Guía Docente

Modalidad A DISTANCIA

Seguridad Informática

Curso 2024/25

Grado en Políticas de Seguridad y Control de la Criminalidad

UCAV

www.ucavila.es

1 Datos descriptivos de la Asignatura

Nombre:	SEGURIDAD INFORMÁTICA
Carácter:	OBLIGATORIO
Código:	40201GQ
Curso:	4º
Duración (Semestral/Anual):	ANUAL
Nº Créditos ECTS:	12
Prerrequisitos:	NINGUNO
Responsable docente:	Dra.Dña.NOELIA GUTIÉRREZ MARTÍN
Email:	noelia.gutierrez@ucavila.es
Departamento (Área Departamental):	CIENCIAS SOCIALES Y JURÍDICAS
Lengua en la que se imparte:	CASTELLANO
Módulo:	TECNOLÓGICO

2 Objetivos y competencias

2.1. COMPETENCIAS BÁSICAS

(Establecidas en el apartado 3.2. del Anexo I del Real Decreto 1393/2007 de 29 de octubre, modificado por el Real Decreto 1393/2010 de 2 de julio).

- CB1. Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio.
- CB2. Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio.
- CB3. Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.
- 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.

2.2. COMPETENCIAS GENERALES

- CG1. Adaptar el desarrollo de nuevas metodologías de trabajo al ámbito de la seguridad, en un escenario multidisciplinar que abarque elementos humanos y tecnológicos, para desarrollar de un modo eficiente las actividades relacionadas con la seguridad.
- CG2. Seleccionar la metodología de trabajo más adecuada para cada problema identificado en el campo de seguridad, mediante la formulación de hipótesis e incluyendo una reflexión sobre la responsabilidad social o ética ligada a la posible solución, para lograr la solución del mismo.
- CG3. Manejar, de un modo adecuado y eficaz para el tratamiento adecuado de la información las herramientas y recursos propios de la sociedad del conocimiento,

con especial atención a los equipos informáticos y, en general, los propios de las TIC.

- CG4. Argumentar la importancia de la gestión y autorregulación emocional, así como de la empatía en el trato con los semejantes con los cuales interactúa en el ejercicio profesional de la seguridad, mostrando una actitud de respeto hacia los derechos fundamentales en particular e individuales en general.

2.3. COMPETENCIAS TRANSVERSALES

- No hay competencias transversales asociadas a esta asignatura.

2.4. COMPETENCIAS ESPECÍFICAS

- CE22 – Detectar amenazas informáticas y analizar y diseñar sistemas de protección de dispositivos y redes para lograr una protección eficaz y, en su caso, la detección de distintos ilícitos cometidos por medio de la Red, así como la identificación de los autores.

2.4. RESULTADOS DE APRENDIZAJE

- Identificar las amenazas y riesgos de seguridad de los sistemas informáticos.
- Definir las implicaciones legales de la seguridad informática.
- Analizar software malicioso implicado en la seguridad informática.
- Manejar los controles de acceso de un sistema operativo.
- Examinar la problemática de seguridad en la red del equipo informático.
- Redactar las políticas de seguridad y mecanismos de protección pertinentes.
- Justificar la necesidad de mecanismos forenses en la seguridad informática.
- Integrar los recursos informáticos para su utilización en el ámbito de la seguridad.
- Juzgar y utilizar mecanismos de protección de recursos informáticos.

3 Contenidos de la asignatura

3.1. PROGRAMA

El desarrollo de esta materia expone los conceptos básicos de seguridad informática que se deben conocer para no poner en peligro los sistemas informáticos que se gestionan o programan desde una institución que se dedica al ámbito de la seguridad.

Se conocen herramientas con la finalidad de proteger los sistemas y detectar los errores de programación o configuración que pueden poner en peligro a los equipos informáticos en caso de ataque.

