Planificación de las enseñanzas

4.1 Estructura básica de las enseñanzas

Tipos de materia		Nº créditos ECTS
Ob	**Obligatorias**	51
Op	**Optativas**	0
PE	**Prácticas Externas**	0
TFM	**Trabajo Fin de Máster (obligatorio en Máster)**	9
	Créditos totales	60

4.2 Organización temporal de las asignaturas

PRIMER CURSO

PRIMER CUATRIMESTRE			
Asignatura	**Tipo**	**ECTS**	**Curso**
Capacidades de los sistemas SIEM	Obligatoria(OB)	3	Primero
Herramientas para el Hacking Ético	Obligatoria(OB)	3	Primero
Introducción a la ciencia forense	Obligatoria(OB)	3	Primero
Introducción a sistemas SIEM	Obligatoria(OB)	3	Primero
Introducción al Hacking Ético	Obligatoria(OB)	3	Primero
Introducción y conceptos básicos	Obligatoria(OB)	3	Primero
La evidencia telemática, técnicas y herramientas	Obligatoria(OB)	3	Primero
Seguridad aplicada a las distintas plataformas móviles e IoT	Obligatoria(OB)	3	Primero
Seguridad y vulnerabilidades	Obligatoria(OB)	3	Primero
Tipos de análisis forense	Obligatoria(OB)	3	Primero
Total ECTS		**30**	

SEGUNDO CUATRIMESTRE			
Asignatura	**Tipo**	**ECTS**	**Curso**
Casos de uso de Blockchain	Obligatoria(OB)	3	Primero
Derecho y seguridad informática	Obligatoria(OB)	3	Primero
Especificaciones de los principales lenguajes	Obligatoria(OB)	3	Primero
Programación segura, vulnerabilidades	Obligatoria(OB)	3	Primero
Régimen jurídico en Internet	Obligatoria(OB)	3	Primero
Smart Contracts	Obligatoria(OB)	3	Primero
Tecnología Blockchain	Obligatoria(OB)	3	Primero
Trabajo fin de máster	Trabajo Fin de Título (TFT)	9	Primero
Total ECTS		**30**	

ANUALES			
Asignatura	**Tipo**	**ECTS**	**Curso**
Total ECTS		**0**	

SEGUNDO CURSO

PRIMER CUATRIMESTRE			
Asignatura	**Tipo**	**ECTS**	**Curso**
Total ECTS		**0**	

SEGUNDO CUATRIMESTRE			
Asignatura	**Tipo**	**ECTS**	**Curso**
Total ECTS		**0**	

ANUALES			
Asignatura	**Tipo**	**ECTS**	**Curso**
Total ECTS		**0**	

TERCER CURSO

PRIMER CUATRIMESTRE			
Asignatura	**Tipo**	**ECTS**	**Curso**
Total ECTS		**0**	

SEGUNDO CUATRIMESTRE			
Asignatura	**Tipo**	**ECTS**	**Curso**
Total ECTS		**0**	

ANUALES			
Asignatura	**Tipo**	**ECTS**	**Curso**
Total ECTS		**0**	

4.3 Estructura en base a itinerarios formativos (si los hubiese)

4.4 Descripción detallada de las asignaturas

ASIGNATURAS PRIMER CURSO

Asignatura: Capacidades de los sistemas SIEM

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Primero

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 20 %
- **Virtual:** 80 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos
Javier José	Martín Limorti		Externo	3

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Habilidades o Destrezas (HD)	• Interpretar los logs del sistema • Gestión de alertas y tickets • Desarrollo de informes	
Competencias (COM)	Básicas / Generales / Transversales: CB6, CB7, CB8, CB9, CB10 y CG1 Específicas: CE1, CE5, CE6 y CE9	

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Pruebas prácticas		10
Evaluación continua, Participación híbrida		40
Pruebas objetivas de tipo test		40

Descripción de contenidos

* Introducción y ámbito de aplicación. * Logs y eventos * Correlación de eventos. * Arquitectura y desarrollo de Informes

Asignatura: Herramientas para el Hacking Ético

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Primero

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 20 %
- **Virtual:** 80 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos
Víctor	Flores Sánchez		Externo	3

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Competencias (COM)	Básicas / Generales / Transversales: CB6, CB7, CB8, CB9, CB10 y CG1 Específicas: CE1, CE5, CE6, CE8 y CE9	
Habilidades o Destrezas (HD)	• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente. • Conocer las herramientas y protocolos usados en el hacking • Saber discernir que metodología aplicar en función del contexto en el que se realice la auditoría.	

