Guía Docente: Seguridad de la Información y Criptografía Aplicada

DATOS GENERALES	
Facultad	Facultad de Ciencias y Tecnología
Titulación	Máster en Ciberseguridad
Plan de estudios	2018
Materia	Ciberseguridad y sistemas
Carácter	Obligatorio
Período de impartición	Primer Trimestre
Curso	Primero
Nivel/Ciclo	Máster
Créditos ECTS	6
Lengua en la que se imparte	Castellano
Prerrequisitos	No se prevén requisitos previos, por tanto los requisitos serán los propios del título.

DATOS DEL PROFESORADO			
Profesor Responsable	Cristina Romero Tris	**Correo electrónico**	cristina.romero.tris@ui1.es
Área		**Facultad**	Facultad de Ciencias y Tecnología
Perfil Profesional 2.0	LinKedin		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA	
Asignaturas de la materia	• Seguridad de la Información y Criptografía Aplicada
Contexto y sentido de la asignatura en la titulación y perfil profesional	Esta asignatura forma parte de las asignaturas obligatorias del primer trimestre del Máster en Ciberseguridad. En esta asignatura se estudian técnicas criptográficas avanzadas que constituyen un pilar fundamental para entender cómo funciona la seguridad informática en la actualidad. Durante la asignatura, se describirán brevemente los conceptos de seguridad de la información y criptografía básicos, ya que el objetivo es profundizar en conceptos más avanzados y complejos sobre criptografía. En las primeras unidades se hará un repaso de las bases matemáticas y los principales sistemas de criptografía. A continuación, se estudiarán temas más complejos, como las curvas elípticas y la criptografía cuántica.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE	
Competencias de la asignatura	• CB6: Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación. • CG4: Conocer la normativa técnica y disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad. • CE02: Conocer las tendencias actuales en técnicas de ciberataque • CE09: Analizar e identificar las vulnerabilidades de un sistema informático, y ser capaz de desarrollar métodos de protección de la información. • CE12: Comprender y saber aplicar técnicas criptográ?cas avanzadas.
Resultados de aprendizaje de la asignatura	• Adquirir las competencias básicas y generales detalladas anteriormente. • Distinguir entre los diferentes modelos criptográficos y aplicarlos correctamente en función del contexto. • Capacidad de realización de juicios críticos sobre sistemas criptográficos actuales. • Conocer y aplicar técnicas criptográficas avanzadas para la confidencialidad y privacidad del intercambio de datos

PROGRAMACION DE CONTENIDOS	

Breve descripción de la asignatura	En esta asignatura se verá, entre otros:
	
	• Técnicas criptográficas:
	  ◦ Aplicaciones de la criptografía.
	  ◦ Control de integridad de mensajes.
	• La criptografía en el mundo real:
	  ◦ Criptografía (privacidad, integridad, autenticidad, no repudio).
	  ◦ Comercio electrónico.
	• Certificados y firma electrónica:
	  ◦ Certificados digitales.
	  ◦ Entidades de certificación.
	  ◦ Normativa vigente.

	• Técnicas criptográficas avanzadas: ◦ Criptografía cuántica. ◦ Criptografía basada en identidad.
Contenidos	Unidad didáctica 1: Elementos matemáticos de la criptografía - Primalidad - Aritmética modular - Cuerpos finitos Unidad didáctica 2: Bases de la criptografía - Criptosistemas de clave privada - Criptosistemas de clave pública Unidad didáctica 3: Protocolos criptográficos - Firma y certificado digital - Infraestructura de clave pública - Criptografía distribuida y compartición de secretos - Pruebas de conocimiento nulo Unidad didáctica 4: Criptografía de curvas elípticas - Geometría de las curvas elípticas - Relación entre curvas elípticas y cuerpos finitos - Protocolos criptográficos basados en curvas elípticas Unidad didáctica 5: Introducción a los Pairings - Bases matemáticas para la definición de Pairings - Qué son los pairings - Intercambio de claves a tres partes - Criptografía basada en la identidad Unidad didáctica 6: Criptografía cuántica - Conceptos básicos - Intercambio de claves - Protocolo BB84

