1. DATOS BÁSICOS

Asignatura	Criptografía aplicada y control de accesos
Titulación	Máster Universitario en Seguridad de las Tecnologías de la Información y las Comunicaciones
Escuela/ Facultad	Arquitectura, Ingeniería y Diseño
Curso	Primero
ECTS	6 ECTS
Carácter	Obligatorio
Idioma/s	Castellano
Modalidad	Presencial: 0DCS001103 Online: P630001103
Semestre	Primer semestre
Curso académico	2024/2025
Docente coordinador	
Docente	Presencial: Dr. Alfonso Muñoz Muñoz/Alberto López González Online: Dr. Jordi Serra Ruiz

2. PRESENTACIÓN

Se profundizará en el estudio de las bases de los sistemas para preservar la confidencialidad, los algoritmos criptográficos y su aplicación práctica en el ámbito de la seguridad electrónica. El alumno aprenderá los fundamentos y la implementación de los algoritmos de cifrado simétricos y asimétricos, así como nuevos paradigmas criptográficos. Así mismo, se familiarizará con las infraestructuras de clave pública (PKI), las tecnologías de certificación y su uso corporativo. También conocerá cuáles son los principales prestadores de servicios de certificación españoles, así como la normativa vigente.

Dentro de este módulo, el estudiante aprenderá técnicas de control y administración de usuarios empleando sistemas de autenticación robusta multifactor y sistemas para la provisión de identidades y soluciones de metadirectorio. Asimismo, conocerá el caso particular de la gestión de identidades en entornos Web.

3. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

Competencias básicas:

- CG4: Emitir juicios en función de criterios, de normas externas o de reflexiones personales.
- CG6: Capacidad para integrarse en equipos de trabajo multidisciplinares de manera eficaz y cooperativa.

Competencias específicas:

- CE6: Comprender y saber aplicar los fundamentos de las técnicas criptográficas y su empleo actual en el ámbito de la seguridad electrónica

- CE7: Conocer los fundamentos de las infraestructuras de clave pública (PKI), las tecnologías de certificación y su uso corporativo. También conocerá cuáles son los principales prestadores de servicios de certificación españoles, así como la normativa vigente.
- CE8: Analizar las técnicas de control y administración de usuarios empleando sistemas de autenticación robusta y sistemas para la provisión de identidades.

Resultados de aprendizaje:
- RA1: El estudiante será capaz de aplicar los conceptos básicos utilizando técnicas de aprendizaje cooperativo.
- RA2: El estudiante será capaz de trabajar en equipo, comunicarse de forma oral y escrita y aplicar los contenidos de las asignaturas para realizar juicios críticos.

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
CG6, CE6, CE7	RA1
CG4, CG6, CE6, CE7, CE8	RA2

4. CONTENIDOS

La materia está organizada en los siguientes contenidos:

3.1. Técnicas criptográficas
1. Algoritmos criptográficos
2. Aplicaciones actuales de la criptografía
3. Control de integridad

3.2. Certificación y firma electrónica
1. Firma digital y firma electrónica
2. Las Infraestructuras de Clave Pública (PKI)
3. Tecnologías de certificación y su uso corporativo
4. Principales prestadores de servicios de certificación españoles
5. Normativa vigente

3.3. Gestión de identidades y accesos
1. Métodos y tecnologías de identificación
2. Métodos, tecnologías y modelos de Autenticación, autorización y Auditoria (AAA)

5. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE

A continuación, se indican los tipos de metodologías de enseñanza-aprendizaje que se aplicarán:
- Clase magistral.
- Método del caso.
- Aprendizaje cooperativo.
- Aprendizaje basado en proyectos.

