1. Datos básicos de la asignatura/módulo

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 – P630001103 Online – 0DCS001103
Semestre	Primer semestre
Curso académico	2020/2021
Docente coordinador	Presencial: Dr. Luis Antonio de Salvador Carrasco Online: Dr. Luis Antonio de Salvador Carrasco

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. OMPETENCIAS 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

1.1 TÉCNICAS CRIPTOGRÁFICAS

Unidad 1. Técnicas criptográficas I

- 1.1. Introducción a la criptografía.
- 1.2. Fundamentos históricos.
- 1.3. Base matemática.
- 1.4 Esteganografía

Unidad 2. Técnicas criptográficas II

- 2.1. Transposición y sustitución.
- 2.2. Algoritmos clásicos.
- 2.3. Cifrado polialfabético.
- 2.4. Criptografía simétrica

Unidad 3. Técnicas criptográficas III

- 3.1. Criptoanálisis.
- 3.2. Gestión de claves.
- 3.3. Elementos del sistema de cifrado.
- 3.4. AES

1.2 CERTIFICACIÓN Y FIRMA ELECTRÓNICA

Unidad 4. Certificación y firma electrónica I

- 4.1. Cifrado de Clave Pública.
- 4.2. Curvas elípticas.
- 4.3. Curvas elípticas aplicadas.
- 4.4. Criptografía cuántica.

Unidad 5. Certificación y firma electrónica II

- 5.1. Firma digital.
- 5.2. Esquemas y formatos de firma digital.
- 5.3. Infraestructura de Clave Pública.
- 5.4. Conceptos avanzados de PKI

1.3 GESTIÓN DE IDENTIDADES Y ACCESOS

Unidad 6. Gestión de identidades y accesos

- 5.1. Autenticación y control de accesos.
- 5.2. Sistemas biométricos y combinados.
- 6.3. Sistemas de autenticación
- 6.4. Modelos de control de acceso

5. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE

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

- Clases magistrales
- 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

Tipo de 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	**150 h**

MODALIDAD ONLINE

Tipo de 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	**150 h**

7. EVALUACIÓN

Para desarrollar las competencias y alcanzar los resultados de aprendizaje indicados, deberás realizar las actividades que se indican en la tabla inferior:

MODALIDAD PRESENCIAL

Actividad evaluable	Actividad de aprendizaje	Peso (%)
Actividad 1	Ejercicios para resolver por equipos	15%
Actividad 2	Examen de conocimientos básicos y realización de problemas.	25%
Actividad 3	Prueba de evaluación.	15%
Actividad 4	Presentación de un artículo especializado.	15%
Actividad 5	Participación en los debates iniciados en clase	5%
Actividad 6	Práctica seguridad contraseñas y credenciales	10%
Actividad 7	Práctica Red Windows/Linux control de accesos, ataques y gestión de identidad	15%

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. Una vez superada esta fecha, 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

MODALIDAD ONLINE

Actividad evaluable	Actividad de aprendizaje	Peso (%)
A1	Ejecución de cifrado RC4	15%
A2	Expansión de clave en AES	10%
A3	Adición en Curvas Elípticas	10%
A4	Entendiendo SSL/TLS	15%
A5	Ruptura de contraseñas	15%
A6	Listas de control de accesos	10%
A7	Prueba de Conocimientos	25%

En el Campus Virtual, cuando accedas a la asignatura, podrás ver en detalle los enunciados de las actividades que tendrás que realizar, así como el procedimiento y la fecha de entrega 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**. Una vez superada esta fecha, 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.

MODALIDAD PRESENCIAL

7.1. Convocatoria ordinaria

Para superar la asignatura en convocatoria ordinaria deberás:

- Entregar la actividad 1 de M3.1.
- Obtener una nota mínima de 4 en las pruebas objetivas de M3.1 y M3.2 (actividades 2 y 3).
- Obtener al menos un 3 en las 2 prácticas (actividades 6 y 7)
- Obtener una media ponderada de todas las actividades igual o superior a 5.

7.2. Convocatoria extraordinaria

Para superar la asignatura convocatoria extraordinaria deberás entregar las actividades que indique el profesor (correspondientes a las partes no entregadas o suspensas ya sean las mismas actividades u otras equivalentes a éstas). La nota de cada actividad deberá ser igual o mayor que 3 y la de las pruebas objetivas igual o mayor que 4. La media ponderada de todas las actividades de evaluación deberá ser igual o mayor a 5.

MODALIDAD ONLINE

7.3. Convocatoria ordinaria

Para superar la asignatura en convocatoria ordinaria deberás:

- Obtener una nota media ponderada de todas las actividades que figuran en la tabla igual o superior a 5, y obtener en la prueba de conocimiento una calificación igual o superior a 5.