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Pruebas objetivas de tipo test		40
Evaluación continua, Participación híbrida	Continua	40
Pruebas prácticas		20

Descripción de contenidos

* Footprinting * Fingerprinting * Redes * Metaesploit

Asignatura: Introducción a la ciencia forense

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Primero

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 20 %
- **Virtual:** 80 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos
José Aurelio	García Mateos		Externo	2
Juan Manuel	Corchado Rodríguez		Interno	1

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Competencias (COM)	Básicas / Generales / Transversales: CB6, CB7, CB8, CB9, CB10 y CG1 Específicas: CE1, CE8, CE9 y CE10	
Habilidades o Destrezas (HD)	• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente. • Conocer las responsabilidades de la figura del perito informático y los escenarios de actuación de este tipo de profesionales. • Conocer y aplicar una metodología sistemática a la hora de realizar un peritaje informático en un escenario real.	

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Pruebas objetivas de tipo test		40
Evaluación continua, Participación híbrida	Continua	40
Pruebas prácticas		20

Descripción de contenidos

* Introducción, objetivos, aspectos relevantes y ámbitos relevantes *
La figura del perito informático, funciones y atribuciones * Perito informático de gestión y mediación tecnológica *
Metodologías de actuación.

Asignatura: Introducción a sistemas SIEM

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Primero

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 20 %
- **Virtual:** 80 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos
Pablo	Plaza Martínez		Externo	1
Juan Manuel	Corchado Rodríguez		Interno	2

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Competencias (COM)	Básicas / Generales / Transversales: CB6, CB7, CB8, CB9, CB10 y CG1 Específicas: CE1, CE5, CE6, CE8 y CE9	
Habilidades o Destrezas (HD)	• Adquisición de los conceptos generales de la gestión de incidentes • Arquitecturas frecuentes • Procedimiento de recolección de la información relacionada con incidentes de seguridad	

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Pruebas prácticas		20
Evaluación continua, Participación híbrida		40
Pruebas objetivas de tipo test		40

Descripción de contenidos

* Introducción * Evolución * Arquitecturas SIEM

Asignatura: Introducción al Hacking Ético

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Primero

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 20 %
- **Virtual:** 80 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos
Víctor	Flores Sánchez		Externo	3

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Competencias (COM)	Básicas / Generales / Transversales: CB6, CB7, CB8, CB9, CB10 y CG1 Específicas: CE1, CE5, CE6, CE8 y CE9	
Habilidades o Destrezas (HD)	• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente. • Conocer y saber aplicar las metodologías existentes para poder realizar auditorías de seguridad de forma sistemática. • Desarrollar auditorías de seguridad en entornos específicos a partir las directrices marcadas por una metodología.	

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Pruebas objetivas de tipo test		40
Pruebas prácticas		20
Evaluación continua, Participación híbrida	Continua	40

Descripción de contenidos

* Introducción, metodologías existentes * Tipos de amenazas(vulnerabilidades, riesgo, exposición o impacto). * Actuaciones (Evitarlos, Transferirlos, Reducirlos, Asumirlos) * Tipos de metodologías (Cuantitativas, Cualitativas). * Metodologías existentes

Asignatura: Introducción y conceptos básicos

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Primero

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 20 %
- **Virtual:** 80 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos
Javier José	Martín Limorti		Externo	2
Miguel	De Lucas Postigo		Externo	1

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Competencias (COM)	Básicas / Generales / Transversales: CB1, CB2, CB3, CB4, CB5 y CG1 Específicas: CE5 y CE6	
Habilidades o Destrezas (HD)	• Adquirir las competencias básicas, generales y específicas sobre la Ciberseguridad y la CiberInteligencia. • Adquisición de los principios generales sobre seguridad informática, y en especial, sobres seguridad en Internet, las redes de ordenadores y los nodos informáticos que la forman. • Distinguir entre los diferentes modelos criptográficos y aplicarlos correctamente en función del contexto.	

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Pruebas prácticas		20
Pruebas objetivas de tipo test		40
Evaluación continua, Participación híbrida	Continua	40

Descripción de contenidos

* Introducción, definición y objetivos de la Ciberseguridad. * La seguridad en cifras. * Aspectos relevantes de la seguridad. * Criptografía (Privacidad, Integridad, Autenticidad, No repudio). * Criptografía simétrica (AES) y Funciones Hash. * CiberInteligencia.

