ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

615000355 - Seguridad De La Informacion

PLAN DE ESTUDIOS

61SI - Grado En Sistemas De Informacion

CURSO ACADÉMICO Y SEMESTRE

2022/23 - Segundo semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	615000355 - Seguridad de la Informacion
No de créditos	3 ECTS
Carácter	Obligatoria
Curso	Segundo curso
Semestre	Cuarto semestre
Período de impartición	Febrero-Junio
Idioma de impartición	Castellano
Titulación	61SI - Grado en Sistemas de Informacion
Centro responsable de la titulación	61 - Escuela Tecnica Superior De Ingenieria De Sistemas Informaticos
Curso académico	2022-23

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Maria Angeles Mahillo Garcia	1110	mariaangeles.mahillo@upm.es	Sin horario. Las tutorias serán publicadas al principio del 2º Semestre en función de los horarios de impartición de las clases

Jesus Sanchez Lopez	1117	jesus.sanchezl@upm.es	Sin horario. Las tutorías serán publicadas al principio del 2º Semestre en función de los horarios de impartición de las clases
Giannicola Scarpa (Coordinador/a)	4304	g.scarpa@upm.es	Sin horario. Las tutorías serán publicadas al principio del 2º Semestre en función de los horarios de impartición de las clases

* Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

3. Conocimientos previos recomendados

3.1. Asignaturas previas que se recomienda haber cursado

- Fundamentos De Seguridad

- Logica Y Matematica Discreta

- Algebra

3.2. Otros conocimientos previos recomendados para cursar la asignatura

El plan de estudios Grado en Sistemas de Informacion no tiene definidos otros conocimientos previos para esta asignatura.

4. Competencias y resultados de aprendizaje

4.1. Competencias

CC1 - Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente.

CT8 - Trabajo en equipo: Ser capaz de trabajar como miembro de un equipo interdisciplinar con la finalidad de contribuir a desarrollar proyectos con pragmatismo y sentido de la responsabilidad, asumiendo compromisos teniendo en cuenta los recursos disponibles.

4.2. Resultados del aprendizaje

RA184 - Conoce y aplica métodos y algoritmos matemáticos que se usarán en las implementaciones criptográficas.

RA418 - Conoce la firma digital DSA.

RA415 - Analiza y aplica el algoritmo RSA para el cifrado y el descifrado de datos.

RA419 - Conoce y analiza el funcionamiento de las funciones hash MD5, SHA-1 y SHA2, aplicando los algoritmos.

RA148 - Es capaz de trabajar como miembro de un equipo con la finalidad de contribuir a desarrollar proyectos con pragmatismo y sentido de la responsabilidad, asumiendo compromisos y teniendo en cuenta los recursos disponibles. Se desenvuelve de modo que logra generar confianza y credibilidad en un grupo de colaboradores, además del compromiso para el logro de la visión corporativa a través de negociaciones y motivaciones, y no de manera coercitiva e individualista.

RA251 - Conoce y aplica los esquemas de protección de la información basados en la aplicación de técnicas criptográficas asimétrica (RSA y D-H)

RA257 - Conoce y calcula los NNC y las CP en el uso del algoritmo de cifrado RSA y realiza diferentes ataques al sistema.

RA252 - Compara los sistemas de cifra simétrica con los de cifra asimétrica y es capaz de aplicar los algoritmos adecuados a cada situación.

RA255 - Conoce formas y mecanismos de autenticación así como la utilidad de los certificados digitales.

RA254 - Analiza y aplica el algoritmo RSA para la firma digital.

RA78 - Desarrolla sistemas de gestión de la seguridad de la información SGSI, de acuerdo a estándares y normas internacionales.

RA77 - Conoce y aplica los esquemas de protección de la información basados en la aplicación de técnicas criptográficas.

RA470 - Conoce la definición de Curvas Elípticas y sus aplicaciones en criptografía.

