Este documento es una adenda a la guía docente de la asignatura para incluir los cambios derivados de la **situación excepcional de docencia no presencial** que se aplica desde el 13 de marzo de 2020 a causa de la crisis sanitaria COVID-19

ADENDA a la Guía docente de la asignatura

Asignatura	SEGURIDAD Y CRIPTOGRAFÍA		
Materia	INGENIERÍA DE SISTEMAS TELEMÁTICOS		
Módulo	BLOQUE DE ITINERARIOS TECNOLÓGICOS EN TIC (BI)		
Titulación	MÁSTER UNIVERSITARIO DE INVESTIGACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES		
Plan	624	**Código**	54630
Periodo de impartición	2º CUATRIMESTRE	**Tipo/Carácter**	OPTATIVA
Nivel/Ciclo	MÁSTER	**Curso**	1º
Créditos ECTS	5 ECTS		
Lengua en que se imparte	CASTELLANO INGLÉS (materiales de lectura y charlas complementarias)		
Profesor/es responsable/s	JUAN CARLOS GARCÍA ESCARTÍN		
Datos de contacto (E-mail, teléfono…)	E-mail: juagar@tel.uva.es		
Horario de tutorías	Véase www.uva.es → Centros → Campus de Valladolid → Escuela Técnica Superior de Ingenieros de Telecomunicación → Tutorías		
Departamento	TEORÍA DE LA SEÑAL Y COMUNICACIONES E INGENIERÍA TELEMÁTICA		

5. Bloques temáticos

El nuevo programa debe incluir **un ajuste de contenidos que permita la adquisición de competencias necesaria en base al ritmo de docencia mantenido usando el Campus Virtual. También es necesario modificar el método formativo y la evaluación,** considerando, además de las 5 semanas presenciales, el resto de la docencia no presencial.

Si la asignatura se organiza en dos o más bloques temáticos, se puede hacer individualmente para todos ellos o juntarlo en esta adenda en un único bloque. Si algún bloque temático estaba finalizado el 12 de marzo, no habrá que incluirlo en esta adenda.

5. Bloques temáticos

Bloque 1: SEGURIDAD Y CRIPTOGRAFÍA

Carga de trabajo en créditos ECTS: 5

a. Contextualización y justificación

La asignatura consta de un único bloque con 12 temas cortos en los que se introducen de forma eminentemente práctica los principios de los sistemas de criptografía simétrica y asimétrica, firma digital, tecnología *blockchain*, generadores de números aleatorios...

Estos conocimientos serán fundamentales para el desarrollo de aplicaciones seguras y se complementarán con charlas invitadas de expertos en el tema.

b. Objetivos de aprendizaje

1. Conocer las primitivas básicas disponibles en sistemas de seguridad.
2. Comprender las ventajas e inconvenientes de diferentes sistemas de cifrado.
3. Comprender la importancia de seguir las prácticas recomendables en la implementación de sistemas de seguridad.
4. Conocer las herramientas matemáticas básicas detrás de los sistemas de cifrado y seguridad más habitual.
5. Conocer los programas informáticos utilizados en tareas de ciberseguridad.
6. Ser capaz de evaluar la aleatoriedad de una secuencia binaria.
7. Conocer los protocolos de divulgación responsable de vulnerabilidades y problemas de seguridad.
8. Ser capaz de presentar de forma clara resultados de investigación.
9. Ser capaz de analizar la seguridad de un sistema informático.
10. Ser capaz de evaluar críticamente los resultados de investigación, los artículos y exposiciones de otros.

c. Contenidos ADAPTADOS

Los contenidos se estructurarán en 12 temas de 3 a 5 horas con una introducción teórica y cerca de dos tercios de ejemplos prácticos.

TEMAS 1 A 3: DOCENCIA PRESENCIAL SEGÚN LA GUÍA.

TEMARIO ADAPTADO:

4. Aplicaciones de las funciones hash (II): Blockchain. Bitcoin (I).

Uso de funciones hash en cuadernos públicos. Blockchain: fundamentos generales. Ejemplos prácticos con Bitcoin.