Asignatura: La evidencia telemática, técnicas y herramientas

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Primero

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 20 %
- **Virtual:** 80 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos
José Aurelio	García Mateos		Externo	3

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Competencias (COM)	Básicas / Generales / Transversales: CB6, CB7, CB8, CB9, CB10 y CG1 Específicas: CE1, CE8, CE9 y CE10	
Habilidades o Destrezas (HD)	• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente. • Conocer las principales herramientas de un perito informático, así como el entorno de trabajo, es decir el Laboratorio Informático Forense. • Utilizar las técnicas periciales adecuadamente para la extracción de evidencias que puedan ser pruebas utilizables en un contexto judicial.	

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Pruebas prácticas		20
Evaluación continua, Participación híbrida	Continua	40
Pruebas objetivas de tipo test		40

Descripción de contenidos

* La evidencia telemática * Preservación de la evidencia digital * Como recuperar datos perdidos * Pen-test, herramientas y programas forenses * Cibercrimen, ciberataques, ciberamas, ciberdefensas * Tecno vigilancia y las fuerzasde seguridad * Laboratorio informático forense.

Asignatura: Seguridad aplicada a las distintas plataformas móviles e IoT

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Primero

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 20 %
- **Virtual:** 80 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos
Manuel	López Pérez		Externo	1
Javier José	Martín Limorti		Externo	1
Pablo	Plaza Martínez		Externo	1

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Competencias (COM)	Básicas / Generales / Transversales: CB6, CB7, CB8, CB9, CB10 y CG1 Específicas: CE1, CE2, CE3 y CE6	
Habilidades o Destrezas (HD)	• Aplicación de la ciberseguridad en entornos móviles • Ciberseguridad en sistemas IoT • Ciberseguridad en sistemas IIoT	

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Pruebas objetivas de tipo test		40
Pruebas prácticas		20
Evaluación continua, Participación híbrida		40

Descripción de contenidos

* Seguridad en Sistemas Cloud e integración entre plataformas. * Seguridad en las distintas plataformas móviles. * La gestión de la ciberseguridad en dispositivos de IoT e IIoT.

Asignatura: Seguridad y vulnerabilidades

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Primero

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 20 %
- **Virtual:** 80 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos
Manuel	López Pérez		Externo	2
Juan Manuel	Corchado Rodríguez		Interno	1

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Competencias (COM)	Básicas / Generales / Transversales: CB6, CB7, CB8, CB9, CB10 y CG1 Específicas: CE1, CE5, CE6 y CE9	
Habilidades o Destrezas (HD)	• Adquirir de las competencias básicas, generales y específicas detalladas anteriormente. • Distinguir las diferentes vulnerabilidades • Conocer y saber utilizar las herramientas que permiten asegurar un sistema informático. • Analizar la seguridad física y lógica de cualquier infraestructura tecnológica	

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Pruebas objetivas de tipo test		40
Evaluación continua, Participación híbrida	Continua	40
Pruebas prácticas		20

Descripción de contenidos

* Vulnerabilidades * Seguridad física de los equipos * Ataques a credenciales * Seguridad de aplicaciones web

Asignatura: Tipos de análisis forense

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Primero

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 20 %
- **Virtual:** 80 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos
José Aurelio	García Mateos		Externo	2
Juan Manuel	Corchado Rodríguez		Interno	1

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Competencias (COM)	Básicas / Generales / Transversales: CB6, CB7, CB8, CB9, CB10 y CG1 Específicas: CE1, CE8, CE9 y CE10	
Habilidades o Destrezas (HD)	• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente. • Conocer los tipos de Análisis forense en función de sus naturaleza. • Redacción de la documentación correspondiente.	

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Evaluación continua, Participación híbrida		40
Pruebas objetivas de tipo test		40
Pruebas prácticas		20

Descripción de contenidos

* Análisis forense de la memoria RAM * Análisis forense en Sistemas Windows * Análisis forense en Sistemas GNU/Linux * Análisis forense en Navegadores y Correo electrónico * Redacción de un informe pericial * Tipos de informe.

