



UNIVERSIDAD
POLITÉCNICA
DE MADRID

PROCESO DE
COORDINACIÓN DE LAS
ENSEÑANZAS PR/CL/001



E.T.S. de Ingeniería de
Sistemas Informáticos

ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

615000244 - Seguridad De La Informacion

PLAN DE ESTUDIOS

61IW - Grado En Ingenieria Del Software

CURSO ACADÉMICO Y SEMESTRE

2020/21 - Segundo semestre

Índice

Guía de Aprendizaje

| | |
|--------------------------------------------------|----|
| 1. Datos descriptivos..... | 1 |
| 2. Profesorado..... | 1 |
| 3. Conocimientos previos recomendados..... | 2 |
| 4. Competencias y resultados de aprendizaje..... | 3 |
| 5. Descripción de la asignatura y temario..... | 4 |
| 6. Cronograma..... | 6 |
| 7. Actividades y criterios de evaluación..... | 9 |
| 8. Recursos didácticos..... | 13 |
| 9. Otra información..... | 14 |
| 10. Adendas..... | 15 |

1. Datos descriptivos

1.1. Datos de la asignatura

| | |
|--------------------------------------------|----------------------------------------------------------------------|
| Nombre de la asignatura | 615000244 - Seguridad de la Información |
| No de créditos | 3 ECTS |
| Carácter | Obligatoria |
| Curso | Segundo curso |
| Semestre | Cuarto semestre |
| Período de impartición | Febrero-Junio |
| Idioma de impartición | Castellano |
| Titulación | 61IW - Grado en Ingeniería del Software |
| Centro responsable de la titulación | 61 - Escuela Técnica Superior De Ingeniería De Sistemas Informáticos |
| Curso académico | 2020-21 |

2. Profesorado

2.1. Profesorado implicado en la docencia

| Nombre | Despacho | Correo electrónico | Horario de tutorías * |
|-------------------------------------------------|----------|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Maria Angeles Mahillo Garcia (Coordinador/a) | 1110 | mariaangeles.mahillo@upm. es | L - 09:00 - 15:00 Las tutorías 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 |
| Jorge Ramio Aguirre | 1106 | jorge.ramio@upm.es | L - 09:00 - 15:00 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
- Algebra
- Logica Y Matematica Discreta

3.2. Otros conocimientos previos recomendados para cursar la asignatura

- Criptografía simétrica

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

RA336 - Analiza y aplica el algoritmo ElGamal para la firma digital

RA86 - Desarrolla sistemas de gestión de la seguridad de la información SGSI, de acuerdo a estándares y normas internacionales

RA334 - Analiza y aplica el algoritmo RSA para el cifrado y el descifrado de datos.

RA337 - Conoce la firma digital DSA

RA200 - Conoce formas y mecanismos de autenticación así como la utilidad de los certificados digitales

RA198 - Analiza y aplica el algoritmo RSA para la firma digital.

RA199 - Conoce y calcula los NNC y las CP en el uso del algoritmo de cifrado RSA y realiza diferentes ataques al sistema.

RA143 - Conoce y aplica métodos y algoritmos matemáticos que se usarán en las implementaciones criptográficas.

RA118 - 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.

RA197 - Compara los sistemas de cifra simétrica con los de cifra asimétrica y es capaz de aplicar los algoritmos adecuados a cada situación

RA85 - Conoce y aplica los esquemas de protección de la información basados en la aplicación de técnicas criptográficas

RA344 - Conoce y analiza el funcionamiento de las funciones hash MD5, SHA-1 y SHA-2, aplicando los algoritmos..