5. Descripción de la asignatura y temario

5.1. Descripción de la asignatura

En esta asignatura se estudia la protección de la información utilizando técnicas de criptografía asimétrica, firma digital y certificados digitales. Tambien introduce en las fases e implantación de un Sistema de Gestión de la Seguridad de la Información.

5.2. Temario de la asignatura

1. Criptografía Asimétrica o de clave pública.
    1.1. Introducción
    1.2. Ventajas y desventajas de la cifra asimétrica frente a la simétrica
    1.3. Intercambio de clave de Diffie y Hellman.
    1.4. Algoritmo Extendido de Euclides para el cálculo de inversos
    1.5. Algoritmo de Exponenciación Rápida para la cifra
2. Principios del algoritmo RSA
    2.1. Principios
    2.2. Parámetros y generación de claves
    2.3. Cifrado y descifrado
    2.4. El cifrado por bloques de texto
3. Características de las claves y de los elementos de cifra en RSA
    3.1. Claves privadas parejas
    3.2. Claves públicas parejas

3.3. Números no cifrables

4. Ataques al RSA

4.1. Ataque basado en la factorización del módulo n

4.2. Ataque por cifrado cíclico con la clave pública

4.3. Ataque basado en la paradoja del cumpleaños

4.4. Ataques por canal lateral

5. Curvas Elípticas

5.1. Definición de curvas elípticas continuas y discretas

5.2. Criptografía basada en curvas elípticas

5.3. Intercambio de clave de Diffie y Hellman con curvas elípticas

6. Funciones hash

6.1. Características y propiedades de las funciones hash.

6.2. Funciones hash MD5, SHA-1 y familia SHA-2

6.3. Introducción a SHA-3

6.4. Ataque por paradoja del cumpleaños

7. Algoritmos de firma digital

7.1. Firma digital RSA

7.2. Firma estándar DSA

8. Sistemas de autenticación y certificados digitales

8.1. Mecanismos y formas de autenticación

8.2. Introducción a los certificados digitales

8.3. Concepto de Autoridad de Certificación

8.4. Algoritmos y características de un certificado digital X.509

9. Sistema de Gestión de la Seguridad de la Información

9.1. Introducción a políticas y planes de seguridad.

9.2. Implantación de un SGSI.

9.3. Fases de un SGSI.

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Tele-enseñanza	Actividades de evaluación
1	**Clase de teoría** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
2	**Clase de teoría** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
3		**Clase de prácticas** Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		**Evaluación Progresiva del Bloque I del temario.** EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 00:30
4	**Clase de teoría** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
5	**Clase de teoría** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
6		**Clase de prácticas** Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		**Evaluación Progresiva del Bloque II del temario.** EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 00:30
7	**Clase de teoría** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
8	**Clase de teoría** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
9		**Clase de prácticas** Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		**Evaluación Progresiva del Bloque III del temario.** EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 00:30
10	**Clase de teoría** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
11	**Clase de teoría** Duración: 02:00 LM: Actividad del tipo Lección Magistral			

12		**Clase de prácticas** Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio		**Evaluación Progresiva del Bloque IV del temario.** EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 00:30
13	**Clase de teoría** Duración: 02:00 LM: Actividad del tipo Lección Magistral			**Actividades de la competencia Transversal** TG: Técnica del tipo Trabajo en Grupo Evaluación continua y sólo prueba final No presencial Duración: 00:00
14	**Clase de teoría** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
15		**Clase de prácticas** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
16				
17				**Evaluación Progresiva del Bloque V del temario.** EX: Técnica del tipo Examen Escrito Evaluación continua y sólo prueba final Presencial Duración: 00:30 **Examen de Recuperación del Bloque I del temario.** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Presencial Duración: 00:30 **Examen de Recuperación del Bloque II del temario.** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Presencial Duración: 00:30 **Examen de Recuperación del Bloque III del temario.** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Presencial Duración: 00:30 **Examen de Recuperación del Bloque IV del temario.** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Presencial Duración: 00:30

Para el cálculo de los valores totales, se estima que por cada crédito ECTS el alumno dedicará dependiendo del plan de estudios, entre 26 y 27 horas de trabajo presencial y no presencial.