Asignatura: Casos de uso de Blockchain

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Segundo

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 20 %
- **Virtual:** 80 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos
Pablo	Plaza Martínez		Externo	2
Manuel	López Pérez		Externo	1

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Habilidades o Destrezas (HD)	• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente. • Conocer los principios casos de uso de esta tecnologia	
Competencias (COM)	Básicas / Generales / Transversales: CB6, CB7, CB8, CB9 CB10 y CG1 Específicas: CE5, CE6, CE8 y CE9	

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Evaluación continua, Participación híbrida		40
Pruebas prácticas		20
Pruebas objetivas de tipo test		40

Descripción de contenidos

* Criptomonedas. * Bitcoin * Ethereum * Smart contracts

Asignatura: Derecho y seguridad informática

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Segundo

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 20 %
- **Virtual:** 80 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos
Federico	Bueno de Mata		Interno	2
Pablo	Mezquita Domínguez		Externo	1

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Competencias (COM)	Básicas / Generales / Transversales: CB6, CB7, CB8, CB9, CB10 y CG1 Específicas: CE5, CE9 y CE10	
Habilidades o Destrezas (HD)	• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente. • Conocer el marco jurídico aplicable a Internet y a la informática en general. • Saber evaluar si un sistema informático cumple con la legislación vigente. • Saber evaluar si las acciones que se llevan a cabo pueden constituir un delito informático.	

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Pruebas prácticas		20
Evaluación continua, Participación híbrida		40
Pruebas objetivas de tipo test		40

Descripción de contenidos

* Delitos informáticos, caracteres y consecuencias. * El acceso ilegal a datos reservados y sistemas de información. Hacking, intimidad y espionaje industrial * La alteración, destrucción o inutilización de datos. Virus, crackings, ataques DdS. * La posición jurídica
de los responsables y encargados de los tratamientos de ficheros de datos. *
Las estafas y fraudes informáticos. Phising y spoofing. *
Acceso no autorizado a determinados servicios informáticos. * La alusión de las medidas tecnológicas que protegen la propiedad intelectual. * La responsabilidad de los proveedores de servicios de la sociedad la información.

Asignatura: Especificaciones de los principales lenguajes

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Segundo

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 20 %
- **Virtual:** 80 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos
Carlos	Morales Diego		Externo	1
Manuel	López Pérez		Externo	2

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Competencias (COM)	Básicas / Generales / Transversales: CB6, CB7, CB8, CB9, CB10 y CG1 Específicas: CE1, CE2, CE3 y CE6	
Habilidades o Destrezas (HD)	• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente. • Conocer las posibles amenazas que puede sufrir el software desarrollado para un lenguaje de programación concreto. • Desarrollas buenas practicas a la hora del desarrollo software.	

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Evaluación continua, Participación híbrida		40
Pruebas objetivas de tipo test		40
Pruebas prácticas		20

Descripción de contenidos

* Vulnerabilidades y fallosde desarrollo en JAVA * Vulnerabilidades y fallosde desarrollo en PHP * Vulnerabilidades y fallosde desarrollo en .NET * Buenas prácticas en el desarrollo del software

Asignatura: Programación segura, vulnerabilidades

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Segundo

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 20 %
- **Virtual:** 80 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos
Carlos	Morales Diego		Externo	3

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Habilidades o Destrezas (HD)	• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente. • Aplicar un modelo de programación segura en el desarrollo de software de aplicación. • Conocer las vulnerabilidades en el desarrollo de software, desde el punto de vista del programa software, así como de las debilidades de las arquitecturas computacionales. • Capacitar para evaluar y emitir un juicio sobre el mismo las vulnerabilidades de un producto software previamente a desarrollar.	
Competencias (COM)	Básicas / Generales / Transversales: CB6, CB7, CB8, CB9, CB10 y CG1 Específicas: CE1, CE2, CE3 y CE6	

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Evaluación continua, Participación híbrida		40
Pruebas objetivas de tipo test		40
Pruebas prácticas		20

Descripción de contenidos

* Desbordamiento de buffer (estructura de memoria, pila de procesadores, desbordamiento de pila, creación de Shellcodes). * Herramientas (Pax, Stackguard, ProPolice, ASLR). * Otras tecnologías de protección (DEP,SEHOP). * EMET * Analizadores de código (Desbordamiento de memoria, variables, pila, herramientas existentes, etc.). * Condiciones de carrera(Condiciones en secuencias no atómicas, Bloqueode ficheros). * Criptografía Asimétricas (Fundamentos teóricos, cifrado, firma digital, aspectos importantes, algoritmos asimétricos, etc.). * Otras herramientas criptográficas (criptografía visual, dinero electrónico, certificado digital, infraestructura de claves públicas)