RA335 - Analiza y aplica el algoritmo ElGamal para el cifrado y el descifrado de datos

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. También 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. Algoritmo de Elgamal
 - 5.1. Principios
 - 5.2. Parámetros y generación de claves
 - 5.3. Cifrado y descifrado
 - 5.4. El cifrado por bloques de texto
- 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 digital Elgamal
 - 7.3. 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 | | Resolución de ejercicios con software de la asignatura o problemas relacionados con el contenido de la asignatura Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio | Clase de teoría: Impartición de contenidos Duración: 01:00 LM: Actividad del tipo Lección Magistral | |
| 2 | | Resolución de ejercicios con software de la asignatura o problemas relacionados con el contenido de la asignatura Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio | Clase de teoría: Impartición de contenidos Duración: 01:00 LM: Actividad del tipo Lección Magistral | |
| 3 | | Resolución de ejercicios con software de la asignatura o problemas relacionados con el contenido de la asignatura Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio | Clase de teoría: Impartición de contenidos Duración: 01:00 LM: Actividad del tipo Lección Magistral | |
| 4 | | Resolución de ejercicios con software de la asignatura o problemas relacionados con el contenido de la asignatura Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio | Clase de teoría: Impartición de contenidos Duración: 01:00 LM: Actividad del tipo Lección Magistral | |
| 5 | | Resolución de ejercicios con software de la asignatura o problemas relacionados con el contenido de la asignatura Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio | Clase de teoría: Impartición de contenidos Duración: 01:00 LM: Actividad del tipo Lección Magistral | |
| 6 | | Resolución de ejercicios con software de la asignatura o problemas relacionados con el contenido de la asignatura Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio | Clase de teoría: Impartición de contenidos Duración: 01:00 LM: Actividad del tipo Lección Magistral | |
| 7 | | Resolución de ejercicios con software de la asignatura o problemas relacionados con el contenido de la asignatura Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio | Clase de teoría: Impartición de contenidos Duración: 01:00 LM: Actividad del tipo Lección Magistral | |

| | | | | |
|----|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8 | | Resolución de ejercicios con software de la asignatura o problemas relacionados con el contenido de la asignatura Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio | Clase de teoría: Impartición de contenidos Duración: 01:00 LM: Actividad del tipo Lección Magistral | |
| 9 | | Resolución de ejercicios con software de la asignatura o problemas relacionados con el contenido de la asignatura Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio | Clase de teoría: Impartición de contenidos Duración: 01:00 LM: Actividad del tipo Lección Magistral | |
| 10 | | Resolución de ejercicios con software de la asignatura o problemas relacionados con el contenido de la asignatura Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio | Clase de teoría: Impartición de contenidos Duración: 01:00 LM: Actividad del tipo Lección Magistral | |
| 11 | | Resolución de ejercicios con software de la asignatura o problemas relacionados con el contenido de la asignatura Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio | Clase de teoría: Impartición de contenidos Duración: 01:00 LM: Actividad del tipo Lección Magistral | Examen Tema 1, 2, 3, 4 (Ev. Continua) EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 02:00 |
| 12 | | Resolución de ejercicios con software de la asignatura o problemas relacionados con el contenido de la asignatura Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio | Clase de teoría: Impartición de contenidos Duración: 01:00 LM: Actividad del tipo Lección Magistral | |
| 13 | | Resolución de ejercicios con software de la asignatura o problemas relacionados con el contenido de la asignatura Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio | Clase de teoría: Impartición de contenidos Duración: 01:00 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 | | Resolución de ejercicios con software de la asignatura o problemas relacionados con el contenido de la asignatura Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio | Clase de teoría: Impartición de contenidos Duración: 01:00 LM: Actividad del tipo Lección Magistral | |
| 15 | | Resolución de ejercicios con software de la asignatura o problemas relacionados con el contenido de la asignatura Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio | Clase de teoría: Impartición de contenidos Duración: 01:00 LM: Actividad del tipo Lección Magistral | |
| 16 | | | | |
| 17 | | | | Examen Tema 5, 6, 7, 8, 9 (Ev. Continua) EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 02:00 Examen "Sólo prueba final" de todo el contenido de la asignatura EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Presencial Duración: 02:30 |