* El cronograma sigue una planificación teórica de la asignatura y puede sufrir modificaciones durante el curso

derivadas de la situación creada por la COVID-19.

7. Actividades y criterios de evaluación

7.1. Actividades de evaluación de la asignatura

7.1.1. Evaluación continua

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
3	Evaluación Progresiva del Bloque I del temario.	EX: Técnica del tipo Examen Escrito	Presencial	00:30	18%	4 / 10	CC1
6	Evaluación Progresiva del Bloque II del temario.	EX: Técnica del tipo Examen Escrito	Presencial	00:30	18%	4 / 10	CC1
9	Evaluación Progresiva del Bloque III del temario.	EX: Técnica del tipo Examen Escrito	Presencial	00:30	18%	4 / 10	CC1
12	Evaluación Progresiva del Bloque IV del temario.	EX: Técnica del tipo Examen Escrito	Presencial	00:30	18%	4 / 10	CC1
13	Actividades de la competencia Transversal	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:00	10%	0 / 10	CT8
17	Evaluación Progresiva del Bloque V del temario.	EX: Técnica del tipo Examen Escrito	Presencial	00:30	18%	0 / 10	CC1

7.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
13	Actividades de la competencia Transversal	TG: Técnica del tipo Trabajo en Grupo	No Presencial	00:00	10%	0 / 10	CT8

17	Evaluación Progresiva del Bloque V del temario.	EX: Técnica del tipo Examen Escrito	Presencial	00:30	18%	0 / 10	CC1
17	Examen de Recuperación del Bloque I del temario.	EX: Técnica del tipo Examen Escrito	Presencial	00:30	18%	0 / 10	CC1
17	Examen de Recuperación del Bloque II del temario.	EX: Técnica del tipo Examen Escrito	Presencial	00:30	18%	0 / 10	CC1
17	Examen de Recuperación del Bloque III del temario.	EX: Técnica del tipo Examen Escrito	Presencial	00:30	18%	0 / 10	CC1
17	Examen de Recuperación del Bloque IV del temario.	EX: Técnica del tipo Examen Escrito	Presencial	00:30	18%	0 / 10	CC1

7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Examen "Sólo prueba final" de todo el contenido de la asignatura	EX: Técnica del tipo Examen Escrito	Presencial	02:30	90%	0 / 10	

7.2. Criterios de evaluación

1. SISTEMA DE EVALUACIÓN

De acuerdo con la normativa reguladora de evaluación del aprendizaje en las titulaciones oficiales de grado y máster universitario de la universidad politécnica de Madrid, aprobada por Consejo de Gobiermo en su sesión del 26 de mayo de 2022, el sistema de evaluación que contribuye a favorecer el aprendizaje del estudiante y el logro de los resultados de aprendizaje y la adquisición de las competencias correspondientes es el sistema de evaluación distribuida o progresiva.

La asignatura tiene seis partes diferenciadas:

- Competencia Transversal. Actividad de participación obligatoria de los estudiantes que no puede recuperarse.
- Bloques temáticos I - V. Actividad de evaluación de los estudiantes que puede recuperarse (se evalúa en el periodo de docencia).

No obstante en determinadas circunstancias, que se indican en los apartados siguientes, el alumnado podrá recuperar parte de la asignatura (Bloques temáticos I - V) co el sistema global.

2. CRITERIOS DE CALIFICACIÓN.

2.1. CONVOCATORIA ORDINARIA.

2.1.1 EVALUACIÓN DISTRIBUIDA O PROGRESIVA.

Los instrumentos que se van a utilizar en la evaluación del proceso de aprendizaje del alumnado en la evaluación progresiva se detallan a continuación:

Técnica evaluativa: TG: Técnica del tipo Trabajo de Grupo (Competencia Transversal. Actividad obligatoria para el alumnado en tiempo y forma. No recuperable)

Descripción: Realización de actividades relacionadas con la competencia "Trabajo en equipo" .

