CRIPTOGRAFÍA APLICADA Y SEGURIDAD DE LA INFORMACIÓN

1.- Datos de la Asignatura					
Código	306641	Plan	M205	ECTS	3
Carácter	Obligatorio	Curso	1	Periodicidad	Primer semestre
Idioma de impartición asignatura		Español			
Área	LENGUAJJES Y SISTEMAS INFORMÁTICOS				
Departamento	INFORMÁTICA Y AUTOMÁTICA				
Plataforma virtual	Indique “Studium” y/u otras si fuera preciso				

1.1.- Datos del profesorado*			
Profesor Coordinador	Ángel Luis Sánchez Lázaro	Grupo / s	1
Departamento	INFORMÁTICA Y AUTOMÁTICA		
Área	LENGUAJJES Y SISTEMAS INFORMÁTICOS		
Centro	Facultad de Ciencias		
Despacho	D1515		
Horario de tutorías	Consultar https://diaweb.usal.es, o STUDIUM		
URL Web	*https://produccioncientifica.usal.es/investigadores/56146/detalle*		
E-mail	alsl@usal.es	Teléfono	Ext 6097

1.1.- Datos del profesorado*			
Profesor Coordinador	Santiago Suárez Suárez	Grupo / s	
Departamento			
Área			
Centro			
Despacho			
Horario de tutorías			
URL Web			
E-mail	sarez@policia.es	Teléfono	690705695

1.1.- Datos del profesorado*			
Profesor	Santiago González González	Grupo / s	
Departamento			
Área			
Centro			
Despacho			
Horario de tutorías			

URL Web			
E-mail	ggonzalez7zrv@policia.es	Teléfono	620433951

2.- Recomendaciones previas

No existen

3.- Objetivos de la asignatura

Conocer los fundamentos de la criptografía clásica y moderna y su aplicación en la protección de datos y comunicaciones.
Conocer algoritmos de cifrado tanto simétrico como asimétrico y su uso para confidencialidad y autenticación por firma digitales
Conocer la gestión de claves e infraestructuras de seguridad.
Conocer el uso de criptografía en blockchain y los protocolos seguros de red y almacenamiento.
Conocer los ataques a sistemas criptográficos y medidas de protección.
Conocer los conceptos y tendencias actuales “Harvest now and decryp later”
Conocer el Impacto disruptivo de la computación cuántica en las tecnologías de la información, tecnologías de la operación y en la identidad digital.
 Acciones comunes en TI-TO e identidad digital
 Plan de acción de la Policía Nacional (operativo-táctico-estratégico)
 Servicio de Infraestructuras Criptográficas Avanzadas (S.I.C.A.) de la Policía Nacional
 Hoja de ruta hacia una transición postcuántica garantista
 PKI´s desplegadas con tecnología postcuántica y certificados generados en curva elíptica
 Criptoactivos, ¿Qué son?, donde se encuentran que implican.
 Descubrimiento, informes de monitorización y gestión para una estrategia PQC eficiente y efectiva

Resultados de aprendizaje *Complete esta columna si su titulación ha sido adaptada al RD822/2021*

3.1: Conocimientos:
C03: Distinguir, describir y explicar los fundamentos y aplicaciones del cifrado simétrico, asimétrico y los principales protocolos criptográficos

3.2: Habilidades:
H03-HC03: Identificar y analizar fuentes de información relevantes para la seguridad y la actuación policial en ciberamenazas.
H04-HC04: Analizar e identificar infracciones y patrones de ciberdelincuencia y ciberataques en el marco de la legislación penal y administrativa.
H10-HP06: Aplicar herramientas de inteligencia artificial en la prevención e investigación de ciberdelitos.
H11-HP07: Aplicar métodos y técnicas en la investigación de la cibercriminalidad.

3.3: Competencias:
K05: Analizar continuamente la situación sociopolítica en el ámbito competencial de la Policía Nacional en materia de ciberinteligencia, ciberseguridad y ciberdelincuencia, con el fin de detectar cambios presentes o futuros y fomentar el aprendizaje autorregulado y autónomo.
K06: Promover la formación en ciberinteligencia, ciberseguridad y ciberdelincuencia dentro de la Policía Nacional mediante los medios disponibles.