Tema 1. El marco de la ciberseguridad

Tema 2. Concienciación en Ciberseguridad

Tema 3. Ciberseguridad en el almacenamiento

Tema 4. Ciberseguridad en las Redes

Tema 5. Ciberseguridad en el Software

Tema 6. Ransomware

3.2. BIBLIOGRAFÍA

- Centro Criptológico Nacional (2020). Guía de Seguridad de las TIC: CCN-STIC 817-Esquema Nacional de Seguridad – Gestión de ciberincidentes. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html
- Centro Criptológico Nacional (2020). Norma de Seguridad de las TIC CCN-STIC-220 – Arquitecturas Virtuales. https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/5192-ccn-stic-220-arquitecturas-virtuales/file.html
- European Union Agency for Cibersecurity (2018). Handbook on security of personal data processing. https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

- Souppaya, M.; Scarfone, K. & Dodson, D. (2022). Secure Software Development Framework (SSDF) Version 1.1: (Draft) NIST Special Publication 800-218. https://doi.org/10.6028/nist.sp.800-218
- Surya Kusuma, R.; Umar, R. & Riadi, I. (2021). View of Network Forensics Against Ryuk ransomware Using Trigger, Acquire, Analysis, Report and Action (TAARA) Method. https://kinetik.umm.ac.id/index.php/kinetik/article/view/1225/124124265
- Agencia Española de Protección de Datos (2019). Gabinete Jurídico REF00148/2019. AEPD. https://www.aepd.es/es/documento/2019-0148.pdf.
- BBC (2015). El vírus que tomó control de mil máquinas y les ordenó autodestruirse. BBC News Mundo. https://bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet.
- Instituto Nacional de Ciberseguridad (2018). ¿Has revisado tu nivel de seguridad? Utiliza las auditorías de sistemas. https://www.incibe.es/protege-tu-empresa/blog/has-revisado-tu-nivel-seguridad-utiliza-las-auditorias-sistemas
- Instituto Nacional de Ciberseguridad (2020). ¿Qué son y para qué sirven los SIEM, IDS e IPS? https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

4 Indicaciones metodológicas

La asignatura se desarrollará a través de los siguientes métodos y técnicas generales, que se aplicarán diferencialmente según las características propias de la asignatura:

- **Estudio del alumno**: trabajo individual del alumno en el que estudie la materia teórica. Para ello, el alumno contará tanto con el manual de la asignatura como con el material complementario de consulta y estudio de la plataforma on-line.
- **Tutoría on-line y telefónica**: tutoría individual del alumno con el profesor en la que este le oriente en el estudio, le dirija los trabajos que esté realizando y le resuelva las dudas que se le planteen.

- **Actividades de evaluación**: exámenes finales y otras pruebas de evaluación (trabajo obligatorio).

5 Evaluación

La evaluación es un componente fundamental de la formación del alumno. Está compuesta por un examen final escrito y la evaluación continua, que consta de ejercicios y actividades evaluables.

La evaluación de esta asignatura se realiza mediante la media del examen (valorado en un 60%) y la realización de un trabajo de evaluación continua (con valor del 40%).

- Examen (60 % de la nota final)

  El examen consistirá en una prueba escrita con una serie de preguntas tipo test sobre los contenidos teóricos de la asignatura.

  La superación de dicho examen constituye un requisito indispensable para la superación de la asignatura. El alumno deberá tener en el examen al menos un 5 para poder realizar la ponderación de notas. El alumno con nota inferior se considerará suspenso. El alumno dispondrá de dos convocatorias de examen por curso académico.

  En el caso de que el examen estuviera aprobado, pero el alumno hubiera suspendido el trabajo obligatorio, la nota del examen no se guardará. El alumno tendrá que hacer el examen de nuevo.

- Trabajo de evaluación continua (40% de la nota final)

  El alumno deberá tener en el trabajo al menos un 5 para poder realizar la ponderación de notas. El alumno con nota inferior se considerará suspenso. En el caso de que el trabajo estuviera aproado, la nota solo se guardará dentro del mismo curso académico.

  El trabajo constará siempre de una parte escrita y una exposición oral del mismo.