Peso: 10%

Fecha: Semana 13 del periodo de docencia

Resultados de aprendizaje evaluados: Es capaz de trabajar como miembro de un equipo con la finalidad de contribuir a desarrollar proyectos con pragmatismo y sentido de la responsabilidad, asumiendo compromisos y teniendo en cuenta los recursos disponibles. Se desenvuelve de modo que logra generar confianza y credibilidad en un grupo de colaboradores, además del compromiso para el logro de la visión corporativa a través de negociaciones y motivaciones, y no de manera coercitiva e individualista.

Técnica evaluativa: EX: Técnica del tipo Examen Escrito

Descripción: Examen Bloque temático I. (Liberado si la nota es >= 4)

Peso: 18%

Fecha: Semana 3.

Resultados de aprendizaje evaluados: Compara los sistemas de cifra simétrica con los de cifra asimétrica y es capaz de aplicar los algoritmos adecuados a cada situación. Conoce y aplica los esquemas de protección de la información basados en la aplicación de técnicas criptográficas. Conoce y aplica métodos y algoritmos matemáticos que se usarán en las implementaciones criptográficas.

Temas que pertenecen al Bloque I: Tema 1

Técnica evaluativa: EX: Técnica del tipo Examen Escrito
Descripción: Examen Bloque temático II. (Liberado si la nota es >= 4)
Peso: 18%
Fecha: Semana 6.
Resultados de aprendizaje evaluados: Analiza y aplica el algoritmo RSA para el cifrado y el descifrado de datos. Conoce y calcula los NNC y las CP en el uso del algoritmo de cifrado RSA.
Temas que pertenecen al Bloque II: Temas 2 y 3

Técnica evaluativa: EX: Técnica del tipo Examen Escrito
Descripción: Examen Bloque temático III. (Liberado si la nota es >= 4)
Peso: 18%
Fecha: Semana 9.
Resultados de aprendizaje evaluados: Conoce y realiza diferentes ataques al sistema RSA. Conoce la definición de Curvas Elípticas y sus aplicaciones en criptografía.
Temas que pertenecen al Bloque III: Temas 4 y 5

Técnica evaluativa: EX: Técnica del tipo Examen Escrito
Descripción: Examen Bloque temático IV. (Liberado si la nota es >= 4)
Peso: 18%
Fecha: Semana 12.
Resultados de aprendizaje evaluados: Analiza y aplica el algoritmo RSA para la firma digital. Conoce la firma digital DSA. Conoce y analiza el funcionamiento de las funciones hash MD5 y SHA-1, aplicando los algoritmos. Conoce formas y mecanismos de autenticación así como la utilidad de los certificados digitales.
Temas que pertenecen al Bloque IV: Temas 6, 7 y 8

Técnica evaluativa: EX: Técnica del tipo Examen Escrito
Descripción: Examen Bloque temático V.
Peso: 18%
Fecha: Fecha indicada por la Subdirección de Ordenación Académica y de Postgrado. (Semana 17.)
Resultados de aprendizaje evaluados: Desarrolla sistemas de gestión de la seguridad de la información SGSI, de acuerdo a estándares y normas internacionales.
Temas que pertenecen al Bloque V: Tema 9.

Para superar la asignatura se necesita obtener una nota igual o superior a 5 una vez evaluadas las actividades anteriores. Para superar la competencia transversal deberán realizarse todas las actividades propuestas para la misma y obtener una calificación APTO. La calificación numérica a sumar a la nota de la asignatura vendrá dada

por la evaluación de una o varias de las actividades propuestas.

