1. DESCRIPCIÓN DEL TÍTULO

1.1. DATOS BÁSICOS

NIVEL	DENOMINACIÓN ESPECIFICA	CONJUNTO	CONVENIO	CONV. ADJUNTO
Máster	Máster Universitario en Ciberdelincuencia por la Universidad Antonio de Nebrija	No		Ver Apartado 1: Anexo 1.

LISTADO DE ESPECIALIDADES
No existen datos

RAMA	ISCED 1	ISCED 2
Ingeniería y Arquitectura	Servicios de seguridad	Protección de la propiedad y las personas

NO HABILITA O ESTÁ VINCULADO CON PROFESIÓN REGULADA ALGUNA
AGENCIA EVALUADORA
Fundación para el Conocimiento Madrimasd
UNIVERSIDAD SOLICITANTE
Universidad Antonio de Nebrija
LISTADO DE UNIVERSIDADES

CÓDIGO	UNIVERSIDAD
052	Universidad Antonio de Nebrija

LISTADO DE UNIVERSIDADES EXTRANJERAS	
CÓDIGO	UNIVERSIDAD
No existen datos	

LISTADO DE INSTITUCIONES PARTICIPANTES
No existen datos

1.2. DISTRIBUCIÓN DE CRÉDITOS EN EL TÍTULO

CRÉDITOS TOTALES	CRÉDITOS DE COMPLEMENTOS FORMATIVOS	CRÉDITOS EN PRÁCTICAS EXTERNAS
60		6
CRÉDITOS OPTATIVOS	**CRÉDITOS OBLIGATORIOS**	**CRÉDITOS TRABAJO FIN GRADO/ MÁSTER**
12	36	6

LISTADO DE ESPECIALIDADES	
ESPECIALIDAD	CRÉDITOS OPTATIVOS
No existen datos	

1.3. Universidad Antonio de Nebrija

1.3.1. CENTROS EN LOS QUE SE IMPARTE

LISTADO DE CENTROS	
CÓDIGO	CENTRO
28045921	Escuela Politécnica Superior

1.3.2. Escuela Politécnica Superior

1.3.2.1. Datos asociados al centro

TIPOS DE ENSEÑANZA QUE SE IMPARTEN EN EL CENTRO		
PRESENCIAL	SEMIPRESENCIAL	A DISTANCIA
Sí	Sí	Sí
PLAZAS DE NUEVO INGRESO OFERTADAS		
PRIMER AÑO IMPLANTACIÓN	**SEGUNDO AÑO IMPLANTACIÓN**	
130	150	

	TIEMPO COMPLETO	
	ECTS MATRÍCULA MÍNIMA	**ECTS MATRÍCULA MÁXIMA**
PRIMER AÑO	30.0	60.0
RESTO DE AÑOS	30.0	60.0
	TIEMPO PARCIAL	
	ECTS MATRÍCULA MÍNIMA	**ECTS MATRÍCULA MÁXIMA**
PRIMER AÑO	12.0	30.0
RESTO DE AÑOS	12.0	30.0
NORMAS DE PERMANENCIA		
http://www.nebrija.com/carreras-universitarias/pdf/reglamento-general-alumnado-v2.pdf		
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

2. JUSTIFICACIÓN, ADECUACIÓN DE LA PROPUESTA Y PROCEDIMIENTOS

Ver Apartado 2: Anexo 1.

3. COMPETENCIAS

3.1 COMPETENCIAS BÁSICAS Y GENERALES
BÁSICAS
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
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
GENERALES
CG1 - El alumno debe adquirir aquellos conocimientos sobre recursos humanos que le permitan trabajar en un equipo de ciberdelincuencia
CG2 - El alumno debe ser capaz de entender cómo su profesión afecta a otros departamentos de la empresa o institución en el ámbito de la ciberdelincuencia.
CG3 - El alumno debe dominar las técnicas de lucha contra la ciberdelincuencia suficientes en el ámbito de la ciberdelincuencia que le permitan obtener y analizar información, evaluar su relevancia y validez, sintetizarla y adaptarla al contexto.
CG4 - El alumno debe ser capaz de tratar situaciones complejas e impredecibles de forma sistemática y creativa, con juicio crítico, con información incompleta, asumiendo riesgos, tomando decisiones y comunicándolas a una audiencia profesional del ámbito de la ciberseguridad y ciberdelincuencia
CG5 - El alumno debe ser capaz de comunicarse correctamente tanto oralmente como por escrito, utilizando la tecnología más actual, en el ámbito de la ciberseguridad y ciberdelincuencia.
CG6 - El alumno debe ser capaz de actuar de forma autónoma en la planificación e implementación de proyectos y decisiones sobre prevención y actuación frente a la ciberdelincuencia.
CG7 - El alumno debe ser capaz de desempeñar diferentes roles dentro de un equipo de la ciberseguridad y ciberdelincuencia, en particular el de líder.
CG8 - El alumno, en el ámbito de la actuación frente a la ciberdelincuencia, debe ser capaz de reconocer la necesidad del cambio y debe tener la habilidad necesaria para gestionarlo.
CG9 - El alumno debe ser capaz de actuar de forma autónoma en un marco de libertad responsable, en el ámbito de la actuación frente a la ciberdelincuencia.
CG10 - El alumno debe ser capaz de aportar valor a la empresa o institución mediante su creatividad y participación en la actuación frente a la ciberdelincuencia
CG11 - Capacidad para integrar en su actuación frente a la ciberdelincuencia, los valores y políticas de igualdad efectiva, especialmente entre mujeres y hombres y atención a la discapacidad.
3.2 COMPETENCIAS TRANSVERSALES
No existen datos
3.3 COMPETENCIAS ESPECÍFICAS
CE1 - Ser capaz de analizar y desarrollar sistemas de seguridad web aplicado a la prevención de la ciberdelincuencia.
CE2 - Ser capaz de asesorar sobre el cumplimiento de la legislación reguladora de la protección de datos en materia de seguridad
CE3 - Ser capaz de planificar y aplicar medidas de prevención contra fraudes en comercio electrónico.
CE4 - Ser capaz de aplicar las propiedades biométricas al área de seguridad informática y de las comunicaciones.
CE5 - Ser capaz de distinguir los diferentes agentes implicados en seguridad informática, y saber asesorarlos de forma integrada permitiendo la colaboración con otros departamentos de la entidad.

CE6 - Ser capaz de programar y analizar tareas en diversos lenguajes de programación en el área de seguridad informática y de las comunicaciones.
CE7 - Ser capaz de utilizar las herramientas científico técnicas para evaluar la fiabilidad y robustez de sistemas informáticos complejos, aplicado a la prevención de la ciberdelincuencia.
CE10 - Ser capaz de diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos, aplicado a la prevención de la ciberdelincuencia.
CE11 - Ser capaz de utilizar con destreza las principales herramientas de detección y clasificación de malware y de realizar ejercicios sencillos de ingeniería inversa en el contexto de la ciberseguridad
CE12 - Ser capaz de realizar, presentar y defender, una vez obtenidos todos los créditos del plan de estudios, un ejercicio original ante un tribunal universitario, consistente en un proyecto de investigación en el campo de la ciberdelincuencia en el que se sinteticen las competencias adquiridas en las enseñanzas.

4. ACCESO Y ADMISIÓN DE ESTUDIANTES

4.1 SISTEMAS DE INFORMACIÓN PREVIO

Ver Apartado 4: Anexo 1.

4.2 REQUISITOS DE ACCESO Y CRITERIOS DE ADMISIÓN

4.2. Requisitos de Acceso y Criterios de Admisión

4.2.1. Acceso

Según lo establecido en el artículo 16 del RD 1393/2007, modificado por el RD 861/2010 podrán acceder a estos estudios los estudiantes que reúnan cualquiera de las siguientes condiciones:

- Estar en posesión de un título universitario oficial español u otro expedido por una institución de educación superior del Espacio Europeo de Educación Superior que faculte en el país expedidor del título para el acceso a enseñanzas de Máster.
- Los titulados conforme a sistemas educativos ajenos al Espacio Europeo de Educación Superior podrán acceder sin necesidad de la homologación de sus títulos, previa comprobación por la Universidad de que aquellos acreditan un nivel de formación equivalente a los correspondientes títulos universitarios oficiales españoles y que facultan, en el país expedidor del título, para el acceso a enseñanzas de postgrado. El acceso por esta vía no implicará, en ningún caso, la homologación del título previo de que esté en posesión el interesado, ni su reconocimiento a otros efectos que el de cursar las enseñanzas de Máster. En los supuestos en los que se exija la homologación de cualquier título, diploma o estudio obtenido en el extranjero para el acceso a la Universidad, la Universidad Antonio de Nebrija podrá admitir con carácter condicional a los estudiantes que acrediten haber presentado la correspondiente solicitud de la homologación mientras se resuelva el procedimiento de dicha homologación. Dentro del Plan de Ordenación Académica que tiene implementado la Universidad, se ha desarrollado el ¿Procedimiento de Matrícula Condicionada¿ que recoge estos supuestos.
- En caso de alumnos con necesidades educativas especiales derivadas de discapacidad, se evaluará la necesidad de posibles adaptaciones curriculares, itinerarios o estudios alternativos.

Criterios de admisión

4.2.2 Forma de entrega de la documentación necesaria para la admisión.

Con carácter general, la documentación de admisión se presentará en el Departamento de Admisiones.

El estudiante deberá aportar los originales o copias compulsadas de la documentación presentada, en plazo establecido por la Universidad para formalizar su matrícula. La inexactitud, falsedad u omisión de los datos, manifestación o documento aportados por el estudiante en el periodo de admisión, determinará la imposibilidad de continuar con el ejercicio del derecho desde el momento en que la Universidad tenga constancia de tales hechos, procediéndose a la anulación de la solicitud de admisión presentada y la plaza adjudicada, sin perjuicio de las responsabilidades penales, civiles o administrativas a que hubiera lugar.

Para acceder a los másteres universitarios oficiales es necesario, entregar la siguiente documentación:

- Solicitud de Admisión cumplimentada.
- Documento identificativo D.N.I o pasaporte en vigor
- 2 Fotografía tamaño carnet

- En caso de que sea necesario, carta emitida por la Universidad en la que se ha cursado el nivel que da acceso al estudio de Máster en el país expendedor del título.

- Certificación Académica con las notas del estudio que da acceso al Master.

- Título universitario oficial español.

- Título oficial expedido por una institución de educación superior extranjera perteneciente al **Espacio Europeo de Educación Superior (EEES)** que faculte, en el país de expedición, para acceder a las enseñanzas de máster oficial.

- Título oficial expedido en un sistema educativo extranjero no perteneciente al EEES. En este caso, el acceso estará condicionado a la comprobación que los estudios cursados corresponden a un nivel de formación equivalente al de los títulos universitarios oficiales españoles y que capacitan para acceder a estudios de máster oficial en el país en el que se ha expedido el título. Este trámite no implica, en ningún caso, la homologación del título previo, ni su reconocimiento para otra finalidad que no sea la de acceder a los estudios de máster.

- Carta de intenciones personalizada dirigida al Director del Programa Máster Universitario en Ciberdelincuencia en la que expliquen los motivos por los que desea realizar los estudios de Máster así como las expectativas académicas y profesionales que lo llevan a esta elección.

- Curriculum Vitae actualizado.

- Dos cartas de recomendación.

En el caso de que los estudios con los que se accede a la preinscripción de Máster estén cursados en una instrucción de Educación Superior Extranjera, tanto el título como el certificado académico (notas) deberán ser oficiales y estar expedidos por las autoridades competentes, de acuerdo con el ordenamiento jurídico del país de origen. Además, tendrán que cumplir los requisitos que se indican con detalle en el ¿Procedimiento de acceso y admisión de Master_PO12¿ del Plan de Ordenación Docente que tiene implementado la Universidad.

Si el número de solicitantes excede del número de plazas ofertadas se tomará como criterio de admisión el expediente académico del estudiante (nota media).

Por tanto, todo aquel interesado en acceder a los estudios del Máster en Ciberdelincuencia deberá presentar, sin excepción, su expediente académico pues será la nota media del mismo la que decida su admisión en el Máster, en el caso de que el número de solicitudes supere al número de plazas ofertadas.

Una vez se completen las plazas, en el caso de haber más interesados en acceder, estos quedarán en lista de espera ante posibles vacantes que puedan surgir antes del comienzo de curso, aplicándose los criterios de admisión y selección detallados en el punto 4 para el resto de solicitantes.

4.2.3. Proceso de Admisión

1.- Prueba de nivel de lengua española para extranjeros 10%

Con el fin de conocer el nivel real de conocimientos de la lengua española por parte de los estudiantes extranjeros, el Instituto de Lenguas Modernas diseñará una prueba de posicionamiento del idioma. Las pruebas de nivel consisten en un examen escrito con preguntas tipo test, de comprensión oral y escrita, y uso de la lengua con una duración 60 minutos. Son de carácter presencial u online. En función de los resultados de esta prueba, se posicionará al alumno en el nivel correspondiente.

No será necesario que el candidato realice la prueba de posicionamiento de idiomas si entrega documento que acredite el conocimiento de lengua española en el nivel B2 del MCER. Se validará la acreditación del nivel a través de los títulos oficiales admitidos por la tabla de certificados admitidos por ACLES).

http://www.acles.es , y además serán revisados por el Instituto de Lenguas Modernas.

2.- Entrevista personal 90% para extranjeros, 100% para hispanohablantes.

Realizado por el profesorado y por asesores universitarios de la Universidad, esta entrevista está orientada a comprobar la idoneidad del candidato y el perfil del mismo de acuerdo con la titulación. Se trata de determinar si el candidato/a posee la suficiente motivación, formación y conocimientos, habilidades, aptitudes, destrezas de comunicación, actividades extracurriculares e intereses de futuro necesarios para ser admitido como estudiante en este posgrado de la Universidad Nebrija.

3.- Pruebas específicas del título: no proceden

4.2.4. Proceso de Matriculación

Una vez que el alumno ha sido admitido procederá a realizar la matriculación que consta de las siguientes fases:

Derechos de inscripción anual

Los candidatos deben realizar la reserva de plaza. Esta pre-matrícula económica garantiza la plaza del candidato en la Universidad. Estos derechos de inscripción anual no se devolverán salvo los alumnos que están admitidos condicionalmente, o no superen los requisitos legales de acceso.

Matrícula

Los candidatos pre-matriculados que deseen formalizar su matrícula académica en la Universidad deberán, dentro de los plazos señalados, seguir los siguientes pasos:

1.- Entrega de documentación: acreditar que cumple con los requisitos establecidos por la legislación universitaria española para la admisión al Máster.

2.- Formalización del proceso de matrícula vía Internet: El servicio de auto matrícula de la página Web de la Nebrija permite a los estudiantes admitidos realizar todos los trámites académicos, económicos y administrativo en los plazos establecidos. Para ello, recibirán, junto con su carta de admisión, la clave de acceso y la contraseña personal necesarios para poder realizar su auto matrícula. Formalizada la automatrícula, el candidato adquiere la condición de alumno de la Universidad Nebrija.

3.- Realizar el pago de la matrícula del curso, según la modalidad elegida por el alumno.

Plazos para realizar matrícula

1.- La matrícula se realizará con carácter anual, la fecha de apertura variará en función del comienzo del Programa. No obstante la matricula deberá realizarse obligatoriamente con al menos una semana de antelación al comienzo del periodo lectivo.

2.- Se abrirá con carácter excepcional un periodo extraordinario para los alumnos que quieran comenzar los estudios en el segundo semestre, la matriculación deberá realizarse antes de la realización de los exámenes parciales del segundo semestre.

4.3 APOYO A ESTUDIANTES

4.3 Apoyo y Orientación a estudiantes, una vez matriculados.

El apoyo y la orientación al alumno se realizan, a partir de ese momento, a través de los siguientes cauces:

1.- Director y profesores del Máster, cuya función es estimular y dirigir el aprendizaje de los alumnos. El Director del Máster designa el tutor/a de cada grupo al comienzo de curso.

2.- Profesor-Tutor, es un referente real para cada alumno. La responsabilidad del tutor es dar ejemplo, animar, estimular y dirigir el aprendizaje de sus tutorados. En el día a día debe aclarar dudas, orientar esfuerzos, transmitir la idea de la solidez de la enseñanza y de la institución.

Asimismo el tutor deberá realizar ***las tutorías***, reunirse de forma individual con sus tutorados tantas veces como fuera conveniente y, al menos, una vez al semestre. Para todo ello el tutor debe comunicar a principio de curso las horas de atención a sus tutorados.

Es importante que los tutores de los estudiantes de Máster estén en comunicación permanente con el Departamento de Carreras Profesionales (CP) para conocer la orientación profesional de los alumnos y las actividades de búsqueda de prácticas que realiza cada uno de sus tutorados.

El tutor debe coordinar los temas comunes con todos los profesores del grupo. En este sentido, debe mantenerse informado por el resto de los profesores del grupo y tomar las medidas oportunas, en su caso, sobre posibles incidencias como faltas reiteradas de asistencia, bajo rendimiento, etc. Una de sus funciones prioritarias es facilitar la comunicación de los Directores de Departamento, Coordinadores y de la Secretaría de Cursos con los estudiantes.

Coordinar los temas comunes con todos los profesores del grupo, debe mantenerse informado por el resto de los profesores del grupo y tomar las medidas oportunas, en su caso, sobre posibles incidencias como faltas reiteradas de asistencia, bajo rendimiento, etc.

A su vez, debe informar a sus tutorados sobre las recomendaciones que las Reuniones de Coordinación y Evaluación Académica han hecho sobre su aprendizaje, su rendimiento y su actitud en las diferentes asignaturas y actividades.

La libertad de acción del tutor para cumplir sus responsabilidades es amplia, responsabilizándose ante el Director del Programa y siempre bajo su supervisión.