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 |
|------|-------------------------------------------|---------------------------------------|---------------|----------|-----------------|-------------|------------------------|
| 11 | Examen Tema 1, 2, 3, 4 (Ev. Continua) | EX: Técnica del tipo Examen Escrito | Presencial | 02:00 | 50% | 0 / 10 | CC1 |
| 13 | Actividades de la competencia Transversal | TG: Técnica del tipo Trabajo en Grupo | No Presencial | 00:00 | 10% | 0 / 10 | CT8 |
| 17 | Examen Tema 5, 6, 7, 8, 9 (Ev. Continua) | EX: Técnica del tipo Examen Escrito | Presencial | 02:00 | 40% | 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 | Examen "Sólo prueba final" de todo el contenido de la asignatura | EX: Técnica del tipo Examen Escrito | Presencial | 02:30 | 90% | 0 / 10 | CC1 |

7.1.3. Evaluación convocatoria extraordinaria

| Descripción | Modalidad | Tipo | Duración | Peso en la nota | Nota mínima | Competencias evaluadas |
|-------------|-----------|------|----------|-----------------|-------------|------------------------|
|-------------|-----------|------|----------|-----------------|-------------|------------------------|

| | | | | | | |
|----------------------------------------------------------------------------|-------------------------------------|------------|-------|-----|--------|-----|
| Examen "Convocatoria Extraordinaria" de todo el contenido de la asignatura | EX: Técnica del tipo Examen Escrito | Presencial | 02:30 | 90% | 0 / 10 | CC1 |
|----------------------------------------------------------------------------|-------------------------------------|------------|-------|-----|--------|-----|

7.2. Criterios de evaluación

1. ELECCIÓN DEL SISTEMA DE EVALUACIÓN

De acuerdo con la normativa reguladora de los sistemas de evaluación en los procesos formativos vinculados a los títulos de grado y máster universitario con planes de estudio adaptados al R.D. 1393/2007. *"En la convocatoria ordinaria de cada asignatura, la elección entre el sistema de evaluación continua o el sistema de evaluación mediante una prueba final corresponde al estudiante. El sistema de evaluación continua será el que se aplique en general a todos los estudiantes de cada asignatura. El estudiante que desee seguir el sistema de evaluación mediante sólo una prueba final, deberá comunicarlo por escrito al coordinador de la asignatura o, por delegación de este, a los profesores de la misma mediante el procedimiento, y en el plazo, que se fijen en la Guía de Aprendizaje de la asignatura o, si la Guía de Aprendizaje no lo fijase, según lo que determine la Jefatura de Estudios del Centro responsable de la titulación. En todo caso, el plazo que se fije para que el estudiante pueda realizar esta opción deberá ser, al menos, de dos semanas a contar desde el inicio de la actividad docente de la asignatura para dicho estudiante."*

El alumno que desee seguir el sistema de evaluación mediante sólo prueba final, deberá comunicarlo respondiendo a la consulta que la asignatura formulará en la plataforma Moodle de la misma. Fecha tope la indicada en el cronograma facilitado a los alumnos al inicio del curso. La competencia transversal se evaluará durante la impartición de las clases independientemente de la modalidad de evaluación elegida, la calificación se sumará a las obtenidas en la evaluación de las demás actividades.

Modalidad: TG: Técnica del tipo Trabajo en Grupo (Competencia Transversal)

Actividades: Las indicadas al inicio de la impartición de la asignatura

Resultados de aprendizaje: 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.

2. CRITERIOS DE CALIFICACIÓN.

2.1. CONVOCATORIA ORDINARIA.

2.1.1 EVALUACIÓN CONTINUA.

Los instrumentos que se van a utilizar en la evaluación de proceso de aprendizaje de los alumnos en evaluación continua se detallan a continuación

Modalidad: EX: Técnica del tipo Examen Escrito. Temas 1, 2, 3, 4

Resultados de aprendizaje: 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.

Modalidad: EX: Técnica del tipo Examen Escrito. Temas 5, 6, 7, 8, 9

Resultados de aprendizaje: Analiza y aplica el algoritmo Elgamal para el cifrado y el descifrado de datos. Analiza y aplica el algoritmo Elgamal para la firma digital. 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.