No se admitirán trabajos fuera de la fecha límite de entrega, que será comunicada al alumno con suficiente antelación.

EJERCICIOS Y ACTIVIDADES EVALUABLES	PROPORCIÓN
Trabajo de evaluación continua	40%
Examen final	60%
TOTAL	**100%**

Criterios de calificación de la evaluación continua

Los criterios para la evaluación del trabajo de evaluación continua, donde se resumen los aspectos a valorar y el porcentaje que representa cada uno de los mismos:

COMPONENTES EVALUABLES	PROPORCIÓN
Corrección gramatical y ortográfica	10%
Estructura clara y organización del documento	10%
Aplicación de los conceptos aprendidos en la asignatura	30 %
Justificación de las diferentes decisiones tomadas en la implementación de las diferentes medidas	30 %
Conclusiones personales	20%
TOTAL	**100%**

6 Apoyo tutorial

Para el apoyo tutorial, el alumno tendrá a su disposición un equipo docente encargado de acompañar al alumno durante toda su andadura en el proceso formativo, prestando una atención personalizada al alumno. Sus funciones están claramente diferenciadas complementándose al mismo tiempo. Las personas principales de este acompañamiento tutorial son:

- **Coordinador:** encargado de resolver cualquier problema docente a nivel general y de dar al alumno toda la información de carácter general necesaria en su proceso formativo.
- **Orientador Académico Personal:** encargado de planificar al alumno el estudio de la asignatura en función del tiempo disponible, incluso realiza nuevas planificaciones ajustándose a nuevos periodos marcados por el alumno según sus circunstancias personales y familiares. Otra de sus funciones es la de realizar un seguimiento del estudio del alumno, así como de dar al alumno información de carácter general necesaria en su proceso formativo.
- **Profesor docente:** encargado de resolver todas las dudas específicas de la asignatura y de informar al alumno de todas las pautas que debe seguir para realizar el estudio de la asignatura.

El alumno dispondrá de un horario de tutorías para contactar con estas tres figuras durante toda su formación académica. La información sobre el horario la encontrará el alumno en la plataforma virtual.

Horario de tutorías de la asignatura:

El alumno deberá consultar los horarios de clases de la asignatura en el apartado correspondiente dentro de la página web de la UCAV: www.ucavila.es. Igualmente, se informará de ellos en la Plataforma Blackboard.

En relación a los horarios de atención en tutorías para consultas, aclaración de dudas, revisiones de trabajos y exámenes, etc., el profesor informará en la plataforma Blackboard de las franjas en las que tenga disponibilidad, pudiendo variar de un cuatrimestre a otro y también durante los meses de verano. Todo ello será informado oportunamente y con suficiente antelación a través del Campus Virtual.

Herramientas para la atención tutorial: Plataforma Blackboard, atención telefónica y atención presencial siempre que sea posible. Las tutorías se solicitarán previamente por correo electrónico o plataforma.

7 Horario de la asignatura y Calendario de temas

Horario de la asignatura: El alumno deberá consultar los horarios de clases de la asignatura en el apartado correspondiente dentro de la página web de la UCAV: www.ucavila.es. Igualmente, se informará de ellos en la Plataforma Blackboard.

El peso de cada unidad formativa dentro de cada asignatura queda determinado en el cronograma por el tiempo dedicado a la misma. El alumno deberá acometer el estudio marcado por la herramienta de planificación utilizada en el campus virtual, después de la planificación realizada con su tutor. A continuación, se muestra una tabla con las unidades didácticas que componen la asignatura y las unidades de tiempo que, orientativamente, se requieren para su estudio.

UNIDADES DIDÁCTICAS	UNIDAD DE TIEMPO	HORAS DEDICACIÓN
Unidad 1	16,66 %	25 HORAS
Unidad 2	16,66 %	25 HORAS
Unidad 3	16,66 %	25 HORAS
Unidad 4	16,66 %	25 HORAS
Unidad 5	16,66 %	25 HORAS
Unidad 6	16,70 %	25 HORAS
TOTAL	**100 %**	**150**