Se recomienda al profesorado realizar esta función tutorial para participar con mayor intensidad en la motivación, la generación de expectativas y los logros de sus estudiantes.

Además, cada alumno cuenta con el asesoramiento y apoyo de un Profesor-Tutor de Trabajo de Fin de Máster, que el Coordinador de la asignatura selecciona tras la propuesta razonada del estudiante, un procedimiento que se describe con mayor detalle en esta Memoria, al dar cuenta de la planificación del programa.

Finalmente, cabe señalar en este epígrafe dedicado a la descripción de los sistemas de apoyo y orientación de los estudiantes, una vez matriculados, que el primer día de clase el alumno recibe una carpeta que contiene la Guía de la Actividad docente; un documento que recoge las normativas vigentes en la Universidad.

3.- Dentro del Departamento de Atención Integral al Alumno, se ha creado recientemente el Servicio de Orientación al Estudiante cuyo objetivo es prestar ayuda a cualquier miembro de la Comunidad Universitaria que en determinado momento pueda encontrarse en una situación que sienta difícil de superar sin apoyo.

Ofrece la posibilidad de expresar y comentar la situación personal a un psicólogo/psicopedagogo con experiencia que puede aconsejar al estudiante, valorando si se trata de un problema menor o si puede requerir más intervención especializada y seguimiento, todo ello garantizando la total confidencialidad y reserva.

Se accede por derivación del tutor del grupo, que es generalmente la persona con la que el estudiante tiene el contacto diario y que puede detectar la necesidad de asesoramiento psicológico más allá de lo que éste pueda proporcionarle.

Además de los tutores y de los miembros del Servicio de Orientación al Estudiante con la Secretaría Académica de la Facultad, con el Director de la titulación, la Vicedecana y el Decano. Asimismo, podrán ayudarles en todo lo necesario, una vez matriculados, el Departamento de Sistemas y Servicios Informáticos, el Departamento Internacional, el Departamento de Infraestructuras y Servicios o, entre otros, el Departamento de Promoción y Admisiones.

Modalidad semipresencial y a distancia

La Universidad Antonio de Nebrija tiene muy interiorizados los procedimientos de los sistemas de apoyo y orientación de los estudiantes una vez matriculados. De manera general todos los Departamentos, tanto Académicos como de Servicios, están siempre orientados a facilitar el acceso a la Universidad del alumnado de nuevo ingreso.

En relación a la modalidad de enseñanza semipresencial y a distancia del título, una vez ha cerrado el proceso de automatrícula, podrá acceder a los diferentes entornos virtuales para el desarrollo de sus estudios y a la documentación correspondiente necesaria de apoyo para su uso y aplicación:

- Portal del Alumnado.
- Campus Virtual (soportado por la plataforma Blackboard Learn).
- Office365: Correo electrónico, OneDrive, etc.
- Biblioteca: Recursos accesibles a través del Catálogo-OPAC, bibliografías seleccionadas, libros electrónicos, etc.

Con el objetivo de facilitar la introducción a la modalidad semipresencial y a distancia en los contextos virtuales de enseñanza y aprendizaje y de dar el apoyo necesario a los alumnos de estas modalidades se ha creado una plataforma dentro de la organización de la Universidad: Global Campus Nebrija (GCN). Desde esta unidad se realiza la atención integral al alumnado (virtual y presencial) y se facilita el material de instrucción necesario (guías y manuales) para el trabajo y comunicación de los estudiantes en los entornos virtuales, así como se gestiona el material y los recursos digitales multiplataforma. Adicionalmente, GCN realiza el análisis de las tecnologías y metodologías docentes de la Universidad.

Dentro de esta organización (GCN) se encontrará el Gestor de programa de la modalidad de enseñanza semipresencial o a distancia, que será el responsable de la atención integral a los alumnos del programa en coordinación con los Departamentos Académicos, de Servicios y de Desarrollo Universitario.

Además, se realizará una Sesión de Bienvenida a través de la herramienta de videoconferencia del Campus Virtual (Blackboard Collaborate), de carácter voluntario, para los estudiantes matriculados en este título. Se trata de un curso de introducción y bienvenida con el objetivo principal de familiarizar a los estudiantes con el funcionamiento del Campus Virtual y de las herramientas digitales de la Universidad Antonio de Nebrija, entre las que se incluyen:

- Accesos a correo electrónico, Portal del Alumnado, Campus Virtual y Catálogo de Biblioteca.
- Consulta y descarga de materiales y recursos electrónicos de la Universidad.
- Envío y recepción de documentación.
- Itinerarios formativos.

- Herramientas de comunicación asíncrona: anuncios, mensajes y foros.
- Herramientas de comunicación síncrona: chats y videoconferencias (Blackboard Collaborate).
- Buzón de actividades y pruebas de evaluación.
- Aplicaciones móviles (Blackboard Learn y Blackboard Collaborate).

Por otro lado, el alumno tendrá a su disposición un profesor tutor, cuya labor es dar asistencia académica y personal a los estudiantes para la consecución de los objetivos del curso. Para ello el tutor dispone de las siguientes herramientas:

- Foros a través del Campus Virtual.
- Correo electrónico.
- Asistencia telefónica en horario prefijado.
- Comunicación virtual síncrona a través de la herramienta Blackboard Collaborate, que permiten la visualización e interacción directa entre profesor y alumno (audio, vídeo y chat) y la visualización conjunta de documentación.

4.3.1 Normativa de Permanencia

El Reglamento del Alumnado de la Universidad Antonio de Nebrija indica en su Artículo 2, en relación a la pérdida de condición de alumno:

Artículo 2. Pérdida de esta condición

La condición de alumno se pierde por alguna de las siguientes causas:

1. La terminación de los estudios y la obtención del título correspondiente.

2. El traslado voluntario del expediente a otro centro universitario.

3. La interrupción voluntaria de los estudios salvo en lo dispuesto para la dispensa de escolaridad.

4. La resolución firme de la Comisión Disciplinaria conforme a lo dispuesto en este Reglamento.

5. El incumplimiento de las obligaciones económicas del alumno/a, ya sea por no haber hecho efectivo el pago de las tasas académicas antes de incorporarse a los diferentes cursos y programas o, en los pagos por periodos o mensualidades, por tener más de dos mensualidades sin pagar y no formalizar el pago de éstas tras haber sido requerido para ello. Todo ello sin perjuicio de las acciones legales que pudieran corresponder a la Universidad por el incumplimiento de las obligaciones económicas contraídas.

6. Incurrir en alguno de los motivos de perdida de condición de alumno descritos en este Reglamento.

7.- Por incumplimiento de las normas previstas en el procedimiento para la matricula condicionada.

Toda persona que, conforme a lo establecido en este artículo, deje de ser alumno de la Universidad Antonio de Nebrija, perderá también todos los derechos que tal condición lleva aparejados, independientemente del momento en que los hubiera podido adquirir.

De igual modo, en su Capítulo 4 indica acerca de la permanencia:

Permanencia del alumno

Artículo 10. Régimen de permanencia

Además de por las demás causas expuestas en este Reglamento y demás normativa de la Universidad vigente y de aplicación, incurrirán en causa de pérdida de la condición de alumno de la Universidad Antonio de Nebrija, causando baja:

a) Los alumnos que no aprueben un porcentaje mínimo de los créditos ECTS que tuviera matriculados en el correspondiente curso académico, excluidos claro está, aquellos que hayan sido objeto de reconocimiento o transferencia. Este porcentaje mínimo para permanecer, estará comprendido entre el 20% y el 40% en el caso de Títulos de Grado y entre el 20% y el 60% para el caso de títulos de Master, a propuesta de cada Facultad y con la aprobación final de Rectorado. Dichos porcentajes serán de aplicación a cualquier alumno de la Universidad independientemente de la modalidad en la que curse sus estudios

Criterio de permanencia en Grado según Facultades:

[¿]

Escuela Politécnica Superior 40 %

[¿]

Para realizar el cómputo del porcentaje no se tendrán en cuenta los ECTS correspondientes a las siguientes asignaturas:

- Prácticas en empresas

- Desarrollo del espíritu participativo y solidario. Únicamente en las vías de obtención de ECTS a través de participación en actividades universitarias. La obtención de ECTS en esta materia a través de la superación de las asignaturas definidas en la misma sí se tendrán en cuentan para el cómputo del porcentaje,

- Trabajo Fin de Grado/Trabajo Fin de Máster

b) Los alumnos que hayan agotado el número máximo de convocatorias en alguna materia.

c) Los alumnos que, transcurrido desde su primera matrícula el doble del tiempo previsto para cursarlos con dedicación plena, no hayan superado los mismos, salvo que aleguen justa causa para ello, entendiéndose por tal la que así sea considerada por la Universidad como por ejemplo a título ilustrativo y no limitativo, la compatibilidad de los estudios con la actividad profesional o laboral. En el cómputo de dicho plazo no se contabilizarán los periodos de dispensa concedidos al alumno.

Artículo 11. Procedimiento

El alumno que se encontrare en los casos A o C a los que se refiere el artículo anterior, dispondrá de un plazo improrrogable de quince días a contar desde aquel en el que la Universidad le comunique la baja para alegar mediante escrito presentado ante la Secretaría de Cursos lo que tuviere por conveniente. Dichas alegaciones serán objeto de examen por parte del Vicerrector de Ordenación Académica o la Comisión Académica correspondiente, quienes decidirán lo que proceda de forma graciable, siendo su decisión irrevocable.

El alumno que se encuentre en el caso B a los que se refiere el artículo anterior, deberá atender a lo previsto en este Reglamento en materia de convocatorias.

A su vez, los Artículos 21 y 22 indican:

Artículo 21. Límite de convocatorias

Salvo que se establezca una norma específica por la Universidad, los alumnos de Grado disponen de cinco convocatorias para obtener los créditos correspondientes a cada materia. Agotadas las cinco convocatorias, la Universidad podrá, discrecionalmente, conceder otra más, si así lo solicita el alumno mediante escrito dirigido a la Secretaria de Cursos.

[¿]

Artículo 22. Última convocatoria

[¿]

La no superación de la última convocatoria (6ª para Grado y 4ª para Máster) supondrá la pérdida de la condición de alumno de la Universidad Antonio de Nebrija, de conformidad con lo dispuesto en este Reglamento y demás normativa general vigente y de aplicación. Con carácter excepcional, el alumno podrá solicitar por escrito al Rector, alegando causa justificada la realización de la 7ª convocatoria para Grado y la 5ª convocatoria para Master. Contra la resolución del Rector resolviendo dicha solicitud, no cabrá recurso alguno.

[¿]

Por último, en el Título V, De las Infracciones y las Sanciones, el Capítulo 2 indica:

Artículo 35. Sanciones

Los distintos tipos de infracciones llevarán aparejada la imposición de las siguientes sanciones y recargos económicos:

c) Infracción muy grave: Suspensión de la condición de alumno por un periodo de entre seis meses y un año, o si así fuera acordado, expulsión definitiva del alumno, con anulación de la matrícula en el curso académico de la resolución y pérdida de cualesquiera derechos académicos y económicos, así como en su caso restitución o indemnización por el daño causado.

4.4 SISTEMA DE TRANSFERENCIA Y RECONOCIMIENTO DE CRÉDITOS	
Reconocimiento de Créditos Cursados en Enseñanzas Superiores Oficiales no Universitarias	
MÍNIMO	**MÁXIMO**
0	0
Reconocimiento de Créditos Cursados en Títulos Propios	
MÍNIMO	**MÁXIMO**
0	54
Adjuntar Título Propio	

Ver Apartado 4: Anexo 2.

Reconocimiento de Créditos Cursados por Acreditación de Experiencia Laboral y Profesional

MÍNIMO	MÁXIMO
0	9

1. **Sistema de Trasferencia y Reconocimiento de Créditos.**

Reconocimiento de Créditos Cursados en Enseñanzas Superiores Oficiales No Universitarias	
Mínimo:	0
Máximo:	0
Reconocimiento de Créditos Cursados en Títulos Propios*	
Mínimo:	0
Máximo:	54
Reconocimiento de Créditos Cursados por Acreditación Experiencias Laboral y Profesional	
Mínimo:	0
Máximo:	9

* Entre ambos no pueden superar el 15% de los ECTS totales del Título

Tabla de reconocimientos entre el título propio Máster en ciberdelincuencia y el Máster Universitario ciberdelincuencia						
Máster en ciberdelincuencia	**ECTS**	**Horas teóricas/ prácticas**	**Máster Universitario en ciberdelincuencia**	**ECTS**	**Reconocimiento**	
Materia cursada			**Materia a reconocer**			
Ciberseguridad y agentes de la Amenaza	6	45/150	Ciberseguridad y agentes de la Amenaza	6	si	
Marco jurídico: proceso penal, aspectos transversales y agente encubierto	6	45/150	Marco jurídico: proceso penal, aspectos transversales y agente encubierto	6	si	
Taller Tecnológico de Ciberdelincuencia	6	45/150	Taller Tecnológico de Ciberdelincuencia	6	si	
Gestión de Proyectos de Investigación aplicado a la Ciberdelincuencia	6	45/150	Gestión de Proyectos de Investigación aplicado a la Ciberdelincuencia	6	Si	
Auditoria Forense de la Ciberdelincuencia	6	45/150	Auditoria Forense de la Ciberdelincuencia	6	si	
Entorno y equipo de Investigación de Ciberdelincuencia	6	45/150	Entorno y equipo de Investigación de Ciberdelincuencia	6	Si	
Metodología de la investigación policial aplicada a la Ciberdelincuencia	6	45/150	Metodología de la investigación policial aplicada a la Ciberdelincuencia	6	Si	
Ciberterrorismo	6	45/150	Ciberterrorismo	6	Si	

Compliance: prevención de delitos empresariales	6	45/150	Compliance: prevención de delitos empresariales	6	Si	
Responsabilidad Social Corporativa Reputación	6	45/150	Responsabilidad Social Corporativa Reputación	6	Si	
Ciberinteligencia	6	45/150	Ciberinteligencia	6	si	
Prácticas profesionales	6	45/150	Prácticas profesionales	6	si	
Trabajo final de Máster	6	45/150	Trabajo final de Máster	6	No	

Conforme señala el art. 13 RD 1393/2007 de 29 de octubre, modificado posteriormente por el RD 861/2010, y por el RD 195/2016, los alumnos matriculados en la Universidad Antonio de Nebrija podrán solicitar reconocimiento o transferencia de créditos cursados en esta u otra Universidad.

Se entiende por reconocimiento la aceptación por parte de la Universidad Antonio de Nebrija de los créditos que, habiendo sido obtenidos en unas enseñanzas oficiales, en ésta u otra Universidad, son computados en otras distintas a efectos de obtención de un título oficial.

Asimismo la transferencia de créditos implica la inclusión en los documentos académicos oficiales acreditativos de las enseñanzas seguidas por cada estudiante, de los créditos obtenidos en enseñanzas oficiales cursadas con anterioridad, en ésta u otra Universidad, que no hayan conducido a la obtención de un título oficial.

Serán objeto de reconocimiento en las nuevas enseñanzas los créditos obtenidos por el estudiante:

- Aquellas materias cuyos reconocimientos y competencias presentan un grado de similitud sustancial con los contenidos de las materias a reconocer.
- Los créditos cursados en otras enseñanzas superiores oficiales.
- Los créditos cursados en enseñanzas universitarias conducentes a la obtención de otros títulos, a los que se refiere el artículo 34.1 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, modificada por la Ley Orgánica 4/2007 de 12 de abril.
- La experiencia laboral y profesional acreditada siempre que dicha experiencia esté relacionada con las competencias inherentes al título.

Se realizará el reconocimiento de créditos por experiencia laboral y profesional acreditada, si dicha experiencia está relacionada con las competencias inherentes al título en la materia objeto de reconocimiento. La acreditación se podrá fundamentar en informes y/o certificados emitidos por las empresas o entidades en las que se desarrolló la actividad, Colegios profesionales, etc. Esto se justifica en la propia redacción del RD 861/2010 que exige la acreditación de esa experiencia y parece lógico que esa acreditación sea realizada por terceros.

ASIGNATURA	ÁMBITO LABORAL	DURACIÓN	EXPERIENCIA PREVIA	COMPETENCIAS	COMPETENCIAS ADQUIRIDAS CON LA EXP. PROF.

