Guía de Asignatura

ASIGNATURA: *Criptografía*

Título: Grado en Ciberseguridad
Materia: *Seguridad Tecnológica*
Créditos: *6 ECTS*
Código: 11GCIB

Índice

1. Organización general

1.1. Datos de la asignatura

TITULACIÓN	*Grado en Ciberseguridad*
ASIGNATURA	*Criptografía*
CÓDIGO - NOMBRE ASIGNATURA	*11GCIB_Criptografía*
Carácter	Obligatoria
Semestre	Tercero
Idioma en que se imparte	Castellano
Requisitos previos	No existen
Dedicación al estudio por ECTS	**25 horas**

1.2. Introducción a la asignatura

Estudio de la criptografía, los fundamentos matemáticos y criptografía clásica, la criptografía de clave privada y de clave pública, los protocolos y aplicaciones criptográficas, y la criptografía cuántica, permitiendo que los alumnos apliquen la criptografía a todos los ámbitos posibles de la ciberseguridad, especialmente en las comunicaciones, bases de datos, sistemas, redes y aplicaciones.

1.3. Competencias y resultados de aprendizaje

CÓDIGO	COMPETENCIAS
C02	Emplear diferentes lenguajes de programación en el desarrollo de algoritmos, aplicaciones y herramientas informáticas en el ámbito de la ciberseguridad.
C03	Desarrollar de forma segura herramientas, aplicaciones y software informáticos.
C04	Administrar y configurar de manera segura los sistemas informáticos, redes, dispositivos y bases de datos frente a amenazas y ataques cibernéticos.
C10	Vigilar y monitorizar el funcionamiento de sistemas, redes y dispositivos desde el punto de vista de la detección de amenazas, riesgos, vulnerabilidades y ataques.
CÓDIGO	HABILIDADES O DESTREZAS
H01	Redactar documentos técnicos en el ámbito de la ciberseguridad empleando la terminología adecuada.
H02	Manejar bibliografía específica en el ámbito de la informática y la ciberseguridad.

H03	Analizar y resolver problemas complejos en el ámbito de la ciberseguridad.
H04	Trabajar en equipos multidisciplinares en el ámbito de la informática.
CÓDIGO	CONOCIMIENTOS O CONTENIDOS
CC7	Comprender y saber aplicar técnicas de criptografía en el ámbito de la ciberseguridad.
CC8	Comprender los requerimientos, técnicas y herramientas de ciberseguridad propias de los diferentes componentes, dispositivos y elementos de un sistema informático o red de comunicaciones.
CC11	Comprender los riesgos, amenazas y vulnerabilidades propias de las diferentes tecnologías, dispositivos y sistemas informáticos, así como las medidas aplicables de prevención y respuesta.

2. Contenidos/temario

- Introducción a la criptografía.
- Fundamentos matemáticos y criptografía clásica.
- Criptografía de clave privada.
- Criptografía de clave pública.
- Otros protocolos y aplicaciones criptográficas.
- Criptografía cuántica.

3. Metodología

La modalidad de enseñanza propuesta para el presente título guarda consonancia con la Metodología General de la Universidad Internacional de Valencia, aprobada por el Consejo de Gobierno Académico de la Universidad y de aplicación en todos sus títulos.

Este modelo, que vertebra el conjunto de procesos de enseñanza y aprendizaje de la institución, combina la naturaleza síncrona (mismo tiempo-diferente espacio) y asíncrona (diferente tiempo -diferente espacio) de los entornos virtuales de aprendizaje, siempre en el contexto de la modalidad virtual.

El elemento síncrono se materializa en sesiones de diferente tipo (clases expositivas y prácticas, tutorías, seminarios y actividades de diferente índole durante las clases online) donde el profesor y el estudiante comparten un espacio virtual y un tiempo determinado que el estudiante conoce con antelación.

Las actividades síncronas forman parte de las actividades formativas necesarias para el desarrollo de la asignatura y, además, quedan grabadas y alojadas para su posterior visualización.

Por otro lado, estas sesiones no solamente proporcionan espacios de encuentro entre estudiante y profesor, sino que permiten fomentar el aprendizaje colaborativo, al generarse grupos de trabajo entre los estudiantes en las propias sesiones.

Los elementos asíncronos del modelo se desarrollan a través del Campus Virtual, que contiene las aulas virtuales de cada asignatura, donde se encuentran los recursos y contenidos necesarios para el desarrollo de actividades asíncronas, así como para la interacción y comunicación con los profesores y con el resto de departamentos de la Universidad.

4. Actividades formativas

La metodología VIU, basada en la modalidad virtual, se concreta en una serie de actividades formativas y metodologías docentes que articulan el trabajo del estudiante y la docencia impartida por los profesores.

Durante el desarrollo de cada una de las asignaturas, se programan una serie de actividades de aprendizaje que ayudan a los estudiantes a consolidar los conocimientos trabajados en cada una de las asignaturas. A continuación, listamos las actividades genéricas que pueden formar parte de cada asignatura, dependiendo de las competencias a desarrollar en los estudiantes en cada asignatura.