Asignatura: Régimen jurídico en Internet

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Segundo

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 20 %
- **Virtual:** 80 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos
Pablo	Mezquita Domínguez		Externo	3

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Competencias (COM)	Básicas / Generales / Transversales: CB6, CB7, CB8, CB9, CB10 y CG1 Específicas: CE5, CE9 y CE10	
Habilidades o Destrezas (HD)	• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente. • Conocer las diferentes leyes orgánicas del marco jurídico nacional aplicables en el contexto tecnológico. • Conocer las implicaciones legales que conlleva diferentes actividades en el marco de Internet, como por ejemplo la compraventa, o las transferencias electrónicas de fondos o datos.	

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Pruebas objetivas de tipo test		40
Evaluación continua, Participación híbrida		40
Pruebas prácticas		20

Descripción de contenidos

* Derecho, copia privada y tecnología anticopia * La responsabilidad de los PSSI por las actividades terceros en Internet. * Regulación jurídica de la compraventa realizada en Internet * Régimen jurídico de las transferencias electrónicas de fondos * Régimen jurídico de las transferencias electrónicas de datos.

Asignatura: Smart Contracts

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Segundo

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 20 %
- **Virtual:** 80 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos
Alfonso	González Briones		Interno	2
Manuel	López Pérez		Externo	1

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Competencias (COM)	Básicas / Generales / Transversales: CB6, CB7, CB8, CB9, CB10 y CG1 Específicas: CE5, CE6, CE8 y CE9	
Competencias (COM)	• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente. • Conocer los principios que rigen un Smart contracts • Conocer los principios un sistema descentralizado. • Aspectos legales de los Smart Contracts	

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Pruebas prácticas		20
Pruebas objetivas de tipo test		40
Evaluación continua, Participación híbrida		40

Descripción de contenidos

* Conocer los principios que rigen un Smart contracts * Conocer los principios un sistema descentralizado. * Aspectos legales de los Smart Contracts

Asignatura: Tecnología Blockchain

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Segundo

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 20 %
- **Virtual:** 80 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos
Alfonso	González Briones		Interno	3

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Competencias (COM)	Básicas / Generales / Transversales: CB6, CB7, CB8, CB9, CB10 y CG1 Específicas: CE5, CE6, CE8 y CE9	
Habilidades o Destrezas (HD)	• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente. • Conocer los principios básicos del Blockchain y las cadenas de bloques • Conocer las características de los algoritmos de consenso.	

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Evaluación continua, Participación híbrida		40
Pruebas prácticas		20
Pruebas objetivas de tipo test		40

Descripción de contenidos

* El concepto de Blockchain, aspectos relevantes. * Criptografia * Sistemas P2P

Asignatura: Trabajo fin de máster

Carácter: Trabajo Fin de Título (TFT) **ECTS:** 9 **Curso:** Primero **Cuatrimestre:** Segundo

Idiomas de impartición: Español, Inglés

Porcentajes de moldalidad de impartición

- **Presencial:** 20 %
- **Virtual:** 80 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Competencias (COM)	Básicas / Generales / Transversales: CB6, CB7, CB8, CB9, CB10 y CG1 Específica : Capacidad para la creación y elaboración de proyectos de originales y pertinentes, con metodología apropiada y establecimiento de conclusiones relevantes en el ámbito de conocimiento de la Seguridad en Internet.	
Habilidades o Destrezas (HD)	• Asegurar la tutela efectiva de los TFM. • Asegurar que los TFM se realicen en el tiempo establecido en la memoria de verificación de los títulos. • Reconocer la actividad docente de los profesores que los dirijan. • Potenciar la realización de TFM en instituciones externas y empresas. • Disponer de los medios necesarios para la realización de los TFM.	

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Calificación numérica (5-10) del tutor/a del trabajo		60
Calificación numérica (5-10) del tribunal		40

Descripción de contenidos

* Elección del tema selección de tutor/a * Elaboración del proyecto para el tutor/ay aprobación * Acuerdo con el tutor para decidir la metodología aplicable * Búsqueda, lectura y selección de información * Consulta, recopilación y selección de datos, fuentes y documentos * Tutorías con el profesor/tutor * Desarrollo metodológico * Establecimiento de las conclusiones * Elaboración del trabajo * Creación de un discurso y soporte para la defensa.