		(mínimo en meses)			
Ciberseguridad y agentes de la Amenaza	Seguridad	6 meses	Experiencia en cualquier empresa, institución pública o privada, u organismo gubernamental o no gubernamental vinculada al área de seguridad	• Competencias básicas: CB6; CB7; CB8; CB9; CB10 • Competencias generales: CG1; CG3; CG4; CG8; CG9 • Competencias específicas:; CE4; CE6; CE7;~~CE8; CE9;~~ CE10; CE11	• Competencias básicas: CB6; CB7; CB8; CB9; CB10 • Competencias generales: CG1; CG3; CG4; CG8; CG9 • Competencias específicas:CE4; CE6; CE7;~~CE8; CE9;~~ CE10; CE11
Marco jurídico: proceso penal, aspectos transversales y agente encubierto	Jurídico	6 meses	Experiencia en cualquier empresa, institución pública o privada, u organismo gubernamental o no gubernamental vinculada al área de jurídica de la seguridad	• Competencias básicas: CB6; CB7; CB8; CB9; CB10 • Competencias generales: CG4; CG5; CG6; CG7; CG10; CG11 • Competencias específicas: CE2; CE3; CE10	• Competencias básicas: CB6; CB7; CB8; CB9; CB10 • Competencias generales: CG4; CG5; CG6; CG7; CG10; CG11 • Competencias específicas: CE2; CE3; CE10
Gestión de Proyectos de Investigación aplicado a la Ciberdelincuencia	Gestión de proyectos	6 meses	Experiencia en cualquier empresa, institución pública o privada, u organismo gubernamental o no gubernamental vinculada al área de proyectos	• Competencias básicas: CB6; CB7; CB8; CB9; CB10 • Competencias generales: CG1; CG3; CG5; CG8; CG9; CG11 • Competencias específicas: CE5; CE6;CE7; ~~CE8~~; CE10	• Competencias básicas: CB6; CB7; CB8; CB9; CB10 • Competencias generales: CG1; CG3; CG5; CG8; CG9; CG11 • Competencias específicas:CE5; CE6;CE7; ~~CE8~~; CE10
Auditoria Forense de la Ciberdelincuencia	Auditoria	6 meses	Experiencia en cualquier empresa, institución pública o privada, u organismo gubernamental o no gubernamental vinculada al área forense	• Competencias básicas: CB6; CB7; CB8; CB9; CB10 • Competencias generales: CG2; CG4; CG7; CG11 • Competencias específicas: CE1; CE3; CE4; CE10; CE11	• Competencias básicas: CB6; CB7; CB8; CB9; CB10 • Competencias generales: CG2; CG4; CG7; CG11 • Competencias específicas: CE1; CE3; CE4; CE10; CE11
Entorno y equipo de Investigación de Ciberdelincuencia	Seguridad y ciberdelito	6 meses	Experiencia en cualquier empresa, institución pública o privada, u organismo gubernamental o no gubernamental vinculada al área de seguridad	• Competencias básicas: CB6; CB7; CB8; CB9; CB10 • Competencias generales: CG5; CG7; CG8; CG10 • Competencias específicas: CE1; CE2; CE3; CE7; ~~CE8; CE9,~~ CE10	• Competencias básicas: CB6; CB7; CB8; CB9; CB10 • Competencias generales: CG5; CG7; CG8; CG10 • Competencias específicas: CE1; CE2; CE3; CE7; ~~CE8; CE9,~~ CE10
Metodología de la investigación policial aplicada a la Ciberdelincuencia	Policial	6 meses	Experiencia en cualquier empresa, institución pública o privada, u organismo gubernamental o no gubernamental vinculada al área de seguridad	• Competencias básicas: CB6; CB7; CB8; CB9; CB10 • Competencias generales: CG3; CG6; CG8; CG10 • Competencias específicas:	• Competencias básicas: CB6; CB7; CB8; CB9; CB10 • Competencias generales: CG3; CG6; CG8; CG10 • Competencias específicas:

				CE1; CE3; CE4; CE10; CE11	CE1; CE3; CE4; CE10; CE11
Ciberterrorismo	Ciberseguridad	6 meses	Experiencia en cualquier empresa, institución pública o privada, u organismo gubernamental o no gubernamental vinculada al área de seguridad	• Competencias básicas: CB6; CB7; CB8; CB9; CB10 • Competencias generales: CG4; CG5; CG9; CG11 • Competencias específicas: CE5; CE10; CE11	• Competencias básicas: CB6; CB7; CB8; CB9; CB10 • Competencias generales: CG4; CG5; CG9; CG11 • Competencias específicas: CE5; CE10; CE11
Compliance: prevención de delitos empresariales	Prevencion de delitos en la empresa	6 meses	Experiencia en cualquier empresa, institución pública o privada, u organismo gubernamental o no gubernamental vinculada al área de prevención de riesgos para la empresa	• Competencias básicas: CB6; CB7; CB8; CB9; CB10 • Competencias generales: CG2; CG4; CG8; CG9; 10; CG11 • Competencias específicas: CE3; CE2; ~~CE9,~~ CE10	• Competencias básicas: CB6; CB7; CB8; CB9; CB10 • Competencias generales: CG2; CG4; CG8; CG9; 10; CG11 • Competencias específicas: CE3; CE2; ~~CE9,~~ CE10
Responsabilidad Social Corporativa Reputación	Responsabilidad social	6 meses	Experiencia en cualquier empresa, institución pública o privada, u organismo gubernamental o no gubernamental vinculada al área de RCS	• Competencias básicas: CB6; CB7; CB8; CB9; CB10 • Competencias generales: CG1; CG2; CG4; CG7; CG8; CG9; CG10; CG11 • Competencias específicas: CE2; CE7; ~~CE9~~; CE10	• Competencias básicas: CB6; CB7; CB8; CB9; CB10 • Competencias generales: CG1; CG2; CG4; CG7; CG8; CG9; CG10; CG11 • Competencias específicas: CE2 CE7; ~~CE9~~; CE10
Ciberinteligencia	Ciberseguridad	6 meses	Experiencia en cualquier empresa, institución pública o privada, u organismo gubernamental o no gubernamental vinculada al área de seguridad	• Competencias básicas: CB6; CB7; CB8; CB9; CB10 • Competencias generales: CG2; CG3; CG4; CG5; CG6; CG9; CG11 • Competencias específicas: CE1; CE3; CE4; CE6; CE7; ~~CE8,~~ CE10; CE11	• Competencias básicas: CB6; CB7; CB8; CB9; CB10 • Competencias generales: CG2; CG3; CG4; CG5; CG6; CG9; CG11 • Competencias específicas: CE1; CE3; CE4; CE6; CE7; ~~CE8,~~ CE10; CE11
Prácticas profesionales	seguridad	6 meses	Experiencia en cualquier empresa, institución pública o privada, u organismo gubernamental o no gubernamental vinculada al área de seguridad	• Competencias básicas: CB6; CB7, CB8; CB9; CB10 • Competencias generales: CG1; CG2; CG3; CG4; CG5; CG6; CG7; CG8, CG9; CG10; CG11 Competencias específicas: CE1; CE2; CE3; CE4; CE5; CE6; CE7; ~~CE8; CE9,~~ CE10; CE11;	• Competencias básicas: CB6; CB7, CB8; CB9; CB10 • Competencias generales: CG1; CG2; CG3; CG4; CG5; CG6; CG7; CG8, CG9; CG10; CG11 Competencias específicas: CE1; CE2; CE3; CE4; CE5; CE6; CE7; ~~CE8; CE9~~; CE10; CE11;

En ningún caso se realizará un reconocimiento general de créditos en función de años de experiencia, ni ningún otro criterio general semejante.

La presentación de este tipo de informes y/o certificados que acrediten la experiencia laboral y profesional será condición necesaria, pero no suficiente, para el reconocimiento de esos créditos, puesto que finalmente será la Universidad Antonio de Nebrija, la que decida si procede o no, el reconocimiento de los créditos a la vista de la acreditación

presentada, en aplicación de la legislación vigente, en el ejercicio de su autonomía universitaria y conforme a su procedimiento interno de reconocimiento de créditos.

La Universidad Nebrija pondrá especial cuidado en el proceso de reconocimiento de créditos por experiencia profesional, que se aplicará con un criterio restrictivo y una correlación clara entre experiencia y competencias reconocidas, para un desarrollo correcto y ordenado del nuevo escenario legal, y en el marco de las instrucciones emanadas Agencia Evaluadora tanto en los procesos de verificación como con vistas a los procesos de acreditación de los títulos.

El número máximo de créditos de los supuestos por experiencia profesional y/o títulos universitarios propios, no podrá ser superior, en su conjunto, al 15% del total de créditos que constituyen el plan de estudios, según el RD 861/2010.

No serán en ningún caso objeto de reconocimiento los estudios cursados en instituciones que no tengan el carácter oficialmente reconocido de Universidades o Centros de Enseñanza Superior o que, cursados en Centros con tal naturaleza, no tengan el carácter de estudios superiores, tales como los de formación permanente profesional o de extensión universitaria. Tampoco podrán ser objeto de reconocimiento los créditos correspondientes a los trabajos de fin de grado o fin de Master.

Procedimiento utilizado por la Universidad para reconocer los aprendizajes previos de los estudiantes en el proceso de admisión a las enseñanzas conducentes al título.

El reconocimiento de créditos deberá ser solicitado por el estudiante en el momento de formalizar su matrícula. El estudiante deberá asimismo abonar las tasas que se establezcan al efecto, y presentar en Secretaría de Cursos la siguiente documentación:

- Certificación Académica Personal (original o fotocopia compulsada) en la que conste la denominación de las materias, la tipologías de las mismas, el número de créditos ECTS y la calificación obtenida por el estudiante, y el programa detallado de las materias (original sellado o fotocopia compulsada) para el reconocimiento de asignaturas básica de la misma rama.

- En el caso de reconocimiento por experiencia laboral y/o laboral, deberán presentar la documentación que lo acredite.

La Comisión Académica de cada departamento estudiará con detalle la documentación aportada por el alumno, que dictará la oportuna resolución aceptando o denegando el reconocimiento y/o transferencia.

Todos los créditos obtenidos por el estudiante en enseñanzas oficiales cursadas en cualquier Universidad, los transferidos, los reconocidos y los superados para la obtención del correspondiente título, serán incluidos en su expediente académico y reflejados en el Suplemento Europeo al Título, caso de que sea solicitado.

El reconocimiento de los créditos en los supuestos por experiencia profesional y/o títulos propios no incorporará calificación de los mismos por lo que no computarán a efectos de baremación del expediente.

La Universidad regula e implementa el reconocimiento de créditos en los expedientes de los alumnos, basándose en la normativa legal vigente y en la propia interna que están reflejados en el ***¿PGA_1 Procedimiento para el reconocimiento y transferencia de créditos¿,*** aprobado por el Vicerrectorado de Ordenación Académica y disponibles en Red Nebrija y en el Portal del Alumno.

4.6 COMPLEMENTOS FORMATIVOS

~~4.6. Complementos de formación.~~

~~Los titulados con perfil de ingreso B y C, según han sido descritos en el epígrafe 4.1 deberán cursar complementos formativos.~~

~~Los perfiles de ingreso B y C, definidos en el punto 4.1 son los siguientes:~~

Perfil de ingreso B:

- Grado en tecnología industrial o titulación equivalente.
- Grado en edificación o titulación equivalente.
- Grado en matemáticas o titulación equivalente.
- Grado en física o titulación equivalente.
- Grado en estadística o titulación equivalente.

Para los titulados de perfil B los complementos formativos obligatorios serán 12 ECTS, y corresponden a las materias:

- Programación I
- Sistemas operativos

Perfil de ingreso C:

- Grado en Derecho
- Grado en Administración y dirección de empresas o titulación equivalente.
- Grado en seguridad
- Grado en criminología
- Grado en economía o titulación equivalente.
- Miembros de las Fuerzas y cuerpos de seguridad del Estado, dependiendo de la titulación de origen de sus candidatos o la equivalencia de la escala a la que pertenecen, que no correspondan al ya definido perfil A.

Para los titulados de perfil C los complementos formativos obligatorios serán 24 ECTS, y corresponden a las materias:

- Programación I
- Bases de datos
- Sistemas operativos
- Redes de ordenadores

Los complementos formativos para ambos perfiles corresponden a asignaturas del Grado en Ingeniería Informática por la Universidad Antonio de Nebrija.

Denominación materia	Programación I	**Unidad temporal**	Semestral	6 ECTS
Idioma de impartición de la materia: español				
Resultados de aprendizaje • Aplicar procedimientos algorítmicos básicos de las tecnologías informáticas. • Evaluar diferentes diseños de aplicaciones para seleccionar el más apropiado para resolver un problema. • Evaluar la estructura y arquitectura de los computadores, así como los componentes básicos que los conforman. • Aplicar los principios fundamentales y técnicas básicas de la programación paralela, concurrente, distribuida y de tiempo real.				
Contenidos Introducción a la Programación. Tipos e instrucciones. Procedimientos. Tipos de datos estructurados. Algoritmos de recorrido y búsqueda.				
Observaciones: • Requisitos previos: ninguno				
Competencias vinculadas a la materia CF1. Aplicar los conocimientos básicos sobre el uso y programación de los ordenadores, sistemas operativos, bases de datos y programas informáticos. CF2. Aplicar el conocimiento de la estructura, organización, funcionamiento e interconexión de los sistemas informáticos, los fundamentos de su pro-				

gramación, y su aplicación para la resolución de problemas. CF3. 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.

Actividades formativas: **Modalidad presencial** **CAF1. Clases teóricas**: Son sesiones presenciales en las que se utiliza la metodología de la lección magistral con apoyo, en su caso, de las herramientas informáticas adecuadas para la explicación de los conceptos teóricos y de las técnicas aplicables **CAF2. Tutorías:** Seguimiento personalizado del alumno a través de la resolución individual de dudas y problemas de la materia, así como del seguimiento de su participación activa en los trabajos en equipo. **CAF3. Trabajo personal del alumno (estudio individual y prácticas)**: Lectura y recensiones de artículos y trabajos de investigación de interés y actualidad. Lectura y resolución de casos prácticos. Organización de trabajos individuales y en equipo. **CAF4. Trabajo en equipo**: Los alumnos, organizados en equipos de trabajo, seleccionarán una idea y presentarán trabajos prácticos y originales **Modalidad semipresencial** **CAF5. Clases teóricas a distancia**: Los contenidos didácticos de la asignatura son posicionados en el Campus Virtual Avanzado, en el apartado de ¿Itinerarios formativos¿. Estos contenidos se ilustran con vídeos y gráficos que hacen más amena su lectura y su estudio por los alumnos. En el apartado ¿Documentación¿ se integran los mismos textos pero sin animaciones, para que los alumnos puedan imprimirlos, si así lo desean. Esto se completa con Tutorías con el profesor y por videoconferencia, en las horas y fechas establecidas. **CAF6. Tutorías a distancia**: Seguimiento personalizado del alumno aprovechando los recursos tecnológicos del Campus Virtual. **CAF3. Trabajo personal del alumno (estudio individual y prácticas)**: Lectura y recensiones de artículos y trabajos de investigación de interés y actualidad. Lectura y resolución de casos prácticos. Organización de trabajos individuales y en equipo. **CAF4. Trabajo en grupo**: Los alumnos, organizados en equipos de trabajo, seleccionarán una idea y presentarán trabajos prácticos y originales **Modalidad a distancia** **CAF5. Clases teóricas a distancia**: Los contenidos didácticos de la asignatura son posicionados en el Campus Virtual Avanzado, en el apartado de ¿Itinerarios formativos¿. Estos contenidos se ilustran con vídeos y gráficos que hacen más amena su lectura y su estudio por los alumnos. En el apartado ¿Documentación¿ se integran los mismos textos pero sin animaciones, para que los alumnos puedan imprimirlos, si así lo desean. Esto se completa con Tutorías con el profesor y por videoconferencia, en las horas y fechas establecidas. **CAF6. Tutorías a distancia**: Seguimiento personalizado del alumno aprovechando los recursos tecnológicos del Campus Virtual. **CAF3. Trabajo personal del alumno (estudio individual y prácticas)**: Lectura y recensiones de artículos y trabajos de investigación de interés y actualidad. Lectura y resolución de casos prácticos. Organización de trabajos individuales y en equipo. **CAF4. Trabajo en grupo**: Los alumnos, organizados en equipos de trabajo, seleccionarán una idea y presentarán trabajos prácticos y originales Modalidad Presencial:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
CAF1	43	100%
CAF2	13	100%
CAF3	77	0%
CAF4	17	0%

Modalidad Semipresencial:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
CAF5	43	0%
CAF6	13	0%
CAF3	79	0%
CAF4	15	0%

Modalidad a distancia:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
CAF5	43	0%
CAF6	13	0%
CAF3	81	0%
CAF4	13	0%

Metodologías docentes:

MD1	Método del Caso	Metodología centrada en la investigación del estudiante sobre un problema real y específico que ayuda al alumno a adquirir la base para un estudio inductivo (Bochrer, y Linsky, 1990). Parte de la definición de un caso concreto para que el alumno sea capaz de comprender, de conocer y de analizar todo el contexto y las variables que intervienen en el caso
MD2	Aprendizaje Cooperativo	Metodología basada en el trabajo en equipo de los estudiantes. Incluye técnicas en las que los alumnos trabajan con-

		juntamente para lograr determinados objetivos comunes de los que son responsables todos los miembros del equipo
MD3	Aprendizaje Basado en Problemas (ABP)	Metodología centrada en el aprendizaje, en la investigación y reflexión que siguen los alumnos para llegar a una solución o posibles soluciones, ante un problema planteado
MD4	Clase magistral	Metodología de enseñanza centrada en la transmisión de conocimientos por parte del docente. Exposición de contenidos ante los estudiantes, que tienen la oportunidad de preguntar.

Modalidad presencial: MD1; MD2; MD3; MD4 Modalidad semipresencial: MD1; MD2; MD3; MD4 Modalidad a distancia: MD1; MD2; MD3; MD4

Sistemas de evaluación: Modalidad Presencial: Para superar con éxito cualquier materia/asignatura, el alumno debe aprobar el examen final presencial. Esto es, en el examen final se debe alcanzar una calificación igual o superior a 5 en una escala de 0-10, siendo 0 la nota mínima y 10 la máxima.

Código	Sistema de Evaluación	Descripción
SE1	Desempeño en Trabajo individual	Desempeño del alumno en Trabajo individual en resolución de ejercicios
SE2	Desempeño en Trabajos grupales	Desempeño del alumno en Trabajos grupales en resolución de ejercicios
SE3	Prueba final presencial	Prueba final individual presencial

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	25	25
SE2	25	25
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad semipresencial Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	35	35
SE2	15	15
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad a distancia: Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	40	40
SE2	10	10
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

En todo caso, la superación de cualquier materia/asignatura, sin excepción, para las tres modalidades está supeditada a aprobar las pruebas finales presenciales correspondientes **Asignatura CF.1**

Denominación de la asignatura: Programación I				
Semestral	Créditos	6	Idioma	Español

Denominación materia	Bases de datos	**Unidad temporal**	Semestral	6 ECTS

Idioma de impartición de la materia: español

Resultados de aprendizaje

- Crear, operar y controlar una base de datos utilizando las herramientas propias del sistema gestor y los lenguajes correspondientes.
- Analizar los requisitos de los usuarios.