1. Clases presenciales

2. Clases virtuales síncronas

Constituyen el conjunto de acciones formativas que ponen en contacto al estudiante con el profesor, con otros expertos y con compañeros de la misma asignatura en el mismo momento temporal a través de herramientas virtuales. Las actividades recurrentes (por ejemplo, las clases) se programan en el calendario académico y las que son ocasionales (por ejemplo, sesiones con expertos externos) se avisan mediante el tablón de anuncios del campus. Estas actividades se desglosan en las siguientes categorías:

a. Clases expositivas: El profesor expone a los estudiantes los fundamentos teóricos de la asignatura.

b. Clases prácticas: El profesor desarrolla junto con los estudiantes actividades prácticas que se basan en los fundamentos vistos en las clases expositivas. En términos generales, su desarrollo consta de las siguientes fases, pudiéndose adaptar en función de las necesidades docentes:

I. La primera fase se desarrolla en la sala principal de la videoconferencia, donde el profesor plantea la actividad.

II. A continuación, divide a los estudiantes en grupos de trabajo a través de las salas colaborativas y se comienza con la actividad. En esta fase el profesor va entrando en cada sala colaborativa rotando los grupos para resolver dudas, dirigir el trabajo o dar el feedback oportuno. Los estudiantes también tienen posibilidad de consultar al profesor en el momento que consideren necesario.

III. La tercera fase también se desarrolla en la sala principal y tiene como objetivo mostrar el ejercicio o explicar con ejemplos los resultados obtenidos. Por último, se ponen en común las conclusiones de la actividad realizada.

No obstante, el profesor puede utilizar otras metodologías activas y/o herramientas de trabajo colaborativo en estas clases.

c. Seminarios: En estas sesiones un experto externo a la Universidad acude a presentar algún contenido teórico-práctico directamente vinculado con el temario de la asignatura. Estas sesiones permiten acercar al estudiante a la realidad de la disciplina en términos no sólo profesionales, sino también académicos. Todas estas sesiones están vinculadas a contenidos de las asignaturas y del programa educativo.

3. Actividades asíncronas supervisadas

Se trata de un conjunto de actividades supervisadas por el profesor de la asignatura vinculadas con la adquisición por parte de los estudiantes de los resultados de aprendizaje y el desarrollo de sus competencias. Estas actividades, diseñadas con visión de conjunto, están relacionadas entre sí para ofrecer al estudiante una formación completa e integral. Esta categoría se desglosa en el siguiente conjunto de actividades:

a. Actividades y trabajos prácticos: se trata de un conjunto de actividades prácticas realizadas por el estudiante por indicación del profesor que permiten al estudiante adquirir las competencias del título, especialmente aquellas de carácter práctico. Estas actividades, entre otras, pueden ser de la siguiente naturaleza: actividades vinculadas a las clases prácticas (resúmenes, mapas conceptuales, one minute paper, resolución de problemas, análisis reflexivos, generación de contenido multimedia, exposiciones de trabajos, test de autoevaluación, participación en foros, entre otros). Estas actividades serán seleccionadas por el profesor en función de las necesidades docentes. Posteriormente, estas actividades son revisadas por el profesor, que traslada un feedback al estudiante sobre las mismas, pudiendo formar parte de la evaluación continua de la asignatura.

b. Actividades guiadas con recursos didácticos audiovisuales e interactivos: se trata de un conjunto de actividades en las que el estudiante revisa o emplea recursos didácticos (bibliografía, videos, recursos interactivos) bajo las indicaciones realizadas previamente por el profesor; con el objetivo de profundizar en los contenidos abordados en las sesiones teóricas y prácticas. Estas sesiones permiten la reflexión o práctica por parte del estudiante, y pueden complementarse a través de la puesta en común en clases síncronas o con la realización de actividades y trabajos prácticos. Posteriormente, estas actividades son revisadas por el profesor, que traslada un feedback al estudiante sobre las mismas, pudiendo formar parte de la evaluación continua de la asignatura.

4. Tutorías

En esta actividad se engloban las sesiones virtuales de carácter síncrono y las comunicaciones por correo electrónico o campus virtual destinadas a la tutorización de los estudiantes. En ellas, el profesor comparte información sobre el progreso del trabajo del estudiante a partir de las evidencias recogidas, se resuelven dudas y se dan orientaciones específicas ante dificultades concretas en el desarrollo de la asignatura. Pueden ser individuales o colectivas, según las necesidades de los estudiantes y el carácter de las dudas y orientaciones planteadas. Tal y como se ha indicado, se realizan a través de videoconferencia y e-mail.

Se computan una serie de horas estimadas, pues, aunque existen sesiones comunes para todos los estudiantes, éstos posteriormente pueden solicitar al docente tantas tutorías como estimen necesarias.

Dado el carácter mixto de esta actividad formativa, se computa un porcentaje de sincronía estimado del 30%.

5. Estudio autónomo

En esta actividad el estudiante consulta, analiza y estudia los manuales, bibliografía y recursos propios de la asignatura de forma autónoma a fin de lograr un aprendizaje significativo y superar la evaluación de la asignatura de la asignatura. Esta actividad es indispensable para adquirir las competencias del título, apoyándose en el aprendizaje autónomo como complemento a las clases y actividades supervisadas.