7.4. Convocatoria extraordinaria

- Para superar la asignatura convocatoria extraordinaria deberás entregar las actividades que indique el profesor, cuya nota media ponderada debe ser igual o superior a 5, y obtener en las pruebas de conocimiento una calificación igual o superior a 5.

8. CRONOGRAMA

NOVIEMBRE 2020						
L	M	X	J	V	S	D
						1

DICIEMBRE 2020						
L	M	X	J	V	S	D
	1	2	3	4	5	6

ENERO 2021						
L	M	X	J	V	S	D
				1	2	3

2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

FEBRERO 2021

L	M	X	J	V	S	D
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

MARZO 2021

L	M	X	J	V	S	D
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

ABRIL 2021

L	M	X	J	V	S	D
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

MAYO 2021

L	M	X	J	V	S	D
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

JUNIO 2021

L	M	X	J	V	S	D
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

JULIO 2021

L	M	X	J	V	S	D
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

SEPTIEMBRE 2021

L	M	X	J	V	S	D
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26

Periodo no lectivo
Entrega TFM
Defensa TFM
Festivos

Calendario sujeto a cambios en relación con las festividades: los días festivos serán fijados por el Estado y la Comunidad Autónoma correspondiente

MES	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10
Noviembre										
Diciembre										
Enero										
Febrero										
Marzo										
Abril										

Mayo										
Junio										
Julio										

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

MODALIDAD ONLINE

NOVIEMBRE 2020

L	M	X	J	V	S	D
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

DICIEMBRE 2020

L	M	X	J	V	S	D
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

ENERO 2021

L	M	X	J	V	S	D
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

FEBRERO 2021

L	M	X	J	V	S	D
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

MARZO 2021

L	M	X	J	V	S	D
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

ABRIL 2021

L	M	X	J	V	S	D
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

MAYO 2021

L	M	X	J	V	S	D
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

JUNIO 2021

L	M	X	J	V	S	D
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

JULIO 2021

L	M	X	J	V	S	D
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

SEPTIEMBRE 2021

L	M	X	J	V	S	D
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

OCTUBRE 2021

L	M	X	J	V	S	D
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

- Periodo no lectivo
- Entrega TFM
- Defensa TFM
- Festivos
- Examen

SEMESTRE	MES	M1	M2	M3	M4	M5	M6	M7	M8	M9.B	M10
1	Octubre										
	Noviembre										
	Diciembre										
	Enero										
	Febrero										
	Marzo										
2	Abril										
	Mayo										
	Junio										
	Julio										
	Agosto										
	Septiembre										

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

9. BIBLIOGRAFÍA

A continuación, se indica la bibliografía para cada Unidad de Aprendizaje.

Unidad de aprendizaje 1:

- 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.
- Pinardi, Raffaele et al (2013), Peak-Shaped-Based Steganographic Technique for MP3 Audio, Journal of Information Security Vol.4 No.1(2013).

Unidad de aprendizaje 2:

- Carrillo, S., Marín, N., Medina, J.M. (2005). Introducción a las bases de datos. El modelo relacional. Ediciones Paraninfo, S.A. (ISBN 978-8497323963.)
- 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.

Unidad de aprendizaje 3:

- 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.

Unidad de aprendizaje 4:

- 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.

Unidad de aprendizaje 5:

- Schneier, Bruce (2015) Applied Cryptography, USA: Wiley.
- Carrión, David; Fernández, Miguel Ángel; de Salvador, Luis (2008) La Factura Electrónica, España: Delta Publicaciones.

Unidad de aprendizaje 6:

- Gollmann, Dieter, (2003) Computer Security, USA: Wiley.
- CCN (2007) Sistemas de Identificación y Autenticación Electrónica, Guía de Seguridad de las TIC CCN-STIC-415, España: CCN.
- Kohl, J., Neuman, C., (1993) The Kerberos Network Authentication Service (V5), USA: RFC 1510.
- Haller, N., Metz, C., Nesser, P. (1998) A One-Time Password System, USA: Straw, M.
- CCN (2011) Evaluación de Parámetros de Rendimiento en Dispositivos Biométricos Guía de Seguridad de las TIC, CCN-STIC España: CCN.
- D. Hardt, E (2015) The OAuth 2.0 Authorization Framework draft-ietf-oauth-v2-31 USA: OAuth Working Group.
- Kelly, Michael (2002) Is Single Sign n a Security Risk? USA: GIAC Certification, SANS Institute.

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.