Contenidos Introducción a las bases de datos. Diseño Conceptual: Modelo entidad-relación. Diseño Lógico: Modelo Relacional. Algebra relacional. Vistas y disparadores. Transacciones y concurrencia. SQL: Structured Query Language.

Observaciones:

- Requisitos previos: ninguno

Competencias vinculadas a la materia CF4. Conocer y aplicar las características, funcionalidades y estructura de las bases de datos, que permitan su adecuado uso, y el diseño y el análisis e implementación de aplicaciones basadas en ellos.

Actividades formativas: **Modalidad presencial** **CAF1. Clases teóricas**: Son sesiones presenciales en las que se utiliza la metodología de la lección magistral con apoyo, en su caso, de las herramientas informáticas adecuadas para la explicación de los conceptos teóricos y de las técnicas aplicables **CAF2. Tutorías:** Seguimiento personalizado del alumno a través de la resolución individual de dudas y problemas de la materia, así como del seguimiento de su participación activa en los trabajos en equipo. **CAF3. Trabajo personal del alumno (estudio individual y prácticas)**: Lectura y recensiones de artículos y trabajos de investigación de interés y actualidad. Lectura y resolución de casos prácticos. Organización de trabajos individuales y en equipo. **CAF4. Trabajo en equipo**: Los alumnos, organizados en equipos de trabajo, seleccionarán una idea y presentarán trabajos prácticos y originales **Modalidad semipresencial** **CAF5. Clases teóricas a distancia**: Los contenidos didácticos de la asignatura son posicionados en el Campus Virtual Avanzado, en el apartado de ¿Itinerarios formativos¿. Estos contenidos se ilustran con vídeos y gráficos que hacen más amena su lectura y su estudio por los alumnos. En el apartado ¿Documentación¿ se integran los mismos textos pero sin animaciones, para que los alumnos puedan imprimirlos, si así lo desean. Esto se completa con Tutorías con el profesor y por videoconferencia, en las horas y fechas establecidas. **CAF6. Tutorías a distancia**: Seguimiento personalizado del alumno aprovechando los recursos tecnológicos del Campus Virtual. **CAF3. Trabajo personal del alumno (estudio individual y prácticas)**: Lectura y recensiones de artículos y trabajos de investigación de interés y actualidad. Lectura y resolución de casos prácticos. Organización de trabajos individuales y en equipo. **CAF4. Trabajo en grupo**: Los alumnos, organizados en equipos de trabajo, seleccionarán una idea y presentarán trabajos prácticos y originales **Modalidad a distancia** **CAF5. Clases teóricas a distancia**: Los contenidos didácticos de la asignatura son posicionados en el Campus Virtual Avanzado, en el apartado de ¿Itinerarios formativos¿. Estos contenidos se ilustran con vídeos y gráficos que hacen más amena su lectura y su estudio por los alumnos. En el apartado ¿Documentación¿ se integran los mismos textos pero sin animaciones, para que los alumnos puedan imprimirlos, si así lo desean. Esto se completa con Tutorías con el profesor y por videoconferencia, en las horas y fechas establecidas. **CAF6. Tutorías a distancia**: Seguimiento personalizado del alumno aprovechando los recursos tecnológicos del Campus Virtual. **CAF3. Trabajo personal del alumno (estudio individual y prácticas)**: Lectura y recensiones de artículos y trabajos de investigación de interés y actualidad. Lectura y resolución de casos prácticos. Organización de trabajos individuales y en equipo. **CAF4. Trabajo en grupo**: Los alumnos, organizados en equipos de trabajo, seleccionarán una idea y presentarán trabajos prácticos y originales Modalidad Presencial:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
CAF1	43	100%
CAF2	13	100%
CAF3	77	0%
CAF4	17	0%

Modalidad Semipresencial:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
CAF5	43	0%
CAF6	13	0%
CAF3	79	0%
CAF4	15	0%

Modalidad a distancia:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
CAF5	43	0%
CAF6	13	0%

CAF3	81	0%
CAF4	13	0%

Metodologías docentes:

MD1	Método del Caso	Metodología centrada en la investigación del estudiante sobre un problema real y específico que ayuda al alumno a adquirir la base para un estudio inductivo (Bochrer, y Linsky, 1990). Parte de la definición de un caso concreto para que el alumno sea capaz de comprender, de conocer y de analizar todo el contexto y las variables que intervienen en el caso
MD2	Aprendizaje Cooperativo	Metodología basada en el trabajo en equipo de los estudiantes. Incluye técnicas en las que los alumnos trabajan conjuntamente para lograr determinados objetivos comunes de los que son responsables todos los miembros del equipo
MD3	Aprendizaje Basado en Problemas (ABP)	Metodología centrada en el aprendizaje, en la investigación y reflexión que siguen los alumnos para llegar a una solución o posibles soluciones, ante un problema planteado
MD4	Clase magistral	Metodología de enseñanza centrada en la transmisión de conocimientos por parte del docente. Exposición de contenidos ante los estudiantes, que tienen la oportunidad de preguntar.

Modalidad presencial: MD1; MD2; MD3; MD4 Modalidad semipresencial: MD1; MD2; MD3; MD4 Modalidad a distancia: MD1; MD2; MD3; MD4

Sistemas de evaluación: Modalidad Presencial: Para superar con éxito cualquier materia/asignatura, el alumno debe aprobar el examen final presencial. Esto es, en el examen final se debe alcanzar una calificación igual o superior a 5 en una escala de 0-10, siendo 0 la nota mínima y 10 la máxima.

Código	Sistema de Evaluación	Descripción
SE1	Desempeño en Trabajo individual	Desempeño del alumno en Trabajo individual en resolución de ejercicios
SE2	Desempeño en Trabajos grupales	Desempeño del alumno en Trabajos grupales en resolución de ejercicios
SE3	Prueba final presencial	Prueba final individual presencial

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	25	25
SE2	25	25
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad semipresencial Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	35	35
SE2	15	15
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad a distancia: Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	40	40
SE2	10	10
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

En todo caso, la superación de cualquier materia/asignatura, sin excepción, para las tres modalidades está supeditada a aprobar las pruebas finales presenciales correspondientes **Asignatura CF.2**

Denominación de la asignatura: Bases de datos				
Semestral	Créditos	6	Idioma	Español

Denominación materia	Redes de ordenadores	Unidad temporal	Semestral	6 ECTS

Idioma de impartición de la materia: español

Resultados de aprendizaje

- Describir las características, funcionalidades y estructura de los sistemas basados en redes de computadores, incluidos los diferentes niveles del modelo de capas.
- Diseñar e implementar aplicaciones basadas en redes de computadores.
- Diseñar y gestionar redes de computadores.

Contenidos Introducción a las redes de paquetes. Conceptos de transmisión de datos. Medios de transmisión y tecnologías de nivel físico. La capa de enlace de datos. Acceso múltiple y redes de área local. Capa de red y protocolo IP. Servicios y protocolos básicos de red. Seguridad en redes.

Observaciones:

- Requisitos previos: ninguno

Competencias vinculadas a la materia CF5. Conocer, administrar y mantener sistemas, servicios y aplicaciones informáticas. CF6. Aplicar los conocimientos de las características, funcionalidades y estructura de los Sistemas Operativos y diseñar e implementar aplicaciones basadas en sus servicios. CF7. Conocer y aplicar las características, funcionalidades y estructura de los Sistemas Distribuidos, las Redes de Computadores e Internet y diseñar e implementar aplicaciones basadas en ellas.

Actividades formativas: **Modalidad presencial** **CAF1. Clases teóricas**: Son sesiones presenciales en las que se utiliza la metodología de la lección magistral con apoyo, en su caso, de las herramientas informáticas adecuadas para la explicación de los conceptos teóricos y de las técnicas aplicables **CAF2. Tutorías:** Seguimiento personalizado del alumno a través de la resolución individual de dudas y problemas de la materia, así como del seguimiento de su participación activa en los trabajos en equipo. **CAF3. Trabajo personal del alumno (estudio individual y prácticas)**: Lectura y recensiones de artículos y trabajos de investigación de interés y actualidad. Lectura y resolución de casos prácticos. Organización de trabajos individuales y en equipo. **CAF4. Trabajo en equipo**: Los alumnos, organizados en equipos de trabajo, seleccionarán una idea y presentarán trabajos prácticos y originales **Modalidad semipresencial** **CAF5. Clases teóricas a distancia**: Los contenidos didácticos de la asignatura son posicionados en el Campus Virtual Avanzado, en el apartado de ¿Itinerarios formativos¿. Estos contenidos se ilustran con vídeos y gráficos que hacen más amena su lectura y su estudio por los alumnos. En el apartado ¿Documentación¿ se integran los mismos textos pero sin animaciones, para que los alumnos puedan imprimirlos, si así lo desean. Esto se completa con Tutorías con el profesor y por videoconferencia, en las horas y fechas establecidas. **CAF6. Tutorías a distancia**: Seguimiento personalizado del alumno aprovechando los recursos tecnológicos del Campus Virtual. **CAF3. Trabajo personal del alumno (estudio individual y prácticas)**: Lectura y recensiones de artículos y trabajos de investigación de interés y actualidad. Lectura y resolución de casos prácticos. Organización de trabajos individuales y en equipo. **CAF4. Trabajo en grupo**: Los alumnos, organizados en equipos de trabajo, seleccionarán una idea y presentarán trabajos prácticos y originales **Modalidad a distancia** **CAF5. Clases teóricas a distancia**: Los contenidos didácticos de la asignatura son posicionados en el Campus Virtual Avanzado, en el apartado de ¿Itinerarios formativos¿. Estos contenidos se ilustran con vídeos y gráficos que hacen más amena su lectura y su estudio por los alumnos. En el apartado ¿Documentación¿ se integran los mismos textos pero sin animaciones, para que los alumnos puedan imprimirlos, si así lo desean. Esto se completa con Tutorías con el profesor y por videoconferencia, en las horas y fechas establecidas. **CAF6. Tutorías a distancia**: Seguimiento personalizado del alumno aprovechando los recursos tecnológicos del Campus Virtual. **CAF3. Trabajo personal del alumno (estudio individual y prácticas)**: Lectura y recensiones de artículos y trabajos de investigación de interés y actualidad. Lectura y resolución de casos prácticos. Organización de trabajos individuales y en equipo. **CAF4. Trabajo en grupo**: Los alumnos, organizados en equipos de trabajo, seleccionarán una idea y presentarán trabajos prácticos y originales Modalidad Presencial:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
CAF1	43	100%
CAF2	13	100%
CAF3	77	0%
CAF4	17	0%

Modalidad Semipresencial:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF

CAF5	43	0%
CAF6	13	0%
CAF3	79	0%
CAF4	15	0%

Modalidad a distancia:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
CAF5	43	0%
CAF6	13	0%
CAF3	81	0%
CAF4	13	0%

Metodologías docentes:

MD1	Método del Caso	Metodología centrada en la investigación del estudiante sobre un problema real y específico que ayuda al alumno a adquirir la base para un estudio inductivo (Bochrer, y Linsky, 1990). Parte de la definición de un caso concreto para que el alumno sea capaz de comprender, de conocer y de analizar todo el contexto y las variables que intervienen en el caso
MD2	Aprendizaje Cooperativo	Metodología basada en el trabajo en equipo de los estudiantes. Incluye técnicas en las que los alumnos trabajan conjuntamente para lograr determinados objetivos comunes de los que son responsables todos los miembros del equipo
MD3	Aprendizaje Basado en Problemas (ABP)	Metodología centrada en el aprendizaje, en la investigación y reflexión que siguen los alumnos para llegar a una solución o posibles soluciones, ante un problema planteado
MD4	Clase magistral	Metodología de enseñanza centrada en la transmisión de conocimientos por parte del docente. Exposición de contenidos ante los estudiantes, que tienen la oportunidad de preguntar.

Modalidad presencial: MD1; MD2; MD3; MD4 Modalidad semipresencial: MD1; MD2; MD3; MD4 Modalidad a distancia: MD1; MD2; MD3; MD4

Sistemas de evaluación: Modalidad Presencial: Para superar con éxito cualquier materia/asignatura, el alumno debe aprobar el examen final presencial. Esto es, en el examen final se debe alcanzar una calificación igual o superior a 5 en una escala de 0-10, siendo 0 la nota mínima y 10 la máxima.

Código	Sistema de Evaluación	Descripción
SE1	Desempeño en Trabajo individual	Desempeño del alumno en Trabajo individual en resolución de ejercicios
SE2	Desempeño en Trabajos grupales	Desempeño del alumno en Trabajos grupales en resolución de ejercicios
SE3	Prueba final presencial	Prueba final individual presencial

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	25	25
SE2	25	25
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad semipresencial Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	35	35
SE2	15	15
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad a distancia: Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	40	40
SE2	10	10
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

En todo caso, la superación de cualquier materia/asignatura, sin excepción, para las tres modalidades está supeditada a aprobar las pruebas finales presenciales correspondientes **Asignatura CF.3**

Denominación de la asignatura: Redes de ordenadores				
Semestral	Créditos	6	Idioma	Español

Denominación materia	Sistemas operativos	Unidad temporal	Semestral	6 ECTS

Idioma de impartición de la materia: español

Resultados de aprendizaje

- Describir las características, funcionalidades y estructura de los Sistemas Operativos.
- Definir los conceptos de concurrencia, así como el efecto del sistema operativo sobre el resto del sistema.
- Resumir los métodos de gestión de recursos de un Sistema Operativo.

Contenidos Gestión de Procesos (concepto, planificación, threads, sincronización y comunicación). Gestión de memoria. Gestión de Entrada / Salida. Gestión de Ficheros. Virtualización de SSOO. SSOO y dispositivos móviles. Seguridad en los SSOO. Prácticas de planificación, procesos/hilos y sincronización.

Observaciones:

- Requisitos previos: ninguno

Competencias vinculadas a la materia CF8. Conocer, administrar y mantener sistemas, servicios y aplicaciones informáticas. CF9. Aplicar los conocimientos de las características, funcionalidades y estructura de los Sistemas Operativos y diseñar e implementar aplicaciones basadas en sus servicios.

Actividades formativas: **Modalidad presencial** **CAF1. Clases teóricas**: Son sesiones presenciales en las que se utiliza la metodología de la lección magistral con apoyo, en su caso, de las herramientas informáticas adecuadas para la explicación de los conceptos teóricos y de las técnicas aplicables **CAF2. Tutorías:** Seguimiento personalizado del alumno a través de la resolución individual de dudas y problemas de la materia, así como del seguimiento de su participación activa en los trabajos en equipo. **CAF3. Trabajo personal del alumno (estudio individual y prácticas)**: Lectura y recensiones de artículos y trabajos de investigación de interés y actualidad. Lectura y resolución de casos prácticos. Organización de trabajos individuales y en equipo. **CAF4. Trabajo en equipo**: Los alumnos, organizados en equipos de trabajo, seleccionarán una idea y presentarán trabajos prácticos y originales **Modalidad semipresencial** **CAF5. Clases teóricas a distancia**: Los contenidos didácticos de la asignatura son posicionados en el Campus Virtual Avanzado, en el apartado de ¿Itinerarios formativos¿. Estos contenidos se ilustran con vídeos y gráficos que hacen más amena su lectura y su estudio por los alumnos. En el apartado ¿Documentación¿ se integran los mismos textos pero sin animaciones, para que los alumnos puedan imprimirlos, si así lo desean. Esto se completa con Tutorías con el profesor y por videoconferencia, en las horas y fechas establecidas. **CAF6. Tutorías a distancia**: Seguimiento personalizado del alumno aprovechando los recursos tecnológicos del Campus Virtual. **CAF3. Trabajo personal del alumno (estudio individual y prácticas)**: Lectura y recensiones de artículos y trabajos de investigación de interés y actualidad. Lectura y resolución de casos prácticos. Organización de trabajos individuales y en equipo. **CAF4. Trabajo en grupo**: Los alumnos, organizados en equipos de trabajo, seleccionarán una idea y presentarán trabajos prácticos y originales **Modalidad a distancia** **CAF5. Clases teóricas a distancia**: Los contenidos didácticos de la asignatura son posicionados en el Campus Virtual Avanzado, en el apartado de ¿Itinerarios formativos¿. Estos contenidos se ilustran con vídeos y gráficos que hacen más amena su lectura y su estudio por los alumnos. En el apartado ¿Documentación¿ se integran los mismos textos pero sin animaciones, para que los alumnos puedan imprimirlos, si así lo desean. Esto se completa con Tutorías con el profesor y por videoconferencia, en las horas y fechas establecidas. **CAF6. Tutorías a distancia**: Seguimiento personalizado del alumno aprovechando los recursos tecnológicos del Campus Virtual. **CAF3. Trabajo personal del alumno (estudio individual y prácticas)**: Lectura y recensiones de artículos y trabajos de investigación de interés y actualidad. Lectura y resolución de casos prácticos. Organización de trabajos individuales y en

equipo. **CAF4. Trabajo en grupo**: Los alumnos, organizados en equipos de trabajo, seleccionarán una idea y presentarán trabajos prácticos y originales Modalidad Presencial:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
CAF1	43	100%
CAF2	13	100%
CAF3	77	0%
CAF4	17	0%

Modalidad Semipresencial:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
CAF5	43	0%
CAF6	13	0%
CAF3	79	0%
CAF4	15	0%

Modalidad a distancia:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
CAF5	43	0%
CAF6	13	0%
CAF3	81	0%
CAF4	13	0%

Metodologías docentes:

MD1	Método del Caso	Metodología centrada en la investigación del estudiante sobre un problema real y específico que ayuda al alumno a adquirir la base para un estudio inductivo (Bochrer, y Linsky, 1990). Parte de la definición de un caso concreto para que el alumno sea capaz de comprender, de conocer y de analizar todo el contexto y las variables que intervienen en el caso
MD2	Aprendizaje Cooperativo	Metodología basada en el trabajo en equipo de los estudiantes. Incluye técnicas en las que los alumnos trabajan conjuntamente para lograr determinados objetivos comunes de los que son responsables todos los miembros del equipo
MD3	Aprendizaje Basado en Problemas (ABP)	Metodología centrada en el aprendizaje, en la investigación y reflexión que siguen los alumnos para llegar a una solución o posibles soluciones, ante un problema planteado
MD4	Clase magistral	Metodología de enseñanza centrada en la transmisión de conocimientos por parte del docente. Exposición de contenidos ante los estudiantes, que tienen la oportunidad de preguntar.