METODOLOGÍA	
Actividades formativas	El alumno dispondrá de un espacio dentro del aula virtual, organizado en seis unidades didácticas. Cada unidad didáctica contendrá un apartado de "Contenidos" sobre la temática de la asignatura. Además, un foro de dudas y dos actividades evaluables. Respecto a las actividades evaluables, cada unidad didáctica contará con dos de ellas. Una de ellas siempre será un cuestionario de autoevaluación, y la otra podra variar entre un foro de debate, un estudio de caso, un laboratorio práctico o un trabajo colaborativo. A continuación se describen los tipos de actividades que pueden aparecer. • **Laboratorios criptográficos:** En las unidades didácticas de carácter más práctico, se planteará la realización de unas actividades y problemas con algún tema de interés propio de la unidad. Se trata de que el alumnado utilice los recursos necesarios para investigar y conocer determinados aspectos relacionados con los contenidos tratados en cada unidad didáctica. • **Cuestionarios de autoevaluación**: El alumnado podrá valorar la comprensión de los contenidos mediante la realización de tests de autoevaluación con actividades de refuerzo y aprendizaje. • **Foros de debate:** Son espacios donde el alumnado debatirá y aportará ideas sobre aspectos concretos de la asignatura. Se plantearán foros en dos unidades didácticas, tratando de fomentar el trabajo en equipo para la exploración de conceptos y procedimientos asociados. Todos los alumnos son invitados a proponer los nuevos foros de debate que consideren oportuno sobre temas relacionados con la asignatura, aunque estos no tendran carácter evaluable. • **Trabajo colaborativo:** Se trata de una actividad por grupos en la que cada grupo tendrá que realizar una tarea organizándose y colaborando. La comunicación entre ellos será a través de un foro en el aula virtual. • **Estudio de caso**: Es una actividad de investigación online. Está relacionada con el tema estudiado en la unidad didáctica, pero no es necesario el análisis de la misma previamente a la realización de la actividad. El alumno deberá usar fuentes de información (por ejemplo, internet) para realizar el estudio de caso.

EVALUACIÓN	
Sistema evaluativo	*En caso de que la situación sanitaria impida la realización presencial de los exámenes con todas las garantías, la Universidad Isabel I celebrará dichas pruebas en modalidad online. Para la realización de dichos exámenes, la universidad incorporará la herramienta de proctoring a nuestra plataforma tecnopedagógica, con el objetivo de garantizar los procesos de autentificación del alumno, como el control del entorno durante el desarrollo de las pruebas de evaluación. A su vez, la Universidad Isabel I pondrá a disposición del alumnado una Unidad de Exámenes Online específica para ofrecer apoyo técnico durante todo el proceso y así solventar todas las incidencias que se puedan presentar.* El sistema de evaluación se basará en una selección de las pruebas de evaluación más adecuadas para el tipo de competencias que se trabajen. El sistema de calificaciones estará acorde con la legislación vigente *(Real Decreto 1125/2003, de 5 de septiembre, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y de validez en todo el territorio nacional)*. El sistema de evaluación de la Universidad Isabel I queda configurado de la siguiente

manera:

Sistema de evaluación convocatoria ordinaria

Opción 1. Evaluación continua

Los estudiantes que opten por esta vía de evaluación deberán realizar el **seguimiento de la evaluación continua (EC)** y podrán obtener hasta un **60 %** de la calificación final a través de las actividades que se plantean en la evaluación continua.

Además, deberán realizar un **examen final presencial (EX)** que supondrá el **40 %** restante. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del trabajo realizado durante la evaluación continua y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura.

Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de evaluación continua.

Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de evaluación continua, siempre y cuando al aplicar los porcentajes correspondientes se alcance una calificación mínima de un 5.

Opción 2. Prueba de evaluación de competencias

Los estudiantes que opten por esta vía de evaluación deberán realizar una **prueba de evaluación de competencias (PEC)** y un **examen final presencial (EX)**.

La **PEC** se propone como una prueba que el docente plantea con el objetivo de evaluar en qué medida el estudiante adquiere las competencias definidas en su asignatura. Dicha prueba podrá ser de diversa tipología, ajustándose a las características de la asignatura y garantizando la evaluación de los resultados de aprendizaje definidos. Esta prueba supone el 50 % de la calificación final.

El **examen final presencial**, supondrá el **50 %** de la calificación final. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del seguimiento de las actividades formativas desarrolladas en el aula virtual y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura.

Al igual que con el sistema de evaluación anterior, para la aplicación de los porcentajes correspondientes el estudiante debe haber obtenido una puntuación mínima de un 4 en cada una de las partes de las que consta la opción de prueba de evaluación de competencias.

Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de la prueba de evaluación de competencias siempre y cuando al aplicar los porcentajes correspondientes se alcance una calificación mínima de un 5.