2.1.2. EVALUACIÓN GLOBAL

Los alumnos que no hayan obtenido una calificación superior a 4 en la evaluación de algunos de los bloques temáticos I a IV, tendrán la posibilidad de examinarse de la misma materia mediante un examen escrito, además de tener que examinarse del Bloque V. A la nota del examen se le sumará la nota obtenida en la evaluación de la competencia transversal.

Técnica evaluativa: TG: Técnica del tipo Trabajo de Grupo (Competencia Transversal. Actividad obligatoria para el alumnado en tiempo y forma. No recuperable)
Descripción: Realización de actividades relacionadas con la competencia "Trabajo en equipo" .
Peso: 10%
Fecha: Semana 13 del periodo de docencia
Resultados de aprendizaje evaluados: Es capaz de trabajar como miembro de un equipo con la finalidad de contribuir a desarrollar proyectos con pragmatismo y sentido de la responsabilidad, asumiendo compromisos y teniendo en cuenta los recursos disponibles. Se desenvuelve de modo que logra generar confianza y credibilidad en un grupo de colaboradores, además del compromiso para el logro de la visión corporativa a través de negociaciones y motivaciones, y no de manera coercitiva e individualista.

Técnica evaluativa: EX: Técnica del tipo Examen Escrito
Descripción: Examen Bloque Temático I. (Recuperación)
Peso: 18%
Fecha: Fecha indicada por la Subdirección de Ordenación Académica y de Postgrado.
Resultados de aprendizaje evaluados: Compara los sistemas de cifra simétrica con los de cifra asimétrica y es capaz de aplicar los algoritmos adecuados a cada situación. Conoce y aplica los esquemas de protección de la información basados en la aplicación de técnicas criptográficas. Conoce y aplica métodos y algoritmos matemáticos que se usarán en las implementaciones criptográficas.
Temas que pertenecen al Bloque I: Tema 1

Técnica evaluativa: EX: Técnica del tipo Examen Escrito
Descripción: Examen Bloque Temático II. (Recuperación)
Peso: 18%
Fecha: Fecha indicada por la Subdirección de Ordenación Académica y de Postgrado.
Resultados de aprendizaje evaluados: Analiza y aplica el algoritmo RSA para el cifrado y el descifrado de datos. Conoce y calcula los NNC y las CP en el uso del algoritmo de cifrado RSA.

Temas que pertenecen al Bloque II: Temas 2 y 3

Técnica evaluativa: EX: Técnica del tipo Examen Escrito
Descripción: Examen Bloque temático III. (Recuperación)
Peso: 18%
Fecha: Fecha indicada por la Subdirección de Ordenación Académica y de Postgrado.
Resultados de aprendizaje evaluados: Conoce y realiza diferentes ataques al sistema RSA. Conoce la definición de Curvas Elípticas y sus aplicaciones en criptografía.
Temas que pertenecen al Bloque III: Temas 4 y 5

Técnica evaluativa: EX: Técnica del tipo Examen Escrito
Descripción: Examen Bloque temático IV. (Recuperación)
Peso: 18%
Fecha: Fecha indicada por la Subdirección de Ordenación Académica y de Postgrado.
Resultados de aprendizaje evaluados: Analiza y aplica el algoritmo RSA para la firma digital. Conoce la firma digital DSA. Conoce y analiza el funcionamiento de las funciones hash MD5 y SHA-1, aplicando los algoritmos. Conoce formas y mecanismos de autenticación así como la utilidad de los certificados digitales.
Temas que pertenecen al Bloque IV: Temas 6, 7 y 8

Técnica evaluativa: EX: Técnica del tipo Examen Escrito
Descripción: Examen Bloque temático V.
Peso: 18%
Fecha: Fecha indicada por la Subdirección de Ordenación Académica y de Postgrado.
Resultados de aprendizaje evaluados: Desarrolla sistemas de gestión de la seguridad de la información SGSI, de acuerdo a estándares y normas internacionales.
Temas que pertenecen al Bloque V: Tema 9.