Modalidad presencial: MD1; MD2; MD3; MD4 Modalidad semipresencial: MD1; MD2; MD3; MD4 Modalidad a distancia: MD1; MD2; MD3; MD4

Sistemas de evaluación: Modalidad Presencial: Para superar con éxito cualquier materia/asignatura, el alumno debe aprobar el examen final presencial. Esto es, en el examen final se debe alcanzar una calificación igual o superior a 5 en una escala de 0-10, siendo 0 la nota mínima y 10 la máxima.

Código	Sistema de Evaluación	Descripción
SE1	Desempeño en Trabajo individual	Desempeño del alumno en Trabajo individual en resolución de ejercicios

SE2	Desempeño en Trabajos grupales	Desempeño del alumno en Trabajos grupales en resolución de ejercicios
SE3	Prueba final presencial	Prueba final individual presencial

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	25	25
SE2	25	25
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad semipresencial Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	35	35
SE2	15	15
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad a distancia: Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	40	40
SE2	10	10
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

En todo caso, la superación de cualquier materia/asignatura, sin excepción, para las tres modalidades está supeditada a aprobar las pruebas finales presenciales correspondientes **Asignatura CF.4**

Denominación de la asignatura: Sistemas operativos				
Semestral	Créditos	6	Idioma	Español

Descripción de los complementos formativos:

La Universidad ofrecerá estos complementos formativos en modalidad presencial, semipresencial y a distancia, atendiendo de esta forma a las exigencias de los alumnos que opten por las distintas modalidades del Máster. Estos complementos deberán ser cursados previamente al ingreso en el programa Máster y no forman parte del propio Máster ni pueden sustituir en caso alguno, materias o asignaturas del propio Máster Universitario Ciberdelincuencia.

5. PLANIFICACIÓN DE LAS ENSEÑANZAS

5.1 DESCRIPCIÓN DEL PLAN DE ESTUDIOS
Ver Apartado 5: Anexo 1.
5.2 ACTIVIDADES FORMATIVAS
Clase magistral y fundamentos teóricos
Explicación técnica para la resolución de casos relacionados con las asignaturas o materias
Tutoría
Trabajo individual del estudiante
Trabajo en grupo del estudiante
Puesta en común de resultados y procedimientos
Evaluación
5.3 METODOLOGÍAS DOCENTES
Método del Caso
Aprendizaje Cooperativo
Aprendizaje Basado en Problemas (ABP)
Clase magistral
5.4 SISTEMAS DE EVALUACIÓN
Desempeño del Trabajo individual
Desempeño del Trabajos grupales
Prueba final presencial
Informe de autoevaluación del alumno
Certificado empresarial e Informe de la empresa
Defensa ante tribunal
5.5 SIN NIVEL 1
NIVEL 2: CIBERSEGURIDAD Y AGENTES DE LA AMENAZA
5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Obligatoria
ECTS NIVEL 2	6

DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**

LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

Resultados de aprendizaje

- Sabrá detectar, en un tiempo fijado, un elevado porcentaje de las vulnerabilidades de un sistema en red dado.
- Explicar al menos una manera de introducirse en un sistema cuyas vulnerabilidades han sido detectadas.
- Justificar mediante informes razonados las vulnerabilidades encontradas y el procedimiento detallado que se seguiría para la intrusión.
- Explicar otras técnicas de ataque a un sistema que no sea susceptible de intrusión directa.
- Conocer el tipo de información y los mecanismos de defensa desplegados en un sistema, explicar el impacto de distintas amenazas e intrusiones y en especial de las fugas de información.

5.5.1.3 CONTENIDOS

Contenidos:

La asignatura de Ciberseguridad y agentes de la amenaza identifica los problemas relacionados con la gestión de sistemas informáticos de seguridad, Estructura y organización de modelos Organizativos de un centro de operaciones de ciberseguridad y diseño de planes de auditoría y Planes de seguridad, Normas ISO/IEC. Serie 27XXX, implantación de SGSI, grado de implantación de las normativas de seguridad, Planes de Continuidad. ISO/IEC 22301 y 71599, diseño de planes de seguridad proactivos, desarrollo de políticas de seguridad, despliegue de políticas de seguridad, Metodologías de Respuesta a Incidentes. CSIRTs, seguimiento de políticas de seguridad, autenticación, control de accesos, pruebas de conocimiento nulo y en general la Formación y Concienciación de los procesos y procedimientos para el Análisis de Vulnerabilidades y el estudio de los fallos de seguridad, gestión de memoria, mecanismos de protección de memoria, espacio de usuario y de sistema, Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, exploits locales, exploits remotos, alteraciones básicas, explotaciones de memoria, shellcodes, Estándares. UNE/ISO 31000 y 27005, Laboratorios de Evaluación. Acreditación, escalada de privilegios, integer overflow, manejo de las Metodologías y Herramientas, Magerit/Pilar, buffer overflow, heap overflow, Mitigación de Riesgos y Selección de Controles, inyección de código, protección de ejecutables y perfiles de protección

5.5.1.4 OBSERVACIONES

Observaciones:

- Requisitos previos: ninguno

Actividades formativas:

Modalidad Semipresencial:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	0%
AF2	10	0%
AF3	10	25%
AF4	53	0%
AF5	30	0%
AF6	10	50%
AF7	2	100%

Modalidad a distancia:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	0%
AF2	10	0%
AF3	10	0%
AF4	63	0%

AF5	20	0%
AF6	10	20%
AF7	2	100%

Metodologías docentes:

Modalidad semipresencial: MD1; MD2; MD3; MD4

Modalidad a distancia: MD1; MD2; MD3; MD4

Sistemas de evaluación:

Para superar con éxito cualquier materia/asignatura, el alumno debe aprobar el examen final presencial. Esto es, en el examen final se debe alcanzar una calificación igual o superior a 5 en una escala de 0-10, siendo 0 la nota mínima y 10 la máxima.

Modalidad Presencial:

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad semipresencial

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	25	25
SE2	25	25
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad a distancia:

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	25	25
SE2	25	25
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

En todo caso, la superación de cualquier materia/asignatura está supeditada a aprobar las pruebas finales presenciales e individuales correspondientes.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - El alumno debe adquirir aquellos conocimientos sobre recursos humanos que le permitan trabajar en un equipo de ciberdelincuencia

CG3 - El alumno debe dominar las técnicas de lucha contra la ciberdelincuencia suficientes en el ámbito de la ciberdelincuencia que le permitan obtener y analizar información, evaluar su relevancia y validez, sintetizarla y adaptarla al contexto.

CG4 - El alumno debe ser capaz de tratar situaciones complejas e impredecibles de forma sistemática y creativa, con juicio crítico, con información incompleta, asumiendo riesgos, tomando decisiones y comunicándolas a una audiencia profesional del ámbito de la ciberseguridad y ciberdelincuencia

CG8 - El alumno, en el ámbito de la actuación frente a la ciberdelincuencia, debe ser capaz de reconocer la necesidad del cambio y debe tener la habilidad necesaria para gestionarlo.

CG9 - El alumno debe ser capaz de actuar de forma autónoma en un marco de libertad responsable, en el ámbito de la actuación frente a la ciberdelincuencia.

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

CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

5.5.1.5.2 TRANSVERSALES

No existen datos

5.5.1.5.3 ESPECÍFICAS

CE4 - Ser capaz de aplicar las propiedades biométricas al área de seguridad informática y de las comunicaciones.

CE6 - Ser capaz de programar y analizar tareas en diversos lenguajes de programación en el área de seguridad informática y de las comunicaciones.

CE7 - Ser capaz de utilizar las herramientas científico técnicas para evaluar la fiabilidad y robustez de sistemas informáticos complejos, aplicado a la prevención de la ciberdelincuencia.

CE10 - Ser capaz de diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos, aplicado a la prevención de la ciberdelincuencia.

CE11 - Ser capaz de utilizar con destreza las principales herramientas de detección y clasificación de malware y de realizar ejercicios sencillos de ingeniería inversa en el contexto de la ciberseguridad

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Clase magistral y fundamentos teóricos	35	100
Explicación técnica para la resolución de casos relacionados con las asignaturas o materias	10	100
Tutoría	10	25
Trabajo individual del estudiante	45	0
Trabajo en grupo del estudiante	38	0

Puesta en común de resultados y procedimientos	10	100
Evaluación	2	100
5.5.1.7 METODOLOGÍAS DOCENTES		
Método del Caso		
Aprendizaje Cooperativo		
Aprendizaje Basado en Problemas (ABP)		
Clase magistral		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Desempeño del Trabajo individual	25.0	25.0
Desempeño del Trabajos grupales	25.0	25.0
Prueba final presencial	50.0	50.0
NIVEL 2: MARCO JURÍDICO: PROCESO PENAL, ASPECTOS TRANSVERSALES Y AGENTE ENCUBIERTO		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NO CONSTAN ELEMENTOS DE NIVEL 3		
5.5.1.2 RESULTADOS DE APRENDIZAJE		

Resultados de aprendizaje

- Adquirirá la correcta comprensión de los aspectos relacionados con la legislación reguladora en ciberseguridad y su ámbito de aplicación, y dimensiones de la seguridad de la información la protección de datos, los delitos informáticos y los análisis de riesgos legales, LOPD y Reglamento de desarrollo
- Podrá realizar y ejecutar informes y proyectos científicos y técnicos en cualquier ámbito territorial, relacionado con la ciberseguridad.

5.5.1.3 CONTENIDOS

Contenidos

Aspectos Legales y Regulatorios revisando la legislación que hace referencia a los diferentes aspectos relacionados con la información de carácter personal o que esté protegida mediante algún tipo de regulación. Otro aspecto importante es la legislación que regula el uso de internet y el uso de las aplicaciones relacionadas con la identidad digital, a la hora de desarrollar aplicaciones que utilicen tecnologías relacionadas, firma digital o factura electrónica. Los procedimientos judiciales de hoy día, en muchas ocasiones requieren investigar la información alrededor de los encausados que proporcionan los teléfonos móviles, ordenadores personales y el uso de aplicaciones en la red como son las redes sociales. Los equipos informáticos y

las aplicaciones que corren sobre los mismos generan, intercambian, procesan y almacenan información que puede estar sujeta a regulación, bien por tratarse de información personal, confidencial o con derechos de autor.

Esta información debe investigarse con las garantías necesarias para que sea válida como prueba en el proceso judicial, y para ello hay que conocer tanto información básica sobre los procedimientos judiciales como las metodologías y técnicas de análisis forense que garantizan la manipulación correcta de las evidencias digitales, observando la Normativa sobre identificación, Estudio genérico del marco legal vigente en materia de bienes y servicios informáticos, Introducción a la protección de la información, Aspectos éticos y legislación asociada a la privacidad, Legislación relacionada con el uso de las TIC: protección de datos personales, uso de Internet y identidad digital, centrado en aspectos clave tales como propiedad industrial e intelectual, agente encubierto, protección de datos o regulación de mercados.

Metodología para una gestión proactiva de los riesgos legales inherentes al desarrollo, implantación y despliegue de actividad informática, con especial atención a la industria del software, especialmente relevante en esta materia. Seguridad, privacidad y aspectos prácticos, Técnicas y herramientas de análisis forense sobre ordenadores personales, dispositivos móviles, aplicaciones telemáticas, Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, Métodos de tratamiento de las pruebas digitales en proceso judiciales y generación de informes periciales, Delitos Informáticos. Estudio de la legislación penal en materia de infracciones cuyo medio de comisión u objeto de la misma sean bienes o servicios informáticos, de tal manera que se permita su identificación, su denuncia y correspondiente seguimiento procesal. El módulo da una visión de conjunto sobre los aspectos legales y el marco jurídico institucional en relación a la seguridad informática, analizando y recomendando diversas estrategias en dicho ámbito.

5.5.1.4 OBSERVACIONES

Observaciones:

- Requisitos previos: ninguno

Actividades formativas:

Modalidad Semipresencial:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	0%
AF2	10	0%
AF3	10	25%
AF4	53	0%
AF5	30	0%
AF6	10	50%
AF7	2	100%

Modalidad a distancia:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	0%
AF2	10	0%
AF3	10	0%
AF4	68	0%
AF5	15	0%
AF6	10	20%
AF7	2	100%

Metodologías docentes:

Modalidad semipresencial: MD1; MD2; MD3; MD4

Modalidad a distancia: MD1; MD2; MD3; MD4

Sistemas de evaluación:

Para superar con éxito cualquier materia/asignatura, el alumno debe aprobar el examen final presencial. Esto es, en el examen final se debe alcanzar una calificación igual o superior a 5 en una escala de 0-10, siendo 0 la nota mínima y 10 la máxima.

Modalidad Presencial:

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad semipresencial

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	25	25
SE2	25	25
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad a distancia:

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	25	25
SE2	25	25
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

En todo caso, la superación de cualquier materia/asignatura está supeditada a aprobar las pruebas finales presenciales e individuales correspondientes.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG4 - El alumno debe ser capaz de tratar situaciones complejas e impredecibles de forma sistemática y creativa, con juicio crítico, con información incompleta, asumiendo riesgos, tomando decisiones y comunicándolas a una audiencia profesional del ámbito de la ciberseguridad y ciberdelincuencia
CG5 - El alumno debe ser capaz de comunicarse correctamente tanto oralmente como por escrito, utilizando la tecnología más actual, en el ámbito de la ciberseguridad y ciberdelincuencia.
CG6 - El alumno debe ser capaz de actuar de forma autónoma en la planificación e implementación de proyectos y decisiones sobre prevención y actuación frente a la ciberdelincuencia.
CG7 - El alumno debe ser capaz de desempeñar diferentes roles dentro de un equipo de la ciberseguridad y ciberdelincuencia, en particular el de líder.
CG10 - El alumno debe ser capaz de aportar valor a la empresa o institución mediante su creatividad y participación en la actuación frente a la ciberdelincuencia
CG11 - Capacidad para integrar en su actuación frente a la ciberdelincuencia, los valores y políticas de igualdad efectiva, especialmente entre mujeres y hombres y atención a la discapacidad.
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
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
5.5.1.5.2 TRANSVERSALES
No existen datos
5.5.1.5.3 ESPECÍFICAS
CE2 - Ser capaz de asesorar sobre el cumplimiento de la legislación reguladora de la protección de datos en materia de seguridad
CE3 - Ser capaz de planificar y aplicar medidas de prevención contra fraudes en comercio electrónico.
CE10 - Ser capaz de diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos, aplicado a la prevención de la ciberdelincuencia.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Clase magistral y fundamentos teóricos	35	100
Explicación técnica para la resolución de casos relacionados con las asignaturas o materias	10	100
Tutoría	10	25
Trabajo individual del estudiante	63	0
Trabajo en grupo del estudiante	20	0
Puesta en común de resultados y procedimientos	10	100
Evaluación	2	100

5.5.1.7 METODOLOGÍAS DOCENTES
Método del Caso
Aprendizaje Cooperativo
Aprendizaje Basado en Problemas (ABP)
Clase magistral
5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Desempeño del Trabajo individual	20.0	20.0
Desempeño del Trabajos grupales	30.0	30.0
Prueba final presencial	50.0	50.0

NIVEL 2: TALLER TECNOLÓGICO DE CIBERDELINCUENCIA		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NO CONSTAN ELEMENTOS DE NIVEL 3		

5.5.1.2 RESULTADOS DE APRENDIZAJE

Resultados de aprendizaje

- Detectar, en un tiempo fijado, un elevado porcentaje de las vulnerabilidades de un sistema en red proclive al ciberdelito.
- Explicar al menos una manera de introducirse en un sistema cuyas vulnerabilidades han sido detectadas.
- Justificar mediante informes razonados las vulnerabilidades encontradas y el procedimiento detallado que se seguiría para la intrusión.
- Explicar otras técnicas de ataque a un sistema que no sea susceptible de intrusión directa.
- Conocidas las dependencias entre los distintos servicios en red de un sistema, explicar cómo evolucionarían distintos ataques propuestos y cómo se verían afectadas las distintas partes y el total para cada uno de dichos ciberdelitos.
- Conocido el tipo de información y los mecanismos de defensa desplegados en un sistema, explicar el impacto de distintas amenazas e intrusiones y en especial de las fugas de información.
- Elegir con criterio la mejor herramienta de análisis en el proceso de investigación iniciado por las sospechas de presencia de malware con objeto de producir un ciberdelito.