Sistema de evaluación convocatoria extraordinaria

Todos los estudiantes, independientemente de la opción seleccionada, que no superen las pruebas evaluativas en la convocatoria ordinaria tendrán derecho a una convocatoria extraordinaria.

La convocatoria extraordinaria completa consistirá en la realización de una **prueba de evaluación de competencias** que supondrá el **50 %** de la calificación final y un **examen**

	final presencial cuya calificación será el **50 %** de la calificación final. Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de evaluación de la convocatoria extraordinaria. Los estudiantes que hayan suspendido todas las pruebas evaluativas en convocatoria ordinaria (evaluación continua o prueba de evaluación de competencias y examen final) o no se hayan presentado deberán realizar la convocatoria extraordinaria completa, como se recoge en el párrafo anterior. En caso de que hayan alcanzado una puntuación mínima de un 4 en alguna de las pruebas evaluativas de la convocatoria ordinaria (evaluación continua o prueba de evaluación de competencias y examen final), se considerará su calificación para la convocatoria extraordinaria, debiendo el estudiante presentarse a la prueba que no haya alcanzado dicha puntuación o que no haya realizado. En el caso de que el alumno obtenga una puntuación que oscile entre el 4 y el 4,9 en las dos partes de que se compone la convocatoria ordinaria (EC o PEC y examen), solo se considerará para la convocatoria extraordinaria la nota obtenida en la evaluación continua o prueba de evaluación de competencias ordinaria (en función del sistema de evaluación elegido), debiendo el alumno realizar el examen extraordinario para poder superar la asignatura. Al igual que en la convocatoria ordinaria, se entenderá que el alumno ha superado la materia en convocatoria extraordinaria si, aplicando los porcentajes correspondientes, se alcanza una calificación mínima de un 5.

BIBLIOGRAFÍA Y OTROS RECURSOS	
Bibliografía básica	Fuster Sabater, A. Hernández Encinas, L. Montoya Vitini, F. y Muñoz Masque, J. (2012). *Criptografia, proteccion de datos y aplicaciones*. Ra-Ma Editorial Este libro, escrito en castellano, permite adentrarse y profundizar en el mundo de la criptografía, descubriendo conceptos nuevos y de actualidad. Es una guía precisa y rigurosa para estar al tanto de técnicas, procedimientos e innovaciones que afectan a la seguridad de nuestras comunicaciones. Se incluye, así mismo, un amplio espectro de aplicaciones de uso cotidiano con las que, consciente o inconscientemente, realizamos a diario actividades criptográficas. Ruohonen, K. (2010). *Mathematical Cryptology*. Tampere University of Technology Este libro, escrito en inglés, da un repaso a todos los conceptos relacionados con seguridad de la información y criptografía. Contiene información muy detallada sobre todas las temáticas tratadas en el sector, desde algoritmos de clave pública, a funciones de hash y conceptos avanzados de matemáticas.
Bibliografía complementaria	Areitio, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información.* Editorial Paraninfo Martínez Rodríguez, H y Borges Trenard, M.A. (2012). *Curvas Elipticas En La Criptografia*. EAE Editorial Academia Espanola

	Muñoz Muñoz, A. y Ramió Aguirre, J. (2014). *Cifrado de las comunicaciones digitales. De la cifra clásica al algoritmo RSA.* Ed. OxWord Van Tilborg, H. (1999). *Fundamentals of Cryptology: A Professional Reference and Interactive Henk C. A*. Springer Nash, A. Duane, W. Joseph, C. y Brink, D, (2002). *PKI. Infraestructura de claves públicas.* McGraw Hill Wobst, R. (2007). *Cryptology Unlocked.* John Wiley & Sons
Otros recursos	Resumen histórico sobre los hitos de la criptografía http://world.std.com/~cme/html/timeline.html Web de la agencia del departamento de comercio de EEUU del Instituto Nacional de Estándares y Tecnología http://www.nist.gov/itl/ y de la división de seguridad informática http://csrc.nist.gov/groups/STM/ Artículo original del algoritmo RSA https://people.csail.mit.edu/rivest/Rsapaper.pdf Web para generar el par de claves (pública y privada) de cifrado https://gnupg.org/ Información sobre criptografía cuántica https://uwaterloo.ca/institute-for-quantum-computing/research/areas-research/quantum-cryptography Centro Criptológico Nacional donde indica el nivel de alerta de ciberataques https://www.ccn-cert.cni.es/ Instituto Nacional de Seguridad de España https://www.incibe.es/ Revista de interés sobre criptografía a nivel internacional http://www.insaonline.org/