5. Criptografía simétrica: Cifrado por bloques. Modos de operación. DES. AES.

Criptografía simétrica: fundamentos. Modos de funcionamiento ECB y CBC. Ejemplos prácticos con DES y AES.

6. Aplicaciones de la criptografía simétrica: Generación de PIN en tarjetas de crédito. SUPRIMIDO

Ejemplos prácticos de aplicación.

7. Criptografía asimétrica: RSA y curvas elípticas. Distribución de claves. Infraestructura de clave pública. Certificados.

Fundamentos de Teoría de Números. El sistema RSA. Curvas elípticas. Aplicaciones en distribución de claves. PKI. Cadenas de confianza y certificados.

8. Aplicaciones de criptografía asimétrica (I): Firma electrónica. Ejemplo práctico: Sony PS3.

Ejemplo práctico del uso de firma electrónica y problemas asociados.

9. Aplicaciones de criptografía asimétrica (II): Criptomonedas. Bitcoin (II). SUPRIMIDO.

10. Generación de números aleatorios.

Números aleatorios y pseudoaleatorios. Aplicaciones. Generación de números aleatorios con uso criptográfico. Tests de aleatoriedad.

11. Aplicaciones de generación de números aleatorios. Recolección de entropía. Ejemplo práctico: Debian.

Ejemplos prácticos de generación de números aleatorios y problemas asociados.

12. Conferencias y temas avanzados en seguridad y criptografía. SUPRIMIDO

d. Métodos docentes

Primeros temas: docencia presencial.

Docencia a distancia: Modelo de aula invertida. Se seguirá principalmente el libro: N. Ferguson, B. Schneier y T. Kohno, ***Cryptography Engineering Design Principles and Practical Applications***, (John Wiley & Sons, 2010) o referencias que se proporcionarán mediante el Campus Virtual. Se asignará una lectura a lo alumnos para los créditos de trabajo en casa y se resolverán problemas de tipo práctico durante el horario de clase coordinando las explicaciones mediante el Campus Virtual.

e. Plan de trabajo

Ver Sección 6.

f. Evaluación

Los alumnos serán evaluados de forma continua mediante trabajos. Se suprime la obligación de realizar un examen para aspirar a las notas más altas (sobresaliente y matrícula de honor).

g. Bibliografía básica

- A. J. Menezes, S. A. Vanstone y P. C. van Oorschot, ***Handbook of Applied Cryptography***, 1st ed. (CRC Press, Inc., Boca Raton, FL, USA, 1996).
- D. M. Burton, ***Elementary Number Theory***, 6th ed. (McGraw-Hill Higher Education, 2005).
- N. Ferguson, B. Schneier y T. Kohno, ***Cryptography Engineering Design Principles and Practical Applications***, (John Wiley & Sons, 2010).
- J. Katz e Y. Lindell, ***Introduction to Modern Cryptography: Principles and Protocols***, (Chapman & Hall/CRC Cryptography and Network Security Series 2007).

h. Bibliografía complementaria

Artículos proporcionados por el profesor.

i. Recursos necesarios

1. Acceso al Campus Virtual.
2. Acceso a un ordenador personal con herramientas de programación.

7. Sistema de calificaciones – Tabla resumen

Este apartado será obligatorio incluirlo para la mayoría de los casos. Se trata de aclarar cómo va a obtenerse la "nota final" de la asignatura en este contexto extraordinario de docencia no presencial. A continuación, se muestra un ejemplo

7. Tabla resumen de los instrumentos, procedimientos y sistemas de evaluación/calificación

INSTRUMENTO/PROCEDIMIENTO	PESO EN LA NOTA FINAL	OBSERVACIONES
Evaluación continua: Entrega de trabajos, exposición en clase, trabajos de programación...	100%	Ejercicios guiados. Plazo de entrega final: el de la convocatoria oficial del examen.

Tanto en la convocatoria ordinaria como en la extraordinaria la fecha final de entrega de todos los ejercicios es la del examen final. Se podrán volver a realizar los ejercicios no superados.