ASIGNATURAS SEGUNDO CURSO (si lo hubiera)

ASIGNATURAS TERCER CURSO (si lo hubiera)

4.5 Actividades y metodologías docentes

A continuación se detallan las diferentes acciones formativas que se llevarán a cabo en el contexto del Título Propio de Máster. Para la elaborar este listado de acciones formativas se ha seguido las Directrices para la elaboración de las fichas de planificación docente de asignaturas y guías académicas de titulación de Grado y Máster, aprobado en el consejo de Docencia.

• Actividades introductorias (dirigidas por el profesor).

o Actividades introductorias. Este tipo de actividades serán realizadas al inicio de los módulos, para poner a los alumnos en el contexto de la formación que se va a impartir en el módulo. La información estará disponible en la plataforma online al inicio del módulo y de cada asignatura, junto con los primeros contenidos docentes.

§ Formación Híbrida: Aunque la información de forma online, estará disponible de forma previa a las clases de la formación Híbrida, los profesores realizarán una breve introducción a la materia indicando objetivos, contenidos previos, referencias, así como cualquier otra que pueda ser de interés.

• Actividades teóricas (dirigidas por el profesor).

o Sesión magistral. Presentación sintética, secuencial, motivadora y precisa sobre los aspectos clave de los contenidos de la asignatura. Las clases magistrales, se grabarán y colgarán a través de la plataforma.

§ Formación Híbrida: Clase magistral impartida por el profesor.

Temporalmente, se encuadran a continuación de las actividades introductorias, y previamente a las prácticas guiadas.

En cualquier caso, los alumnos dispondrán de abundante documentación textual y audiovisual en formato digital a través de la plataforma, el seguimiento de estos contenidos será guiado por el profesor y los recursos técnicos disponibles en la propia plataforma.

• Actividades prácticas guiadas (dirigidas por el profesor).

o Prácticas de informática. Una vez que se realice las sesiones formativas magistrales e introductorias y magistrales, se realizarán las actividades guiadas. En estas actividades prácticas se intercalará teoría y práctica para que el alumno pueda construir adecuada su propio mapa mental sobre la material. Se crearán recursos y guiones a tal efecto sobre las prácticas, unidos a videos explicativos.

§ Formación Híbrida. En el contexto de la formación, estas actividades prácticas serán presenciales, dado el carácter técnico de la materia del Máster.

• Atención personalizada (dirigidas por el profesor).

o Tutorías. Se utilizará para comprender y ayudar al estudiante, así como guiarlo en su trabajo individual, tratando de que la formación sea personalizada. Se realizará un seguimiento a través de videoconferencia,

audioconferencia, mensajería (síncrona o asíncrona) y email. A través del campus se realizarán diferentes actividades de interacción y seguimiento, que permitan facilitar el trabajo de los alumnos.

§ Formación Híbrida. Seguimiento realizado de forma presencial en el despacho del profesor.

• Actividades prácticas autónomas (Sin el profesor)

o Preparación de trabajos. Permite al alumno aprender en profundidad sobre un tema determinado. Está estrechamente ligado a la siguiente forma de evaluación, ya que la preparación constituye el paso previo a la realización de trabajos.

o Trabajos. El alumno tendrá que realizar informes o reportes sobre una tema concreto, así como prácticas individuales sobre algunos de los temas que componen las asignaturas. Estos trabajos podrán realizarse de forma individual y en grupo.

o Resolución de problemas. Es un proceso mental que permite la identificación y análisis de un problema y la propuesta de solución. En el marco del máster, los problemas serán eminentemente prácticos.

o Foros de discusión. Los foros se utilizarán de forma online con dos objetivos primarios. En primer lugar, la dinamización de la formación, a través del planteamiento de preguntas en los foros que los alumnos tendrán que contestar, y los profesores podrán evaluar. En segundo lugar, la generación de debates públicos sobre cuestiones que tengan los alumnos, y que puedan ser objeto de interés por parte del resto de alumnos.

Los TFMs serán tutorizados por todos los profesores de la titulación quienes acogerán un máximo de tres trabajos a fin de evaluar la metodología apropiada y guiar al alumno en todas las fases de la elaboración de su trabajo final.

4.6 Calendario de comienzo y fin del programa

4.6.1 Duración del programa en meses: 11

4.6.2 Fechas de inicio

Primer edición: Entre 15 de septiembre y 15 de diciembre

- **Del** 23-10-2023 **al** 23-09-2024

Segunda edición:

- **Del** - **al** -

4.6.3 Número de ediciones: 1