Para superar la asignatura se necesita obtener una nota igual o superior a 5 una vez evaluadas las actividades anteriores.

2.2. CONVOCATORIA EXTRAORDINARIA.

Todos los alumnos que no hayan superado la asignatura en la convocatoria ordinaria tendrán la posibilidad de presentarse a un examen escrito final sobre 9 puntos. A la nota del examen se le sumará la nota obtenida en la evaluación de la competencia transversal en el periodo de docencia.

Técnica evaluativa: TG: Técnica del tipo Trabajo de Grupo (Competencia Transversal. Actividad obligatoria para el alumnado en tiempo y forma. No recuperable)
Descripción: Realización de actividades relacionadas con la competencia "Trabajo en equipo" .

Peso: 10%

Fecha: Semana 13 del periodo de docencia

Resultados de aprendizaje evaluados: Es capaz de trabajar como miembro de un equipo con la finalidad de contribuir a desarrollar proyectos con pragmatismo y sentido de la responsabilidad, asumiendo compromisos y teniendo en cuenta los recursos disponibles. Se desenvuelve de modo que logra generar confianza y credibilidad en un grupo de colaboradores, además del compromiso para el logro de la visión corporativa a través de negociaciones y motivaciones, y no de manera coercitiva e individualista.

Técnica evaluativa: EX: Técnica del tipo Examen Escrito

Descripción: Evaluación de los temas de 1 a 9

Peso: 90%

Fecha: Fecha proporcionada por Sub. Ord. Académica

Resultados de aprendizaje evaluados: Compara los sistemas de cifra simétrica con los de cifra asimétrica y es capaz de aplicar los algoritmos adecuados a cada situación. Conoce y aplica los esquemas de protección de la información basados en la aplicación de técnicas criptográficas. Conoce y aplica métodos y algoritmos matemáticos que se usarán en las implementaciones criptográficas. Analiza y aplica el algoritmo RSA para el cifrado y el descifrado de datos. Conoce y calcula los NNC y las CP en el uso del algoritmo de cifrado RSA. Conoce y realiza diferentes ataques al sistema RSA. Conoce la definición de Curvas Elípticas y sus aplicaciones en criptografía. Analiza y aplica el algoritmo RSA para la firma digital. Conoce la firma digital DSA. Conoce y analiza el funcionamiento de las funciones hash MD5 y SHA-1, aplicando los algoritmos. Conoce formas y mecanismos de autenticación así como la utilidad de los certificados digitales. Desarrolla sistemas de gestión de la seguridad de la información SGSI, de acuerdo a estándares y normas internacionales.

8. Recursos didácticos

8.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
Fundamentos de Seguridad Tomo II	Bibliografía	Autenticación, hash, cifra asimétrica, cuaderno de prácticas
Fundamentos de Seguridad Tomo I	Bibliografía	Seguridad de la Información. Criptografia Clásica, Criptografía Moderna: Cifrado Simétrico.

Seguridad de la Información. Redes, informática y sistemas de información. Areitio, Javier. Paraninfo, 2008	Bibliografía	Ampliación conocimientos
Criptografía Digital. Pastor, José; Sarasa, Miguel Angel. Colección Textos Docentes; Prensas Universitarias de Zaragoza	Bibliografía	Ampliación conocimientos
Cryptography and Network Security. Stallings, William. Pearson, 2020	Bibliografía	Ampliación conocimientos
Plataforma Moodle de GATE para la asignatura	Equipamiento	Plataforma Moodle de GATE para la asignatura
Software	Equipamiento	Software: software de laboratorio propio de libre distribución (http://www.criptored.upm.es/paginas/software.htm)
Sitios web	Recursos web	Todas aquellos sitios web oficiales que estén relacionados con la materia impartida: Red Temática Iberoamericana de Criptografía y Seguridad de la Información Inteco, Agencia de Protección de Datos, Normas UNE (NorWeb), etc.

