquisición de evidencias
 - Caso Práctico

5. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE

A continuación, se indican los tipos de metodologías de enseñanza/aprendizaje que se aplicarán:

- **Encuesta de objetivos e intereses.** Se utiliza para establecer los objetivos de la materia, recoger los intereses del alumno sobre la misma, y posteriormente ir haciendo referencia a lo largo del curso para que el grupo de alumnos vaya valorando la consecución de esos objetivos e intereses.

En la modalidad virtual se realiza un cuestionario inicial con este mismo objetivo, a lo largo del curso se hace referencia a esta encuesta, y se realiza un cuestionario reflexivo final para que el estudiante pueda comprobar su grado de aprendizaje de la materia.

- **Clase magistral, temas de estudio y seminarios:** Las llamadas “clases magistrales” en la modalidad presencial, en modalidad virtual se pueden denominar temas de estudio o seminarios, y se realizan a través de lectura de temas, notas técnicas y seminarios usando webconference (que son grabadas para poder ser accedidas por los estudiantes).
- **Prácticas de laboratorio:** en la modalidad presencial se utilizan principalmente los laboratorios del campus mientras en la modalidad virtual se utiliza la infraestructura de puesto remoto.
 - Investigación por grupos y/o resolución de problemas por grupos.
- **Simulación:** Se utilizarán para el desarrollo del conocimiento condicional. Sirve principalmente para desarrollar contenidos prácticos en la modalidad virtual, aunque también es aplicable en el aula para la modalidad presencial.
- **Estudio de casos prácticos:** Se utilizarán para el desarrollo del conocimiento condicional. En modalidad virtual se utiliza para desarrollar contenidos prácticos de las materias mediante foros y seminarios Esta metodología es también aplicable en el aula para la modalidad presencial.
- **Experiencias de campo, conferencias, visitas a empresas e instituciones:** Se utilizarán para el desarrollo del conocimiento condicional. En modalidad presencial podrán realizarse todas, mientras que en modalidad virtual, solo podrá realizarse la asistencia a conferencias, ya que estarán disponibles remotamente en vivo (mediante tecnologías de difusión tipo streaming) o grabadas y difundidas posteriormente.

6. ACTIVIDADES FORMATIVAS

A continuación, se identifican los tipos de actividades formativas que se realizarán y la dedicación en horas del estudiante a cada una de ellas:

Modalidad presencial:

Actividad formativa	Número de horas
Clases magistrales, lectura de temas principales y materiales complementarios, realización de actividades aplicativas individuales y colaborativas (incluye la participación en foros de aprendizaje colaborativo).	50
Trabajo en grupo de carácter integrador, que consiste en la participación en debates y seminarios, y la realización en grupo de actividades aplicativas de carácter integrador, fundamentalmente en el aula.	25
Trabajo autónomo	50
Tutorías, seguimiento académico y evaluación, tanto en el aula como a través del Campus Virtual	25

Modalidad online:

Actividad formativa	Número de horas
Trabajo autónomo	50
Lectura individual de temas y materiales complementarios y realización de actividades aplicativas individuales. Debates y seminarios virtuales	50
Trabajo grupal de carácter integrador	25
Tutorías, seguimiento académico y evaluación	25

7. EVALUACIÓN

A continuación, se relacionan los sistemas de evaluación, así como su peso sobre la calificación total de la asignatura:

Modalidad presencial:

Sistema de evaluación	Peso
Exámenes y Test	30%
Elaboración de artículos, informes y memorias de diseños	15% - 30%
Técnicas de evaluación alternativas como mapas mentales, diario, debate, portafolios y/o evaluación entre compañeros	15% - 30%
Las experiencias de campo, conferencias, visitas a empresas e instituciones se evaluarán sobre las bases de las intervenciones en un foro de discusión	0% - 10%
Ejercicios, problemas, casos prácticos, diseños, simulaciones e investigación. Actividades Individuales.	15%

Modalidad online:

Sistema de evaluación	Peso
Pruebas de conocimiento, exámenes, test	60%
Elaboración de artículos, informes o memorias de diseños	10% - 20%
Técnicas de evaluación alternativas como mapas mentales, diario, debate, portafolios y/o evaluación entre compañeros	10% - 20%
Las conferencias se evaluarán sobre las bases de las intervenciones en un foro de discusión	0% - 5%
Ejercicios, problemas, casos prácticos, diseños, simulaciones e investigación. Actividades individuales.	10% - 20%

En el Campus Virtual, cuando accedas a la asignatura, podrás consultar en detalle las actividades de evaluación que debes realizar, así como las fechas de entrega y los procedimientos de evaluación de cada una de ellas.

7.1. Convocatoria ordinaria

Para superar la asignatura en convocatoria ordinaria deberás obtener una calificación mayor o igual que 5,0 sobre 10,0 en la calificación final (media ponderada) de la asignatura.

En todo caso, será necesario que obtengas una calificación mayor o igual que 4,0 en la prueba final, para que la misma pueda hacer media con el resto de actividades.

7.2. Convocatoria extraordinaria

Para superar la asignatura en convocatoria ordinaria deberás obtener una calificación mayor o igual que 5,0 sobre 10,0 en la calificación final (media ponderada) de la asignatura.

En todo caso, será necesario que obtengas una calificación mayor o igual que 4,0 en la prueba final, para que la misma pueda hacer media con el resto de actividades.

Se deben entregar las actividades no superadas en convocatoria ordinaria, tras haber recibido las correcciones correspondientes a las mismas por parte del docente, o bien aquellas que no fueron entregadas.

8. CRONOGRAMA

En este apartado se indica el cronograma con fechas de entrega de actividades evaluables de la asignatura:

Actividades evaluables	Fecha
Análisis de la normativa de protección de datos del país	
Análisis de un ataque informático de tipo ransomware	
Intrusión en una red WiFi	
Herramientas criptográficas	
Análisis forense de un dispositivo	

Este cronograma podrá sufrir modificaciones por razones logísticas de las actividades. Cualquier modificación será notificada al estudiante en tiempo y forma.

9. BIBLIOGRAFÍA

La obra de referencia para el seguimiento de la asignatura es:

-

A continuación, se indica bibliografía recomendada:

-

10. UNIDAD DE ATENCIÓN A LA DIVERSIDAD

Estudiantes con necesidades específicas de apoyo educativo:

Las adaptaciones o ajustes curriculares para estudiantes con necesidades específicas de apoyo educativo, a fin de garantizar la equidad de oportunidades, serán pautadas por la Unidad de Atención a la Diversidad (UAD).

Será requisito imprescindible la emisión de un informe de adaptaciones/ajustes curriculares por parte de dicha Unidad, por lo que los estudiantes con necesidades específicas de apoyo educativo deberán contactar a través de: unidad.diversidad@universidadeuropea.es al comienzo de cada semestre.

11. ENCUESTAS DE SATISFACCIÓN

¡Tú opinión importa!

La Universidad Europea te anima a participar en las encuestas de satisfacción para detectar puntos fuertes y áreas de mejora sobre el profesorado, la titulación y el proceso de enseñanza-aprendizaje.

Las encuestas estarán disponibles en el espacio de encuestas de tu campus virtual o a través de tu correo electrónico.

Tu valoración es necesaria para mejorar la calidad de la titulación.

Muchas gracias por tu participación.