6. Examen final

Como parte de la evaluación de cada una de las asignaturas (a excepción de las prácticas y el Trabajo fin de título), se realiza una prueba o examen final. Esta prueba se realiza en tiempo real (con los medios de control antifraude especificados) y tiene como objetivo evidenciar el nivel de adquisición de conocimientos y desarrollo de competencias por parte de los estudiantes. Los exámenes o pruebas de evaluación final se realizan en las fechas y horas programadas con antelación y con los sistemas de vigilancia online (proctoring) de la universidad.

5. Evaluación

5.1. Sistema de evaluación

El Modelo de Evaluación de estudiantes en la Universidad se sustenta en los principios del Espacio Europeo de Educación Superior (EEES), y está adaptado a la estructura de formación virtual propia de esta Universidad. De este modo, se dirige a la evaluación de competencias.

Sistema de Evaluación	Ponderación
Portafolio*	60 %
Sistema de Evaluación	Ponderación
Prueba final*	40 %

***Es requisito indispensable para superar la asignatura aprobar cada apartado (portafolio y prueba final)** con un mínimo de 5 para ponderar las calificaciones.

Los enunciados y especificaciones propias de las distintas actividades serán aportados por el docente, a través del Campus Virtual, a lo largo de la impartición de la asignatura.

Atendiendo a la Normativa de Evaluación de la Universidad, se tendrá en cuenta que la utilización de **contenido de autoría ajena** al propio estudiante debe ser citada adecuadamente en los trabajos entregados. Los casos de plagio serán sancionados con suspenso (0) de la actividad en la que se detecte. Asimismo, el uso de **medios fraudulentos durante las pruebas de evaluación** implicará un suspenso (0) y podrá implicar la apertura de un expediente disciplinario.

5.2. Sistema de calificación

La calificación de la asignatura se establecerá en los siguientes cómputos y términos:

Nivel de aprendizaje	Calificación numérica	Calificación cualitativa
Muy competente	9,0 - 10	Sobresaliente
Competente	7,0 - 8,9	Notable
Aceptable	5,0 -6,9	Aprobado
Aún no competente	0,0 -4,9	Suspenso

Sin detrimento de lo anterior, el estudiante dispondrá de una **rúbrica simplificada** en el aula que mostrará los aspectos que valorará el docente, como así también los **niveles de desempeño que tendrá en cuenta para calificar las actividades vinculadas a cada resultado de aprendizaje.**

La mención de «**Matrícula de Honor**» podrá ser otorgada a estudiantes que hayan obtenido una calificación igual o superior a 9.0. Su número no podrá exceder del cinco por ciento de los estudiantes matriculados en una materia en el correspondiente curso académico, salvo que el número de estudiantes matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola «Matrícula de Honor.

6. Bibliografía

Arboledas Brihuega, D. (2017). *Criptografía sin secretos con Python:* (ed.). RA-MA Editorial. https://elibro-net.universidadviu.idm.oclc.org/es/ereader/universidadviu/106497?page=1

Bray, S. W. (2020). Implementing cryptography using python. John Wiley & Sons, Incorporated.

Chauhan, S. R., & Jangra, S. (2020). Computer security and encryption : An introduction. Mercury Learning & Information.

Dash, S. K. (2023). Ultimate web authentication handbook : Strengthen web security by leveraging cryptography and authentication protocols such as oauth, saml and fido. Orange Education PVT Ltd.

Francisco Javier López Brea Espiau, & José Ramón Soler Fuensanta. (2016). *Mensajes Secretos*. Tirant lo Blanch. https://biblioteca-tirant-com.universidadviu.idm.oclc.org/cloudLibrary/login/login?username=VIU&password=MJE09fZ&redirectto=/ebook/info/9788491194064

Hernández Encinas, L. (2016). *La criptografía:* (ed.). Editorial CSIC Consejo Superior de Investigaciones Científicas. https://elibro-net.universidadviu.idm.oclc.org/es/ereader/universidadviu/41843?page=1

Hernández Encinas, L. Gayoso Martínez, V. & Martín Muñoz, A. (2018). *Criptografía con curvas elípticas:* (ed.). Editorial CSIC Consejo Superior de Investigaciones Científicas. https://elibro-net.universidadviu.idm.oclc.org/es/ereader/universidadviu/106372?page=1

Mason, S. (2016). Electronic Signatures in Law. University of London Press. http://www.jstor.org/stable/j.ctv5137w8

McAndrew, A. (2011). Introduction to cryptography with open-source software. Taylor & Francis Group.

Ortega, C. J. M. (2024). Python aplicado a seguridad y redes. Marcombo, S.A. https://ebookcentral.proquest.com/lib/universidadviu/detail.action?docID=31355143

Rohit, G. S. C. (2024). Ultimate pentesting for web applications : Unlock advanced web app security through penetration testing using burp suite, zap proxy, fiddler, charles proxy, and python for robust defense (english edition). Orange Education PVT Ltd.

Sweigart, A. (2018) Cracking Codes with Python. https://inventwithpython.com/cracking/