5.5.1.3 CONTENIDOS

Contenidos

La expansión de Internet, de la Web y posteriormente de las plataformas móviles han dado lugar a un entorno donde muchos modelos de negocio,procesos y actividades cotidianas se han digitalizado. El auge de la informática móvil, que comenzó con los ordenadores portátiles y las agendas de bolsillo, y ha continuado recientemente hasta incluir los teléfonos móviles, se han ido integrando y cada vez en aplicaciones comerciales donde las bases de datos juegan un papel importante. Esto ha llevado al desarrollo de técnicas, métodos, herramientas y modelos específicos de la Ingeniería del Software que tienen en cuenta la forma de uso, los dispositivos y los protocolos particulares que utilizan. El uso de Internet hace posible interconectar ordenadores personales, servidores con información de empresas y organizaciones, sistemas de control de infraestructuras críticas, teléfonos móviles. Esta tendencia continuará con la evolución de paradigmas como IoT y Smart cities o redes vehiculares, creando nuevos entornos donde dispositivos como los electrodomésticos de casa, nuestro vehículo o los semáforos de las ciudades están también conectados a la red. Esto nos lleva a una sociedad fuertemente dependiente de las tecnologías de la información en donde se mueve un volumen importante de negocio. En este escenario se han replicado también los aspectos negativos de la sociedad como es la ciberdelincuencia, los Ciberataques y ciberactivismo. El objetivo de la asignatura es conocer los principales mecanismos de ataque a los sistemas y a la información que utilizan los delincuentes en la red y saber desplegar, configurar y desarrollar medidas de seguridad para defenderse contra estas amenazas, tales como analizar los distintos tipos de Ciberataques, ciberdelito, ciberespionaje, mediante la resolución y análisis de casos prácticos considerando siempre sus aspectos legales

5.5.1.4 OBSERVACIONES

Observaciones:

- Requisitos previos: ninguno

Actividades formativas:

Modalidad Semipresencial:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	0%
AF2	10	0%
AF3	10	25%
AF4	58	0%
AF5	25	0%
AF6	10	50%
AF7	2	100%

Modalidad a distancia:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	0%
AF2	10	0%
AF3	10	0%
AF4	35	0%
AF5	48	0%
AF6	10	20%
AF7	2	100%

Metodologías docentes:

Modalidad semipresencial: MD1; MD2; MD3; MD4

Modalidad a distancia: MD1; MD2; MD3; MD4

Sistemas de evaluación:

Para superar con éxito cualquier materia/asignatura, el alumno debe aprobar el examen final presencial. Esto es, en el examen final se debe alcanzar una calificación igual o superior a 5 en una escala de 0-10, siendo 0 la nota mínima y 10 la máxima.

Modalidad Presencial:

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad semipresencial

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	10	10
SE2	40	40
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad a distancia:

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	25	25
SE2	25	25
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

En todo caso, la superación de cualquier materia/asignatura está supeditada a aprobar las pruebas finales presenciales e individuales correspondientes.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG2 - El alumno debe ser capaz de entender cómo su profesión afecta a otros departamentos de la empresa o institución en el ámbito de la ciberdelincuencia.

CG3 - El alumno debe dominar las técnicas de lucha contra la ciberdelincuencia suficientes en el ámbito de la ciberdelincuencia que le permitan obtener y analizar información, evaluar su relevancia y validez, sintetizarla y adaptarla al contexto.

CG6 - El alumno debe ser capaz de actuar de forma autónoma en la planificación e implementación de proyectos y decisiones sobre prevención y actuación frente a la ciberdelincuencia.

CG7 - El alumno debe ser capaz de desempeñar diferentes roles dentro de un equipo de la ciberseguridad y ciberdelincuencia, en particular el de líder.

CG8 - El alumno, en el ámbito de la actuación frente a la ciberdelincuencia, debe ser capaz de reconocer la necesidad del cambio y debe tener la habilidad necesaria para gestionarlo.

CG10 - El alumno debe ser capaz de aportar valor a la empresa o institución mediante su creatividad y participación en la actuación frente a la ciberdelincuencia

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

CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
5.5.1.5.2 TRANSVERSALES
No existen datos
5.5.1.5.3 ESPECÍFICAS
CE1 - Ser capaz de analizar y desarrollar sistemas de seguridad web aplicado a la prevención de la ciberdelincuencia.
CE3 - Ser capaz de planificar y aplicar medidas de prevención contra fraudes en comercio electrónico.
CE4 - Ser capaz de aplicar las propiedades biométricas al área de seguridad informática y de las comunicaciones.
CE6 - Ser capaz de programar y analizar tareas en diversos lenguajes de programación en el área de seguridad informática y de las comunicaciones.
CE7 - Ser capaz de utilizar las herramientas científico técnicas para evaluar la fiabilidad y robustez de sistemas informáticos complejos, aplicado a la prevención de la ciberdelincuencia.
CE10 - Ser capaz de diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos, aplicado a la prevención de la ciberdelincuencia.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Clase magistral y fundamentos teóricos	35	100
Explicación técnica para la resolución de casos relacionados con las asignaturas o materias	10	100
Tutoría	10	25
Trabajo individual del estudiante	68	0
Trabajo en grupo del estudiante	15	0
Puesta en común de resultados y procedimientos	10	50
Evaluación	2	100

5.5.1.7 METODOLOGÍAS DOCENTES

Método del Caso
Aprendizaje Cooperativo
Aprendizaje Basado en Problemas (ABP)
Clase magistral

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Desempeño del Trabajo individual	25.0	25.0
Desempeño del Trabajos grupales	25.0	25.0
Prueba final presencial	50.0	50.0

NIVEL 2: GESTIÓN DE PROYECTOS DE INVESTIGACIÓN APLICADO A LA CIBERDELINCUENCIA

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Obligatoria
ECTS NIVEL 2	6

DESPLIEGUE TEMPORAL: Semestral

ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3

6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NO CONSTAN ELEMENTOS DE NIVEL 3		

5.5.1.2 RESULTADOS DE APRENDIZAJE

Resultados de aprendizaje

- La comprensión de los aspectos relacionados con el análisis de entornos atacados, la determinación y reproducción de vectores de ataque, la confidencialidad en bases de datos, la reducción del impacto de ataques en sistemas y la recuperación ante desastres y ataques.
- La comprensión de los aspectos relacionados con las distintas herramientas de seguridad, los mecanismos de seguridad, los informes técnicos de seguridad, los mecanismos criptográficos y los elementos involucrados en la investigación de un entorno de seguridad.
- Descubrir las causas que propiciaron un acceso no autorizado o un fallo total del sistema y el responsable de dicho incidente.

5.5.1.3 CONTENIDOS

Contenidos

Este módulo trata otro de los pilares de la seguridad informática. La seguridad de las aplicaciones que se están ejecutando en una infraestructura informática. Los errores en las aplicaciones online son un punto de entrada muy atractivo para los posibles atacantes y es necesario saber cuáles son las técnicas más avanzadas para su protección. Los principales ataques de intrusión en la red se deben a debilidades o errores en el desarrollo software que son aprovechados para atacar a los sistemas y a la información. Por este motivo es muy importante para una eficaz investigación durante la gestión de proyectos, donde los gestores deberán conocer las principales debilidades conocidas y que han sido utilizadas para atacar a los sistemas, y desde este punto aprender a gestionar un proyecto de forma segura aplicando técnicas de desarrollo que permitan especificar el comportamiento seguro del sistema y poder verificar dicho comportamiento. Un aspecto también relevante es saber incorporar mecanismos de seguridad que ayuden a controlar el acceso seguro a los datos que se manejan desde el software, tales como técnicas criptográficas y de control de acceso a los datos. Recuperación de información, adquisición de datos, metodología de análisis forense, investigación de datos, documentación de procesos, herramientas de recuperación de información, medidas reactivas, protección ante desastres, redundancia de sistemas de ficheros, sistemas de ficheros avanzados. Todos estos aspectos se estructurarán de buenas prácticas de gestión de proyectos seguros, Ingeniería del Software y en especial en gestión de riesgos legales y planificación y gestión de proyectos, Técnicas de diseño de software seguro, Técnicas de intrusión, Verificación de seguridad del software, Enumeración de las principales debilidades de software, Mecanismos de ataque por la ciberdelincuencia

5.5.1.4 OBSERVACIONES

Observaciones:

- Requisitos previos: ninguno

Actividades formativas:

Modalidad Semipresencial:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	0%
AF2	10	0%
AF3	10	25%
AF4	25	0%

AF5	58	0%
AF6	10	50%
AF7	2	100%

Modalidad a distancia:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	0%
AF2	10	0%
AF3	10	0%
AF4	35	0%
AF5	48	0%
AF6	10	20%
AF7	2	100%

Metodologías docentes:

Modalidad semipresencial: MD1; MD2; MD3; MD4

Modalidad a distancia: MD1; MD2; MD3; MD4

Sistemas de evaluación:

Para superar con éxito cualquier materia/asignatura, el alumno debe aprobar el examen final presencial. Esto es, en el examen final se debe alcanzar una calificación igual o superior a 5 en una escala de 0-10, siendo 0 la nota mínima y 10 la máxima.

Modalidad Presencial:

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad semipresencial

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	30	30
SE2	20	20
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50

SE2	0	0
SE3	50	50

Modalidad a distancia:

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	25	25
SE2	25	25
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

En todo caso, la superación de cualquier materia/asignatura está supeditada a aprobar las pruebas finales presenciales e individuales correspondientes.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - El alumno debe adquirir aquellos conocimientos sobre recursos humanos que le permitan trabajar en un equipo de ciberdelincuencia

CG3 - El alumno debe dominar las técnicas de lucha contra la ciberdelincuencia suficientes en el ámbito de la ciberdelincuencia que le permitan obtener y analizar información, evaluar su relevancia y validez, sintetizarla y adaptarla al contexto.

CG5 - El alumno debe ser capaz de comunicarse correctamente tanto oralmente como por escrito, utilizando la tecnología más actual, en el ámbito de la ciberseguridad y ciberdelincuencia.

CG8 - El alumno, en el ámbito de la actuación frente a la ciberdelincuencia, debe ser capaz de reconocer la necesidad del cambio y debe tener la habilidad necesaria para gestionarlo.

CG9 - El alumno debe ser capaz de actuar de forma autónoma en un marco de libertad responsable, en el ámbito de la actuación frente a la ciberdelincuencia.

CG11 - Capacidad para integrar en su actuación frente a la ciberdelincuencia, los valores y políticas de igualdad efectiva, especialmente entre mujeres y hombres y atención a la discapacidad.

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

CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

5.5.1.5.2 TRANSVERSALES

No existen datos

5.5.1.5.3 ESPECÍFICAS

CE5 - Ser capaz de distinguir los diferentes agentes implicados en seguridad informática, y saber asesorarlos de forma integrada permitiendo la colaboración con otros departamentos de la entidad.

CE6 - Ser capaz de programar y analizar tareas en diversos lenguajes de programación en el área de seguridad informática y de las comunicaciones.
CE7 - Ser capaz de utilizar las herramientas científico técnicas para evaluar la fiabilidad y robustez de sistemas informáticos complejos, aplicado a la prevención de la ciberdelincuencia.
CE10 - Ser capaz de diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos, aplicado a la prevención de la ciberdelincuencia.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Clase magistral y fundamentos teóricos	35	100
Explicación técnica para la resolución de casos relacionados con las asignaturas o materias	10	100
Tutoría	10	25
Trabajo individual del estudiante	25	0
Trabajo en grupo del estudiante	58	0
Puesta en común de resultados y procedimientos	10	50
Evaluación	2	100

5.5.1.7 METODOLOGÍAS DOCENTES

Método del Caso
Aprendizaje Cooperativo
Aprendizaje Basado en Problemas (ABP)
Clase magistral

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Desempeño del Trabajo individual	25.0	25.0
Desempeño del Trabajos grupales	25.0	25.0
Prueba final presencial	50.0	50.0

NIVEL 2: AUDITORÍA FORENSE DE LA CIBERDELINCUENCIA

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Obligatoria
ECTS NIVEL 2	6

DESPLIEGUE TEMPORAL: Semestral

ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**

LENGUAS EN LAS QUE SE IMPARTE

CASTELLANO	CATALÁN	EUSKERA
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No

ITALIANO	OTRAS
No	No
NO CONSTAN ELEMENTOS DE NIVEL 3	

5.5.1.2 RESULTADOS DE APRENDIZAJE

Resultados de aprendizaje

- Conocer e interpretar la normativa de centros de respuesta a incidentes de seguridad, seguridad en centros financieros, seguridad en infraestructuras de defensa y principales conceptos de auditoría de sistemas.
- Registrar todas las acciones realizadas por el usuario en el sistema recogiendo la mayor cantidad de parámetros posibles (contexto, cierres de sesión, intentos fallidos en la aplicación, solicitudes de recordatorio y cambios de contraseña, registro, cambios que un usuario realiza sobre los datos de la aplicación recogiendo la mayor cantidad de parámetros posibles. Incluye operaciones de alta, edición, eliminación y consulta de registros (contexto, registro, filtro, etc, validaciones incorrectas y filtros aplicados que eliminaron cadenas de inyección SQL y XSS..)
- Comprensión de los aspectos relacionados con el análisis de riesgos de seguridad, los mecanismos de protección, el diseño de planes de seguridad, los SGSI, y la auditoría de sistemas en entornos sensibles.

5.5.1.3 CONTENIDOS

Contenidos

Esta materia se centra en el estudio de los Sistemas de Gestión de la Seguridad que permitirán diseñar e implementar medidas y planes para mejorar la seguridad informática en una organización. Del mismo modo, se estudiarán las vulnerabilidades más utilizadas para desestabilizar sistemas informáticos permitiendo interrumpir su funcionamiento e incluso tomar control sobre ellos de forma no autorizada. El estudio se complementará con la auditoría de seguridad, Planes de auditoría, auditoría técnica y de certificación, tipos de auditorías, auditorías de SGSI, aspectos documentales, metodologías de auditoría, ejecución de auditorías, herramientas de auditoría, ISO 27000,eEstudio de los fallos de seguridad, gestión de memoria, mecanismos de protección de memoria, espacio de usuario y de sistema, exploits locales, exploits remotos, alteraciones básicas, explotaciones de memoria, shellcodes, escalada de privilegios, integer overflow, buffer overflow, heap overflow, desarrollo de políticas de seguridad,despliegue de políticas de seguridad, seguimiento de políticas de seguridad, autenticación, control de accesos, pruebas de conocimiento nulo, inyección de código, protección de ejecutables, estudio comparativo de auditorías, que servirá para comprender los procesos más avanzados utilizados en dicha disciplina.

5.5.1.4 OBSERVACIONES

Observaciones:

- Requisitos previos: ninguno

Actividades formativas:

Modalidad Semipresencial:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	0%
AF2	10	0%
AF3	10	25%
AF4	63	0%
AF5	20	0%
AF6	10	50%
AF7	2	100%

Modalidad a distancia:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	0%
AF2	10	0%

AF3	10	0%
AF4	53	0%
AF5	30	0%
AF6	10	20%
AF7	2	100%

Metodologías docentes:

Modalidad semipresencial: MD1; MD2; MD3; MD4

Modalidad a distancia: MD1; MD2; MD3; MD4

Sistemas de evaluación:

Para superar con éxito cualquier materia/asignatura, el alumno debe aprobar el examen final presencial. Esto es, en el examen final se debe alcanzar una calificación igual o superior a 5 en una escala de 0-10, siendo 0 la nota mínima y 10 la máxima.

Modalidad Presencial:

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad semipresencial

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	20	20
SE2	30	30
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad a distancia:

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	25	25
SE2	25	25
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %

SE1	50	50
SE2	0	0
SE3	50	50

En todo caso, la superación de cualquier materia/asignatura está supeditada a aprobar las pruebas finales presenciales e individuales correspondientes.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG2 - El alumno debe ser capaz de entender cómo su profesión afecta a otros departamentos de la empresa o institución en el ámbito de la ciberdelincuencia.

CG4 - El alumno debe ser capaz de tratar situaciones complejas e impredecibles de forma sistemática y creativa, con juicio crítico, con información incompleta, asumiendo riesgos, tomando decisiones y comunicándolas a una audiencia profesional del ámbito de la ciberseguridad y ciberdelincuencia

CG7 - El alumno debe ser capaz de desempeñar diferentes roles dentro de un equipo de la ciberseguridad y ciberdelincuencia, en particular el de líder.

CG11 - Capacidad para integrar en su actuación frente a la ciberdelincuencia, los valores y políticas de igualdad efectiva, especialmente entre mujeres y hombres y atención a la discapacidad.

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

CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

5.5.1.5.2 TRANSVERSALES

No existen datos

5.5.1.5.3 ESPECÍFICAS

CE1 - Ser capaz de analizar y desarrollar sistemas de seguridad web aplicado a la prevención de la ciberdelincuencia.

CE3 - Ser capaz de planificar y aplicar medidas de prevención contra fraudes en comercio electrónico.

CE4 - Ser capaz de aplicar las propiedades biométricas al área de seguridad informática y de las comunicaciones.

CE10 - Ser capaz de diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos, aplicado a la prevención de la ciberdelincuencia.

CE11 - Ser capaz de utilizar con destreza las principales herramientas de detección y clasificación de malware y de realizar ejercicios sencillos de ingeniería inversa en el contexto de la ciberseguridad

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Clase magistral y fundamentos teóricos	35	100
Explicación técnica para la resolución de casos relacionados con las asignaturas o materias	10	100
Tutoría	10	25
Trabajo individual del estudiante	53	0
Trabajo en grupo del estudiante	30	0
Puesta en común de resultados y procedimientos	10	100

Evaluación	2	100
5.5.1.7 METODOLOGÍAS DOCENTES		
Método del Caso		
Aprendizaje Cooperativo		
Aprendizaje Basado en Problemas (ABP)		
Clase magistral		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Desempeño del Trabajo individual	25.0	25.0
Desempeño del Trabajos grupales	25.0	25.0
Prueba final presencial	50.0	50.0
NIVEL 2: ENTORNO Y EQUIPO DE INVESTIGACIÓN DE CIBERDELINCUENCIA		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NO CONSTAN ELEMENTOS DE NIVEL 3		
5.5.1.2 RESULTADOS DE APRENDIZAJE		

Resultados de aprendizaje

- Elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática aplicados a la ciberdelincuencia e implementarlos y desarrollarlos mediante los métodos y procesos adecuados.
- Investigación de fraudes relacionados con la informática.
- Detectar evidencias de la debilidad de los sistemas de información con carácter preventivo y con carácter correctivo.
- Comprender y saber aplicar las técnicas y funciones de la investigación de los Sistemas de Información.