9. Otra información

9.1. Otra información sobre la asignatura

Actuación ante comportamientos fraudulentos (Artículo 13)
Los exámenes se realizarán a nivel personal. Si se detecta copia en una prueba de evaluación, se calificará con la puntuación de cero al estudiante o estudiantes implicados (la norma se aplicará por igual tanto a los que copian como a los que se dejan copia, es responsabilidad del alumnado la protección de su propia información)en la calificación final de la convocatoria correspondiente a la celebración de la prueba (ordinaria o extraordinaria). Además, en función de la gravedad del caso, el Tribunal de la asignatura podrá acordar la realización de un examen especial y equivalente para evaluar los resultados de aprendizaje de la asignatura en la siguiente convocatoria oficial. Si la comprobación de fraude académico se produce durante el desarrollo de la prueba, ésta se podrá interrumpir inmediatamente para el/la estudiante o estudiantes implicados/as, debiendo el profesor o profesora comunicar el porqué de la interrupción. El Tribunal de la Asignatura podrá poner los hechos en conocimiento del Director/a del Departamento, y éste a su vez podrá elevarlos al Rector/a para que pudiera abrirse, en su caso, expediente disciplinario.

Publicación de las soluciones (Articulo 19. Punto 9)
En todas las pruebas de evaluación, salvo que el tipo de prueba no lo permita, la solución de las preguntas de la misma se hará pública dentro de los dos días hábiles siguientes a la finalización de la prueba por la totalidad del estudiantado que deben realizarla, en la plataforma Moodle de la asignatura debiendo permanecer publicada durante siete días hábiles o hasta la fecha prevista para la revisión.

Estudiantes que no puedan realizar una prueba de evaluación en la fecha prevista (Artículo 21)
Cuando un/a estudiante, con anterioridad a una prueba de evaluación sepa de una causa justificada que le impida asistir en la fecha programada a los de exámenes hecho público en su momento, o no pueda asistir a una prueba de evaluación programada de por una causa sobrevenida podrá solicitar ser examinado de dicha prueba en fecha distinta a la programada. Para ello deberá consultar el artículo 21 de la normativa reguladora de evaluación del aprendizaje en las titulaciones oficiales de grado y máster universitario de la universidad politécnica de Madrid, aprobada por Consejo de Gobierno en su sesión del 26 de mayo de 2022, para comprobar que la causa está justificada y presentar solicitud junto con la justificación:
- En el caso de tratarse de pruebas fuera del periodo oficial de exámenes, mediante correo electrónico dirigido al coordinador/a de la asignatura, quien propondrá, de acuerdo con el profesor o profesora responsable, una forma alternativa de evaluar los resultados de aprendizaje correspondientes a dicha prueba de evaluación.
- En el caso de tratarse de una prueba de evaluación del periodo oficial de exámenes de la convocatoria ordinaria o extraordinario que permita dejar constancia de la solicitud, mediante correo electrónico dirigido al Jefe/a de

Estudios, quién comunicará a la coordinación de la asignatura la posibilidad de realizar otra prueba de evaluación.

Adelanto de la convocatoria extraordinaria (Articulo 12.4)

Aunque es poco probable para esta asignatura, se recuerda que con carácter excepcional, un/a estudiante podrá solicitar adelantar a la convocatoria de enero la convocatoria extraordinaria de julio de las asignaturas de segundo semestre que tuviera pendientes, siempre y cuando cumpla los siguientes requisitos:

- Que el/la estudiante esté matriculado de todos los créditos pendientes para finalizar sus estudios.
- Que, para concluir sus estudios de grado, le queden como máximo dos asignaturas del 2º semestre, o una asignatura del 1er semestre y otra del 2º semestre (además del TFG o TFM en su caso, de no haberlo defendido aún), en las que haya estado matriculado al menos una vez en un curso académico anterior.