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

2.1.2. EVALUACIÓN "SÓLO EXAMEN FINAL".

Los alumnos que hayan decidido no seguir la evaluación continua, tendrán la posibilidad de presentarse a un examen escrito final sobre 9,0. En el mismo se evaluará tanto los contenidos teóricos como las actividades prácticas realizadas durante el curso. La nota numérica obtenida en la evaluación de la competencia transversal

se sumará a la obtenida en el examen de la convocatoria ordinaria.

Modalidad: EX: Técnica del tipo Examen Escrito. Todos los temas

Resultados de aprendizaje: 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. Analiza y aplica el algoritmo Elgamal para el cifrado y el descifrado de datos. Analiza y aplica el algoritmo Elgamal para la firma digital. 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.

Para superar la asignatura se necesita obtener una nota igual o superior a 5 una vez evaluadas la actividad anterior y la competencia transversal.

2.2. CONVOCATORIA EXTRAORDINARIA.

De acuerdo con la normativa reguladora de los sistemas de evaluación en los procesos formativos vinculados a los títulos de grado y máster universitario con planes de estudio adaptados al R.D. 1393/2007, todos los alumnos que no hayan superado la asignatura en la convocatoria ordinaria tendrán la posibilidad de presentarse a un examen escrito final sobre 9.0 puntos. En el mismo se evaluará tanto los contenidos teóricos como las actividades prácticas realizadas durante el curso. La nota numérica obtenida en la evaluación de la competencia transversal se sumará a la obtenida en el examen de la convocatoria extraordinaria.

Modalidad: EX: Técnica del tipo Examen Escrito. Todos los temas

Resultados de aprendizaje: 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.. Analiza y aplica el algoritmo Elgamal para el cifrado y el descifrado de datos. Analiza y aplica el algoritmo Elgamal para la firma digital. 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.

Para superar la asignatura se necesita obtener una nota igual o superior a 5 una vez evaluadas la actividad anterior y la competencia transversal.

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. Criptografía 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 |
| 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 | Todos 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. |

| | | |
|-----------------------------------|-------|---------------------------------------------------------------------------|
| Transparencia utilizadas en clase | Otros | Conjunto de transparencias utilizadas por los profesores de la asignatura |
|-----------------------------------|-------|---------------------------------------------------------------------------|

9. Otra información

9.1. Otra información sobre la asignatura

Ante la **suspensión de toda actividad educativa presencial** el procedimiento excepcional de:

1. Impartición de clases presenciales: La actividad presencial será sustituida por, la subida a la plataforma de un guión detallado y ejercicios para que los alumnos puedan seguir con el estudio de la asignatura siguiendo las pautas:

- Se informa semanalmente vía Moodle qué diapositivas de las entregadas y publicadas aquí en la plataforma Moodle habrá que leer, y que los profesores habríamos presentado y analizado en aula.
- Además, se indica -si fuera el caso- qué otro tipo de lectura es recomendable para fortalecer los conocimientos que aparecen en dichas diapositivas. Lo mismo podemos decir respecto a la consulta de material de apoyo multimedia y actividades prácticas que se recomiendan hacer sobre la temática en cuestión.
- Por último, se entrega el enunciado de uno o más ejercicios para que sean realizado por los estudiantes. Quien tenga dudas sobre su resolución, deberá hacerlas llegar a los profesores vía este foro de la asignatura, es decir, en el foro "Preguntas relacionadas con el seguimiento del curso".

Independientemente de las consultas recibidas y de sus respectivas respuestas, bien sobre ejercicios, prácticas o sobre el temario, los profesores de la asignatura subirán a Moodle a en semana siguiente la solución de ese o esos trabajos. Además se establecerán tutorías grupales con videoconferencia en los horarios de clases presenciales.

2. Evaluación del alumnado: Si las circunstancias sanitarias no permiten la realización presencial de exámenes dichas pruebas serán reemplazadas por exámenes en formato telemático con el mismo contenido y peso.

10. Adendas

- - El examen Tema 1, 2, 3, 4 (Ev. Continua) de la Semana 11 será No Presencial.