5.5.1.3 CONTENIDOS

Contenido

Los riesgos inherentes dentro de la actividad en los Sistemas de Información, la especialización de muchas empresas en el desarrollo de software, así como la gran inversión hecha en hardware y software, nos obligan cada vez más a maximizar el control y mejorar los procedimientos de investigación sobre estas tareas del departamento de investigación. El entorno de profesionales especializados en revisar el control y llevar a cabo un seguimiento de los estándares de procedimientos, estudiando y analizando los controles organizativos y operativos investigando y analizando los sistemas de aplicación que se están desarrollando o que ya están implantados sobre datos reales y resultados de los sistemas que se estén utilizando. Teniendo en cuenta la gran cantidad de aspectos que puede abarcar el control llevado a cabo por los equipos de investigación, es un proceso normal que exista un

equipo que se especialice en entornos o actividades que requieran conocimientos muy particulares sobre los distintos fenómenos de la ciberdelincuencia. Además de lo anterior, la investigación informática es una tarea fundamental como soporte técnico a procesos legales y de conformidad técnica y acreditación, debiéndose conocer sus aspectos específicos, sabiendo aplicar técnicas avanzadas de testing, validación y verificación del software, saber aplicar técnicas y métodos para asegurar la calidad y la seguridad de los sistemas informáticos

5.5.1.4 OBSERVACIONES

Observaciones:

- Requisitos previos: ninguno

Actividades formativas:

Modalidad Semipresencial:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	0%
AF2	10	0%
AF3	10	25%
AF4	63	0%
AF5	20	0%
AF	10	50%
AF7	2	100%

Modalidad a distancia:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	0%
AF2	10	0%
AF3	10	0%
AF4	43	0%
AF5	40	0%
AF6	10	20%
AF7	2	100%

Metodologías docentes:

Modalidad semipresencial: MD1; MD2; MD3; MD4

Modalidad a distancia: MD1; MD2; MD3; MD4

Sistemas de evaluación:

Para superar con éxito cualquier materia/asignatura, el alumno debe aprobar el examen final presencial. Esto es, en el examen final se debe alcanzar una calificación igual o superior a 5 en una escala de 0-10, siendo 0 la nota mínima y 10 la máxima.

Modalidad Presencial:

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad semipresencial

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	25	25
SE2	25	25
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad a distancia:

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	25	25
SE2	25	25
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

En todo caso, la superación de cualquier materia/asignatura está supeditada a aprobar las pruebas finales presenciales e individuales correspondientes.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG5 - El alumno debe ser capaz de comunicarse correctamente tanto oralmente como por escrito, utilizando la tecnología más actual, en el ámbito de la ciberseguridad y ciberdelincuencia.

CG7 - El alumno debe ser capaz de desempeñar diferentes roles dentro de un equipo de la ciberseguridad y ciberdelincuencia, en particular el de líder.

CG8 - El alumno, en el ámbito de la actuación frente a la ciberdelincuencia, debe ser capaz de reconocer la necesidad del cambio y debe tener la habilidad necesaria para gestionarlo.

CG10 - El alumno debe ser capaz de aportar valor a la empresa o institución mediante su creatividad y participación en la actuación frente a la ciberdelincuencia

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

CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
5.5.1.5.2 TRANSVERSALES
No existen datos
5.5.1.5.3 ESPECÍFICAS
CE1 - Ser capaz de analizar y desarrollar sistemas de seguridad web aplicado a la prevención de la ciberdelincuencia.
CE2 - Ser capaz de asesorar sobre el cumplimiento de la legislación reguladora de la protección de datos en materia de seguridad
CE3 - Ser capaz de planificar y aplicar medidas de prevención contra fraudes en comercio electrónico.
CE7 - Ser capaz de utilizar las herramientas científico técnicas para evaluar la fiabilidad y robustez de sistemas informáticos complejos, aplicado a la prevención de la ciberdelincuencia.
CE10 - Ser capaz de diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos, aplicado a la prevención de la ciberdelincuencia.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Clase magistral y fundamentos teóricos	35	100
Explicación técnica para la resolución de casos relacionados con las asignaturas o materias	10	100
Tutoría	10	25
Trabajo individual del estudiante	53	0
Trabajo en grupo del estudiante	30	0
Puesta en común de resultados y procedimientos	10	100
Evaluación	2	100

5.5.1.7 METODOLOGÍAS DOCENTES

Método del Caso
Aprendizaje Cooperativo
Aprendizaje Basado en Problemas (ABP)
Clase magistral

5.5.1.8 SISTEMAS DE EVALUACIÓN

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍNIMA	PONDERACIÓN MÁXIMA
Desempeño del Trabajo individual	25.0	25.0
Desempeño del Trabajos grupales	25.0	25.0
Prueba final presencial	50.0	50.0

NIVEL 2: METODOLOGÍA DE LA INVESTIGACIÓN POLICIAL APLIACADA A LA CIBERDELINCUENCIA (ITINERARIO POLICIAL)

5.5.1.1 Datos Básicos del Nivel 2

CARÁCTER	Optativa
ECTS NIVEL 2	6

DESPLIEGUE TEMPORAL: Semestral

ECTS Semestral 1	ECTS Semestral 2	ECTS Semestral 3
	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		
NO CONSTAN ELEMENTOS DE NIVEL 3		

5.5.1.2 RESULTADOS DE APRENDIZAJE

Resultados de aprendizaje

- Elaborar planes de intervención policial relacionados con el entorno de seguridad informática aplicados a la ciberdelincuencia e implementarlos y desarrollarlos mediante los métodos y procesos adecuados.
- Investigación de fraudes relacionados con la informática.
- Comprender y saber aplicar las técnicas y funciones de la investigación policial en los Sistemas de Información.

5.5.1.3 CONTENIDOS

Contenidos

El entorno de profesionales las fuerzas y cuerpos de seguridad del estado especializados en revisar el control y llevar a cabo un seguimiento de los estándares de procedimientos, estudiando y analizando los controles organizativos y operativos que formen parte de una investigación oficial. Teniendo en cuenta la gran cantidad de aspectos que puede abarcar el control llevado a cabo por los equipos de investigación las fuerzas y cuerpos de seguridad del estado, es un proceso normal que exista un equipo que se especialice en entornos o actividades que requieran conocimientos muy particulares sobre los distintos fenómenos de la ciberdelincuencia. Además de lo anterior, la investigación informática por parte del sector de las fuerzas y cuerpos de seguridad del estado es una tarea fundamental como soporte técnico a procesos legales y de conformidad técnica y acreditación, debiéndose conocer sus aspectos específicos, sabiendo aplicar técnicas avanzadas de testing, validación y verificación del software, saber aplicar técnicas y métodos para asegurar la calidad y la seguridad de los sistemas informáticos. Investigar y analizar los sistemas de aplicación que se están desarrollando o que ya están implantados. Realizar auditorías de datos reales y resultados de los sistemas que se estén utilizando. Realización de auditorías de seguridad. · Gobierno y Gestión de Servicios de TI. Normas ISO: 20000 y 38500. Análisis y evaluación de riesgos de seguridad, Gestión de políticas de seguridad, Estándares y modelos de gestión de la seguridad, Certificación de un sistema de gestión de la seguridad, Cloud Computing, Sistemas de Gestión de Contenidos, peculiaridades del Comercio Electrónico, y los Aspectos Éticos y Legales que deben regir en todas las actuaciones de las fuerzas y cuerpos de seguridad del estado.

5.5.1.4 OBSERVACIONES

Observaciones:

- Requisitos previos: ninguno

Actividades formativas:

Modalidad Semipresencial:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	0%
AF2	10	0%

AF3	10	25%
AF4	25	0%
AF5	58	0%
AF6	10	50%
AF7	2	100%

Modalidad a distancia:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	0%
AF2	10	0%
AF3	10	0%
AF4	35	0%
AF5	48	0%
AF6	10	20%
AF7	2	100%

Metodologías docentes:

Modalidad semipresencial: MD1; MD2; MD3; MD4

Modalidad a distancia: MD1; MD2; MD3; MD4

Sistemas de evaluación:

Para superar con éxito cualquier materia/asignatura, el alumno debe aprobar el examen final presencial. Esto es, en el examen final se debe alcanzar una calificación igual o superior a 5 en una escala de 0-10, siendo 0 la nota mínima y 10 la máxima.

Modalidad Presencial:

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad semipresencial

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	25	25
SE2	25	25
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad a distancia:

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	35	35
SE2	15	15
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

En todo caso, la superación de cualquier materia/asignatura está supeditada a aprobar las pruebas finales presenciales e individuales correspondientes.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG3 - El alumno debe dominar las técnicas de lucha contra la ciberdelincuencia suficientes en el ámbito de la ciberdelincuencia que le permitan obtener y analizar información, evaluar su relevancia y validez, sintetizarla y adaptarla al contexto.

CG6 - El alumno debe ser capaz de actuar de forma autónoma en la planificación e implementación de proyectos y decisiones sobre prevención y actuación frente a la ciberdelincuencia.

CG8 - El alumno, en el ámbito de la actuación frente a la ciberdelincuencia, debe ser capaz de reconocer la necesidad del cambio y debe tener la habilidad necesaria para gestionarlo.

CG10 - El alumno debe ser capaz de aportar valor a la empresa o institución mediante su creatividad y participación en la actuación frente a la ciberdelincuencia

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

CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

5.5.1.5.2 TRANSVERSALES

No existen datos

5.5.1.5.3 ESPECÍFICAS

CE1 - Ser capaz de analizar y desarrollar sistemas de seguridad web aplicado a la prevención de la ciberdelincuencia.

CE3 - Ser capaz de planificar y aplicar medidas de prevención contra fraudes en comercio electrónico.

CE4 - Ser capaz de aplicar las propiedades biométricas al área de seguridad informática y de las comunicaciones.		
CE10 - Ser capaz de diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos, aplicado a la prevención de la ciberdelincuencia.		
CE11 - Ser capaz de utilizar con destreza las principales herramientas de detección y clasificación de malware y de realizar ejercicios sencillos de ingeniería inversa en el contexto de la ciberseguridad		
5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	**HORAS**	**PRESENCIALIDAD**
Clase magistral y fundamentos teóricos	35	100
Explicación técnica para la resolución de casos relacionados con las asignaturas o materias	10	100
Tutoría	10	25
Trabajo individual del estudiante	53	0
Trabajo en grupo del estudiante	30	0
Puesta en común de resultados y procedimientos	10	100
Evaluación	2	100
5.5.1.7 METODOLOGÍAS DOCENTES		
Método del Caso		
Aprendizaje Cooperativo		
Aprendizaje Basado en Problemas (ABP)		
Clase magistral		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Desempeño del Trabajo individual	15.0	15.0
Desempeño del Trabajos grupales	35.0	35.0
Prueba final presencial	50.0	50.0
NIVEL 2: CIBERTERRORISMO (ITINERARIO POLICIAL)		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	

No	No

LISTADO DE ESPECIALIDADES

No existen datos

NO CONSTAN ELEMENTOS DE NIVEL 3

5.5.1.2 RESULTADOS DE APRENDIZAJE

Resultados de aprendizaje

- Elaborar planes de intervención policial relacionados con el entorno de seguridad informática dentro del Esquema Nacional de seguridad e infraestructuras críticas, aplicados a la Ciberterrorismo y la ciberdelincuencia.
- Saber incorporar en las aplicaciones mecanismos de seguridad que ayuden a controlar el acceso seguro a los datos que se manejan desde el software, tales como técnicas criptográficas y de control de acceso a los datos.
- Comprender y saber aplicar las técnicas y funciones de la investigación policial en los Sistemas de Información, conociendo los mecanismos de ataque por el Ciberterrorismo y la ciberdelincuencia.

5.5.1.3 CONTENIDOS

Contenidos

El uso de Internet hace posible interconectar ordenadores personales, servidores con información de empresas y organizaciones, sistemas de control de infraestructuras críticas, teléfonos móviles. Esto nos lleva a una sociedad fuertemente dependiente de las tecnologías de la información. En este escenario se han replicado también los aspectos negativos de la sociedad como representa el Ciberterrorismo. El objetivo de la asignatura es conocer los principales mecanismos de ataque a los sistemas y a la información que utilizan los ciberterroristas en la red y saber desplegar, configurar y desarrollar medidas de seguridad para defenderse contra estas amenazas. Las fuerzas y cuerpos de seguridad del estado son las encargadas de observar y responder de los operativos que formen parte de una investigación oficial contra el Ciberterrorismo. Teniendo en cuenta la gran cantidad de aspectos que puede abarcar el control llevado a cabo por los equipos de investigación las fuerzas y cuerpos de seguridad del estado, es un proceso normal que exista un equipo que se especialice en entornos o actividades que requieran conocimientos muy particulares sobre los distintos fenómenos del Ciberterrorismo. Además de lo anterior, la investigación informática por parte del sector de las fuerzas y cuerpos de seguridad del estado es una tarea fundamental como soporte técnico a procesos legales y de conformidad técnica y acreditación, debiéndose conocer sus aspectos específicos, sabiendo aplicar técnicas avanzadas de testing, validación y verificación del software, saber aplicar técnicas y métodos para asegurar la calidad y la seguridad de los sistemas informáticos. Investigar y analizar los sistemas de aplicación que se están desarrollando o que ya están implantados. Realizar auditorías de datos reales y resultados de los sistemas que se estén utilizando. Realización de auditorías de seguridad. Gobierno y Gestión de Servicios de TI, Análisis y evaluación de riesgos de seguridad, Gestión de políticas de seguridad, Esquema Nacional de seguridad e infraestructuras críticas, Ciberterrorismo y ciberdelincuencia, Mecanismos de ataque, Protección de infraestructuras TIC. Infraestructuras Críticas, Supervisión de la seguridad, Reacción en casos de ataques de Ciberterrorismo, Análisis forense y los Aspectos Éticos y Legales que deben regir en todas las actuaciones de las fuerzas y cuerpos de seguridad del estado.

5.5.1.4 OBSERVACIONES

Observaciones:

- Requisitos previos: ninguno

Actividades formativas:

Modalidad Semipresencial:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	0%
AF2	10	0%
AF3	10	25%
AF4	58	0%
AF5	25	0%
AF6	10	50%
AF7	2	100

Modalidad a distancia:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF

AF1	35	0%
AF2	10	0%
AF3	10	0%
AF4	35	0%
AF5	48	0%
AF6	10	20%
AF7	2	100%

Metodologías docentes:

Modalidad semipresencial: MD1; MD2; MD3; MD4

Modalidad a distancia: MD1; MD2; MD3; MD4

Sistemas de evaluación:

Para superar con éxito cualquier materia/asignatura, el alumno debe aprobar el examen final presencial. Esto es, en el examen final se debe alcanzar una calificación igual o superior a 5 en una escala de 0-10, siendo 0 la nota mínima y 10 la máxima.

Modalidad Presencial:

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad semipresencial

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	25	25
SE2	25	25
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad a distancia:

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	25	25
SE2	25	25
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

En todo caso, la superación de cualquier materia/asignatura está supeditada a aprobar las pruebas finales presenciales e individuales correspondientes.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG4 - El alumno debe ser capaz de tratar situaciones complejas e impredecibles de forma sistemática y creativa, con juicio crítico, con información incompleta, asumiendo riesgos, tomando decisiones y comunicándolas a una audiencia profesional del ámbito de la ciberseguridad y ciberdelincuencia

CG5 - El alumno debe ser capaz de comunicarse correctamente tanto oralmente como por escrito, utilizando la tecnología más actual, en el ámbito de la ciberseguridad y ciberdelincuencia.

CG9 - El alumno debe ser capaz de actuar de forma autónoma en un marco de libertad responsable, en el ámbito de la actuación frente a la ciberdelincuencia.

CG11 - Capacidad para integrar en su actuación frente a la ciberdelincuencia, los valores y políticas de igualdad efectiva, especialmente entre mujeres y hombres y atención a la discapacidad.

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

CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

5.5.1.5.2 TRANSVERSALES

No existen datos

5.5.1.5.3 ESPECÍFICAS

CE5 - Ser capaz de distinguir los diferentes agentes implicados en seguridad informática, y saber asesorarlos de forma integrada permitiendo la colaboración con otros departamentos de la entidad.

CE10 - Ser capaz de diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos, aplicado a la prevención de la ciberdelincuencia.