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
A1. Presentación en el aula de conocimientos por parte del profesor utilizando el método de exposición	37,5 h
A2. Actividades de carácter grupal relativas a la aplicación de casos prácticos	50 h
A3. Tutorías y evaluación	25 h
A4. Estudio independiente del alumno	37,5 h
TOTAL	**150h**

Modalidad online:

Actividad formativa	Número de horas
A1. Participación en debates y foros de discusión moderados por el profesor	32,5 h
A2. Realización de actividades aplicativas: estudios de caso, resolución de problemas, elaboración de planes, análisis de situaciones profesionales, etc.	25 h
A3. Trabajo integrador del módulo	10 h
A4. Realización de actividades aplicativas: estudios de caso, resolución de problemas, elaboración de planes, análisis de situaciones profesionales, etc.	25 h
A5. Estudio independiente del alumno	32,5 h
A6. Tutoría y evaluación	25 h
TOTAL	**150h**

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
A1. Realización de prácticas criptográficas con Cryptool y cyberchef	5%
A2. Uso de OpenSSL para el cifrado simétrico	5%

A3. Prueba de evaluación	35%
A4. Prácticas de firma con PGP.	15%
A5. Participación en los debates iniciados en clase	5%
A6. Práctica seguridad contraseñas y credenciales	10%
A7. Práctica Red Windows/Linux control de accesos, ataques y gestión de identidad	25%

En el Campus Virtual, cuando accedas a la asignatura, podrás consultar en detalle las actividades 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.

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.

Modalidad online:

Sistema de evaluación	Peso
A1. Cifrado César	10%
A2. Expansión de clave en AES	25%
A3. Adición en Curvas Elípticas	15%
A4. Certificados y Ruptura de contraseñas	25%
A5. Prueba de Conocimientos	25%

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

En ambas convocatorias (ordinaria y extraordinaria) se permitirá la entrega tardía con un máximo de una semana a partir de la fecha de entrega fijada, con una **penalización de 0,25 puntos sobre 10 por día de**

retraso. Una vez superada la semana, no se permitirá la entrega salvo casos excepcionales de fuerza mayor que deba estudiar el personal docente implicado.

Las actividades se entregarán en el campus virtual, no siendo válida la entrega por correo electrónico.

7.3. Convocatoria ordinaria

Para superar la asignatura en convocatoria ordinaria deberás:

- Obtener una nota media ponderada de las actividades que figuran en la tabla (A1 hasta A4), exceptuando la prueba de conocimiento, igual o superior a 5.
- Obtener en la prueba de conocimiento una calificación igual o superior a 5.

7.4. Convocatoria extraordinaria

Para superar la asignatura en convocatoria extraordinaria deberás:

- Obtener una nota media ponderada de las actividades que figuran en la tabla (A1 hasta A5), exceptuando la prueba de conocimiento, igual o superior a 5.
- Obtener en la prueba de conocimiento una calificación igual o superior a 5.

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.

8. CRONOGRAMA

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

Modalidad presencial:

Actividades evaluables	Fecha
A1. Realización de prácticas criptográficas con Cryptool y cyberchef	W3
A2. Uso de OpenSSL para el cifrado simétrico	W5
A3. Prueba de evaluación	W6
A4. Presentación de un artículo especializado	W6
A5. Participación en los debates iniciados en clase	W7
A6. Práctica seguridad contraseñas y credenciales	W10

A7. Práctica Red Windows/Linux control de accesos, ataques y gestión de identidad	W12

Modalidad online:

Actividades evaluables	Fecha
A1. Cifrado César	SEM 2
A2. Expansión de clave en AES	SEM 5
A3. Adición en Curvas Elípticas	SEM 8
A4. Certificados y Ruptura de contraseñas	SEM 10
A6. Prueba de Conocimientos	SEM 12

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

9. BIBLIOGRAFÍA

M3.1. Técnicas criptográficas

- Singh, Simon, The Code Book (2002) The secret history of codes and code-breaking, USA: Fourth State
- Schneier, Bruce (2015) Applied Cryptography, USA: Wiley
- Kahn, David (1996) The CodeBreakers, USA: Scribner
- Hodge, Andrew (2014) Alan Turing: The Enigma: The Book That Inspired the Film "The Imitation Game, USA: Princeton
- Pinardi, Raffaele et al (2013), Peak-Shaped-Based Steganographic Technique for MP3 Audio, Journal of Information Security Vol.4 No.1(2013)
- Feistel, H. (1973) Cryptography and Computer Privacy. Scientific American, 228, 15-23. http://dx.doi.org/10.1038/scientificamerican0573-15
- Joye, Marc (2008) On White-Box Cryptograpy, Trafford Publishing
- Halevi, Shai et al (2014) Algorithms in HElib, USA: Eurocrypt 2014