5.- Contenidos (temario)

- Fundamentos de criptografía
- Algoritmos de cifrado y firmas Digitales

- Infraestructuras de seguridad y gestión de claves
- Criptografía en blockchain y seguridad de redes
- Ataques a sistemas criptográficos y medidas de protección
- Tema 5. Definiciones contexto y primeras aproximaciones de la criptografía postcuántica.
- ¿Qué es la criptografía postcuántica? ¿Estamos preparados?
- Riesgos y ventajas
- Situación global ante el tránsito de la criptografía clásica a la computación cuántica.
- Algoritmos cuánticos relevantes Algoritmo de Shor (Impacto en RSA, ECC, DSA)
- Algoritmo de Grover (Impacto en cifrados simétricos y hashes)
- Conceptos y tendencias de "Harvest now and decryp later"
- Estándares de postcuántica FIPS 203, FIPS 204 y FIPS 205
- Teorema Michael Mosca
- Acciones comunes en TI-TO e identidad digital
- Plan de acción de la Policía Nacional (operativo-táctico-estratégico)
- Servicio de Infraestructuras Criptográficas Avanzadas (S.I.C.A.) de la Policía Nacional
- Hoja de ruta hacia una transición postcuántica garantista
- PKI´s desplegadas con tecnología postcuántica y certificados generados en curva elíptica
- Criptoactivos, ¿Qué son?, donde se encuentran que implican.
- Descubrimiento, informes de monitorización y gestión para una estrategia PQC eficiente y efectiva

6.- Metodologías docentes

Dado el carácter de la titulación según la memoria, la modalidad de impartición es virtual.
Clases teóricas: sesiones con actividades en las que el profesor expone los contenidos fundamentales.
Clases prácticas: actividades encaminadas a la resolución de problemas, casos y situaciones relacionadas con lo presentado de forma teórica.
Foros: se plantearán temas relacionados con aspectos de la materia para su debate por los estudiantes. Los debates estarán moderados por el profesorado. Se desarrollarán en la plataforma virtual de forma asíncrona.

6.1.- Distribución de metodologías docentes

		Horas dirigidas por el profesor		Horas de trabajo autónomo	HORAS TOTALES
		Horas presenciales.	Horas no presenciales.		
Sesiones magistrales					
Prácticas	- En aula (virtual)	24		32	56
	- En el laboratorio				
	- En aula de informática				
	- De campo				
	- Otras (detallar)				
Seminarios					
Exposiciones y debates					
Tutorías					
Actividades de seguimiento online					
Preparación de trabajos				17	17
Otras actividades (detallar)					
Exámenes		2			2
TOTAL		**26**		**49**	**75**

7.- Recursos, bibliografía, referencias electrónicas o de otro tipo

Teoría
Cryptography and Network Security: principles and practice (2022)
Computer security: principles and practice (2018)

Problemas, práctica
Openssl: https://www.openssl.org
GnuPG: https://www.gnupg.org/

Consultar la plataforma de formación para otros recursos

8.- Evaluación

8.1: Criterios de evaluación:
Los instrumentos de evaluación que podrán ser aplicados durante la evaluación continua y sumativa podrán ser los siguientes:
La participación activa en clases.
Resolución de problemas o casos prácticos, individual o en grupo, con exposición y/o defensa oral, en su caso.
Pruebas orales o escritas individuales.

8.2: Sistemas de evaluación:
Participación activa (10% de la calificación final).
Trabajos individuales (40 % de la calificación final)
Pruebas escritas u orales individuales (50% de la calificación final)

8.3: Consideraciones generales y recomendaciones para la evaluación y la recuperación:
Recomendaciones para la recuperación.-

Para la recuperación, se recomienda detectar y analizar los errores cometidos y subsanarlos con la utilización de los materiales y recursos facilitados.

La segunda oportunidad en convocatoria ordinaria (recuperación) consistirá en una prueba de opción múltiple y/o de desarrollo de preguntas cortas, la cual será debidamente comunicada en el campus virtual *Studium* por parte del profesor/a coordinador de la asignatura.

Revisiones de la calificación ante el profesor y Recurso ante la Comisión de Docencia de la Facultad.

Se atenderá a lo establecido en los artículos 18 y 19 del Reglamento de Evaluación de la Universidad de Salamanca aprobado en sesión del Consejo de Gobierno de 19 de diciembre de 2008 y modificado en sesiones de 30 de octubre de 2009, de 28 de mayo de 2015, 27 de mayo de 2021 y 27 de marzo de 2025, sin perjuicio de la comunicación del día, lugar y hora de revisión de calificaciones que establezca el profesor/a de la asignatura.

9.- Organización docente semanal

*Se impartirá a lo largo de 3 semanas, empezando el día 2 de junio. Cada semana se impartirán 8 horas de videoconferencia, en concreto los **martes y jueves** en horario de 17:00 a 21:00 horas por la plataforma de videoconferencias de la USAL. Las sesiones se grabarán para ver en diferido exclusivamente desde la plataforma de formación on-line de la Universidad de Salamanca (https://studium.usal.es).*