M3.2. Certificación y firma electrónica

- Fúster, A., Hernández, L., Montoya, F., Muñoz, J., Martín, A. Criptografía, protección de datos y aplicaciones (2012). Una guía para estudiantes y profesionales. Ra-Ma.
- Rodríguez, E. (2016). La firma digital en el mundo empresarial

M3.3. Gestión de identidades y accesos

- Gollmann, Dieter, (2003) Computer Security, USA: Wiley.
- http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf Cryptographer's panel - https://www.youtube.com/watch?v=k76qLOrna1w https://en.wikipedia.org/wiki/EFF_DES_cracker (1998)
- https://www.cs.cmu.edu/~sbhagava/papers/face-rec-ccs16.pdf
- http://www.graphics.stanford.edu/~niessner/thies2016face.html
- AAA Authorization framework - https://tools.ietf.org/html/rfc2904
- http://web.mit.edu/kerberos/www/
- https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2

10. UNIDAD DE ATENCIÓN A LA DIVERSIDAD

Desde la Unidad de Orientación Educativa y Diversidad (ODI) ofrecemos acompañamiento a nuestros estudiantes a lo largo de su vida universitaria para ayudarles a alcanzar sus logros académicos. Otros de los pilares de nuestra actuación son la inclusión del estudiante con necesidades específicas de apoyo educativo, la accesibilidad universal en los distintos campus de la universidad y la equiparación de oportunidades.
Desde esta Unidad se ofrece a los estudiantes:

1. Acompañamiento y seguimiento mediante la realización de asesorías y planes personalizados a estudiantes que necesitan mejorar su rendimiento académico.
2. En materia de atención a la diversidad, se realizan ajustes curriculares no significativos, es decir, a nivel de metodología y evaluación, en aquellos alumnos con necesidades específicas de apoyo educativo persiguiendo con ello una equidad de oportunidades para todos los estudiantes.
3. Ofrecemos a los estudiantes diferentes recursos formativos extracurriculares para desarrollar diversas competencias que les enriquecerán en su desarrollo personal y profesional.
4. Orientación vocacional mediante la dotación de herramientas y asesorías a estudiantes con dudas vocacionales o que creen que se han equivocado en la elección de la titulación.

Los estudiantes que necesiten apoyo educativo pueden escribirnos a:
orientacioneducativa@universidadeuropea.es

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.

REGLAMENTO PLAGIO

Atendiendo al Reglamento disciplinario de los estudiantes de la Universidad Europea:

- El plagio, en todo o en parte, de obras intelectuales de cualquier tipo se considera falta muy grave.
- Las faltas muy graves relativas a plagios y al uso de medios fraudulentos para superar las pruebas de evaluación, tendrán como consecuencia la pérdida de la convocatoria correspondiente, así como el reflejo de la falta y su motivo, en el expediente académico.

REGLAMENTO DE LA IA

El estudiante debe ser el autor o autora de sus trabajos/actividades.

El uso de herramientas de Inteligencia Artificial (IA) debe ser autorizado por el docente en cada trabajo/actividad, indicando de qué manera está permitido su uso. El docente informará previamente en qué situaciones se podrá usar herramientas de IA para mejorar la ortografía, gramática y edición en general. El estudiante es responsable de precisar la información dada por la herramienta y declarar debidamente el uso de cualquier herramienta de IA, en función de las directrices que marque el docente. La decisión final sobre la autoría del trabajo y la idoneidad del uso reportado de una herramienta de IA recae en el docente y en los responsables de la titulación.