CE11 - Ser capaz de utilizar con destreza las principales herramientas de detección y clasificación de malware y de realizar ejercicios sencillos de ingeniería inversa en el contexto de la ciberseguridad

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Clase magistral y fundamentos teóricos	35	100
Explicación técnica para la resolución de casos relacionados con las asignaturas o materias	10	100
Tutoría	10	25
Trabajo individual del estudiante	53	0
Trabajo en grupo del estudiante	30	0

Puesta en común de resultados y procedimientos	10	100
Evaluación	2	100
5.5.1.7 METODOLOGÍAS DOCENTES		
Método del Caso		
Aprendizaje Cooperativo		
Aprendizaje Basado en Problemas (ABP)		
Clase magistral		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Desempeño del Trabajo individual	40.0	40.0
Desempeño del Trabajos grupales	10.0	10.0
Prueba final presencial	50.0	50.0
NIVEL 2: COMPLIANCE: PREVENCIÓN DE DELITOS EMPRESARIALES(ITINERARIO EMPRESARIAL)		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		
NO CONSTAN ELEMENTOS DE NIVEL 3		
5.5.1.2 RESULTADOS DE APRENDIZAJE		

Resultados de aprendizaje

- Saber programar aplicaciones web utilizando algunas tecnologías de desarrollo Web actuales: frameworks de amplia difusión y programación Asíncrona, particularmente en tareas de investigación, desarrollo e innovación en todos los ámbitos relacionados con la empresa.
- Saber incorporar en las aplicaciones mecanismos de seguridad que ayuden a controlar el acceso seguro a los datos que se manejan desde el software, tales como técnicas criptográficas y de control de acceso a los datos.
- Comprender y saber analizar las innovaciones en los aspectos sociales de la Web que pueden llevar a la creación de nuevas empresas y proteger estas de los ciberdelitos.
- Capacidad para la dirección general, dirección técnica y dirección de proyectos de investigación, desarrollo e innovación y prevención de delitos, en empresas y centros tecnológicos, desde el ámbito de la ciberseguridad.

5.5.1.3 CONTENIDOS

Contenidos

La reforma del Código Penal del año 2010, que introdujo en nuestro ordenamiento la responsabilidad penal de las personas jurídicas. Las personas jurídicas se convierten en penalmente responsables de los delitos cometidos en su nombre o por su cuenta por sus representantes legales y administradores, pero también, por quienes estando sometidos a su autoridad hayan podido realizar los hechos por no haberse ejercido sobre ellos el debido control. Con esta reforma una empresa no sólo debía enfrentarse a las sanciones, generalmente de gran importancia económica, que las distintas regulaciones sectoriales establecen, sino que también debía enfrentarse a la responsabilidad por un delito.Recientemente se introdujo una modificación al respecto de esta responsabilidad penal, en virtud de la cual la persona jurídica quedará exenta de responsabilidad cuando haya adoptado y ejecutado, antes de la comisión del delito, medidas de vigilancia y control idóneas para prevenir delitos de la misma naturaleza o reducir de forma significativa el riesgo de su comisión; la supervisión de esas medidas quede encomendada a un órgano interno con una cierta autonomía (salvo en el caso de las pequeñas empresas); el delito se haya cometido eludiendo por los autores tales medidas; y no se haya producido una omisión o un ejercicio insuficiente de las funciones de control. Esta reforma es clave para el sector del compliance, pues se convierte en algo prácticamente obligatorio para poder eludir la responsabilidad penal que pudiera producirse. Y no es extraña la introducción de esta reforma, pues en muchos casos la comisión del delito escapa de la posibilidad de control del representante de la empresa, especialmente en entidades de gran tamaño, por lo que es acertado que el juez pueda valorar que se tomaron unas medidas diligentes para evitarlo y, de esa forma, exonerar la responsabilidad. Contribuye, en definitiva, a aumentar la seguridad jurídica y, al mismo tiempo, potenciará que las empresas adopten sistemas de control que se extenderán a otros ámbitos de riesgo además del penal.

El compliance o cumplimiento normativo consiste en establecer las políticas y procedimientos adecuados y suficientes para garantizar que una empresa, incluidos sus directivos, empleados y agentes vinculados, cumplen con el marco normativo aplicable. Dentro del marco normativo no han de considerarse únicamente las normas legales, como leyes y reglamentos, sino que también deberían incluirse en el mismo las políticas internas, los compromisos con clientes, proveedores o terceros, y especialmente los códigos éticos que la empresa se haya comprometido a respetar, pues existen multitud de casos en los que una actuación puede ser legal pero no ética. Esta función es llevada a cabo mediante cinco conjuntos de actuaciones, que han de coordinarse entre sí y planearse cuidadosamente:

1. Identificación: se han de identificar los riesgos a los que se enfrenta la empresa, teniendo en cuenta su severidad e impacto y la probabilidad de que se den.
2. Prevención: conociendo los riesgos, se debe diseñar e implementar procedimientos de control que protejan a la empresa.
3. Monitorización y detección: la efectividad de los controles implementados debe ser supervisada, informando a la dirección de la exposición de la empresa a los riesgos, y realizando las auditorías periódicas que sean precisas.
4. Resolución: cuando pese a todo surge algún problema de cumplimiento, debe trabajarse para su solución.
5. Asesoramiento: los directivos y trabajadores deben recibir toda la información necesaria para llevar a cabo su trabajo de acuerdo con la normativa vigente.

Tradicionalmente, estas funciones recaían en los departamentos de asesoría jurídica, al menos a nivel general. Pero debido a la mayor complejidad regulatoria han surgido personas que se especializan en esta función, ya sea desde dentro de la empresa como asesor *in-house*, o bien como parte de compañías especializadas en *compliance*. Por otro lado, la competitividad de las empresas en el sector TIC depende cada vez más de su capacidad de adaptación e innovación, cambiando al ritmo de las tecnologías, por lo que entender la innovación, sus procesos y la relación con las personas es esencial en este ámbito. El alumno entenderá las oportunidades de Internet, de la Web y de la ubicuidad desde el punto de vista de la transformación de negocio o la creación de nuevos modelos de negocio. Gestión de personas y dirección. Procesos de calidad, mejora continua y gestión de riesgos. Detectará evidencias de la debilidad de los sistemas de información con carácter preventivo y con carácter correctivo. La seguridad de la información en las organizaciones, sus aspectos técnicos, procedimentales y económicos relacionados con la seguridad de la información, Consultoría y Auditorías de seguridad, aplicara las técnicas y funciones de la auditoría de los Sistemas de Información, utilizara técnicas y métodos de gestión de equipos de trabajo, Sabrá aplicar y llevar a la práctica un proceso de "lean startup" para llegar a un concepto y modelo de empresa basada en tecnología Web, Entendera el papel del informático en las empresas basadas en tecnología.

5.5.1.4 OBSERVACIONES

Observaciones:

- Requisitos previos: ninguno

Actividades formativas:

Modalidad Semipresencial:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	0%
AF2	10	0%
AF3	10	25%
AF4	53	0%
AF5	30	0%
AF6	10	50%
AF7	2	100%

Modalidad a distancia:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	0%
AF2	10	0%
AF3	10	0%
AF4	63	0%
AF5	20	0%
AF6	10	20%
AF7	2	100%

Metodologías docentes:

Modalidad semipresencial: MD1; MD2; MD3; MD4

Modalidad a distancia: MD1; MD2; MD3; MD4

Sistemas de evaluación:

Para superar con éxito cualquier materia/asignatura, el alumno debe aprobar el examen final presencial. Esto es, en el examen final se debe alcanzar una calificación igual o superior a 5 en una escala de 0-10, siendo 0 la nota mínima y 10 la máxima.

Modalidad Presencial:

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad semipresencial

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	25	25
SE2	25	25
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad a distancia:

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	25	25

SE2	25	25
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

En todo caso, la superación de cualquier materia/asignatura está supeditada a aprobar las pruebas finales presenciales e individuales correspondientes.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG2 - El alumno debe ser capaz de entender cómo su profesión afecta a otros departamentos de la empresa o institución en el ámbito de la ciberdelincuencia.

CG4 - El alumno debe ser capaz de tratar situaciones complejas e impredecibles de forma sistemática y creativa, con juicio crítico, con información incompleta, asumiendo riesgos, tomando decisiones y comunicándolas a una audiencia profesional del ámbito de la ciberseguridad y ciberdelincuencia

CG8 - El alumno, en el ámbito de la actuación frente a la ciberdelincuencia, debe ser capaz de reconocer la necesidad del cambio y debe tener la habilidad necesaria para gestionarlo.

CG9 - El alumno debe ser capaz de actuar de forma autónoma en un marco de libertad responsable, en el ámbito de la actuación frente a la ciberdelincuencia.

CG10 - El alumno debe ser capaz de aportar valor a la empresa o institución mediante su creatividad y participación en la actuación frente a la ciberdelincuencia

CG11 - Capacidad para integrar en su actuación frente a la ciberdelincuencia, los valores y políticas de igualdad efectiva, especialmente entre mujeres y hombres y atención a la discapacidad.

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

CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

5.5.1.5.2 TRANSVERSALES

No existen datos

5.5.1.5.3 ESPECÍFICAS

CE2 - Ser capaz de asesorar sobre el cumplimiento de la legislación reguladora de la protección de datos en materia de seguridad

CE3 - Ser capaz de planificar y aplicar medidas de prevención contra fraudes en comercio electrónico.

CE10 - Ser capaz de diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos, aplicado a la prevención de la ciberdelincuencia.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Clase magistral y fundamentos teóricos	35	100

Explicación técnica para la resolución de casos relacionados con las asignaturas o materias	10	100
Tutoría	10	25
Trabajo individual del estudiante	40	0
Trabajo en grupo del estudiante	43	0
Puesta en común de resultados y procedimientos	10	100
Evaluación	2	100
5.5.1.7 METODOLOGÍAS DOCENTES		
Método del Caso		
Aprendizaje Cooperativo		
Aprendizaje Basado en Problemas (ABP)		
Clase magistral		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Desempeño del Trabajo individual	25.0	25.0
Desempeño del Trabajos grupales	25.0	25.0
Prueba final presencial	50.0	50.0
NIVEL 2: RESPONSABILIDAD SOCIAL CORPORATIVA, REPUTACIÓN (ITINERARIO EMPRESARIAL)		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		
NO CONSTAN ELEMENTOS DE NIVEL 3		
5.5.1.2 RESULTADOS DE APRENDIZAJE		
Resultados de aprendizaje		

- Conocimiento, seguimiento y "control" de toda la información que afecta a su persona, empresa o marca forma parte de lo que se denomina ¿Online Reputación Management¿, o Gestión de Reputación Online.
- Comprender y saber analizar las innovaciones en los aspectos sociales de la Web que pueden llevar a la creación de nuevas empresas y proteger estas de los ciberdelitos.
- Capacidad para la dirección general, dirección técnica y dirección de proyectos de investigación, desarrollo e innovación en empresas y centros tecnológicos, desde el ámbito de la ciberseguridad.

5.5.1.3 CONTENIDOS

Contenidos

La construcción de una marca tiene unos inmensos costes en publicidad y marketing, y un proceso complejo de creación de campañas publicitarias y de comunicación en medios de todo tipo. En este contexto, Internet y las nuevas plataformas de participación social han dado nuevas y modernas herramientas al internauta para opinar, informar y comunicar. El aumento e importancia de este tipo de espacios ha convertido Internet en una plataforma de libertad de expresión sin competencia ni limitaciones, y ello ha supuesto un gran avance para todos. Sin embargo, su uso no siempre es el adecuado o, por lo menos, puede en muchas ocasiones no coincidir con los intereses personales o empresariales de las personas implicadas en informaciones aparecidas en la red. Las opiniones, por ejemplo, son un arma muy poderosa de promoción empresarial cuando son positivas, pero nefastas cuando son negativas. En este segundo caso, hay que poner remedio cuanto antes para contrarrestar las informaciones negativas con el fin de que desaparezcan de la red o, en todo caso, no ocupen posiciones relevantes en los buscadores con el fin de mitigar sus efectos adversos. La Reputación Online es el reflejo del prestigio de una persona, empresa o marca en Internet, creada no solo por la misma, sino también por el resto de personas que intercambian información y opiniones sobre ella en Internet a través de foros, blogs o redes sociales. La Gestión de la Reputación Online va desde la recopilación de toda la información relacionada, pasando por su seguimiento, con criterio de si afecta o no negativamente a la "reputación" e "imagen" de la persona, empresa o marca, pero, además, de su gestión o "control", es decir, de influir sobre dichos contenidos que perjudican a nuestra marca. Una de las maneras más fiables para luchar contra la reputación online negativa es el marketing de contenidos. la creación de contenido online positivo y de calidad contribuirá a paliar posibles consecuencias negativas derivadas de ataques contra tu marca.

5.5.1.4 OBSERVACIONES

Observaciones:

- Requisitos previos: ninguno

Actividades formativas:

Modalidad Semipresencial:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	0%
AF2	10	0%
AF3	10	25%
AF4	58	0%
AF5	25	0%
AF6	10	50%
AF7	2	100%

Modalidad a distancia:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	0%
AF2	10	0%
AF3	10	0%
AF4	35	0%
AF5	48	0%
AF6	10	20%

AF7	2	100%

Metodologías docentes:

Modalidad semipresencial: MD1; MD2; MD3; MD4

Modalidad a distancia: MD1; MD2; MD3; MD4

Sistemas de evaluación:

Para superar con éxito cualquier materia/asignatura, el alumno debe aprobar el examen final presencial. Esto es, en el examen final se debe alcanzar una calificación igual o superior a 5 en una escala de 0-10, siendo 0 la nota mínima y 10 la máxima.

Modalidad Presencial:

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad semipresencial

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	25	25
SE2	25	25
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad a distancia:

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	45	45
SE2	5	5
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

En todo caso, la superación de cualquier materia/asignatura está supeditada a aprobar las pruebas finales presenciales e individuales correspondientes.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - El alumno debe adquirir aquellos conocimientos sobre recursos humanos que le permitan trabajar en un equipo de ciberdelincuencia
CG2 - El alumno debe ser capaz de entender cómo su profesión afecta a otros departamentos de la empresa o institución en el ámbito de la ciberdelincuencia.
CG4 - El alumno debe ser capaz de tratar situaciones complejas e impredecibles de forma sistemática y creativa, con juicio crítico, con información incompleta, asumiendo riesgos, tomando decisiones y comunicándolas a una audiencia profesional del ámbito de la ciberseguridad y ciberdelincuencia
CG7 - El alumno debe ser capaz de desempeñar diferentes roles dentro de un equipo de la ciberseguridad y ciberdelincuencia, en particular el de líder.
CG8 - El alumno, en el ámbito de la actuación frente a la ciberdelincuencia, debe ser capaz de reconocer la necesidad del cambio y debe tener la habilidad necesaria para gestionarlo.
CG9 - El alumno debe ser capaz de actuar de forma autónoma en un marco de libertad responsable, en el ámbito de la actuación frente a la ciberdelincuencia.
CG10 - El alumno debe ser capaz de aportar valor a la empresa o institución mediante su creatividad y participación en la actuación frente a la ciberdelincuencia
CG11 - Capacidad para integrar en su actuación frente a la ciberdelincuencia, los valores y políticas de igualdad efectiva, especialmente entre mujeres y hombres y atención a la discapacidad.
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
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
5.5.1.5.2 TRANSVERSALES
No existen datos
5.5.1.5.3 ESPECÍFICAS
CE7 - Ser capaz de utilizar las herramientas científico técnicas para evaluar la fiabilidad y robustez de sistemas informáticos complejos, aplicado a la prevención de la ciberdelincuencia.
CE10 - Ser capaz de diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos, aplicado a la prevención de la ciberdelincuencia.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Clase magistral y fundamentos teóricos	35	100
Explicación técnica para la resolución de casos relacionados con las asignaturas o materias	10	100
Tutoría	10	25
Trabajo individual del estudiante	73	0
Trabajo en grupo del estudiante	10	0
Puesta en común de resultados y procedimientos	10	100
Evaluación	2	100

5.5.1.7 METODOLOGÍAS DOCENTES
Método del Caso
Aprendizaje Cooperativo

Aprendizaje Basado en Problemas (ABP)		
Clase magistral		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Desempeño del Trabajo individual	35.0	35.0
Desempeño del Trabajos grupales	15.0	15.0
Prueba final presencial	50.0	50.0
NIVEL 2: CIBERINTELIGENCIA (ITINERARIO EMPRESARIAL)		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Optativa	
ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		
NO CONSTAN ELEMENTOS DE NIVEL 3		
5.5.1.2 RESULTADOS DE APRENDIZAJE		

Resultados de aprendizaje

- Transformación de la información en inteligencia para ejecutar análisis complejos de datos estructurados y no estructurados en plataformas y grandes volúmenes de información (Big Data).
- Recopilación, a través de Cyber Threat Intelligence de datos obtenidos de la monitorización de sistemas o redes, para la detección de posibles amenazas cibernéticas que pudieran pasar desapercibidas por las herramientas convencionales de monitorización de redes.
- Capacidad de explotación de las fuentes de información del ciberespacio por los órganos de obtención y la entrega de esa información para la producción de inteligencia.
- Determinar de manera proactiva las capacidades, psicología y motivaciones de nuestros atacantes, permitirá a nuestra estrategia de Ciber Seguridad, prevenir y anticipar ataques reales a través de la Ciber Inteligencia, diseñando y mejorando los sistemas y procesos de detección y respuesta

5.5.1.3 CONTENIDOS

Contenidos

La inteligencia es el producto obtenido de la recolección, evaluación, análisis, integración e interpretación de toda la información disponible, potencialmente significativa y que permita su transformación en conocimiento, de forma que resulte útil al decisor a la hora de tomar sus decisiones con el menor nivel de incertidumbre posible, siguiendo el ciclo de Inteligencia. La Ciberinteligencia (Cyberintelligence) se refiere a las actividades de inteligencia en los procesos de la Ciberseguridad que se ocupan de analizar (Intenciones-oportunidades de los ciberactores) y prevenir, identificar, localizar y atribuir ataques o amenazas a través del ciberespacio. En un mundo cibernético, donde las amenazas evolucionan día con día, han surgido nuevas necesidades de Seguridad, Vigilancia y Resiliencia pues la administración tradicional de seguridad, sin el entendimiento adecuado de los riesgos a los cuales nuestra organización se encuentra expuesta, no es suficiente para protegernos. A pesar de que hoy día la conciencia de seguridad ha ido en aumento y se procura una mayor inversión en seguridad, los ciber ataques se han vuelto más frecuentes y los costos tangibles e intangibles mucho más

extensos; pues si bien en un comienzo las pérdidas financieras pueden determinarse rápidamente, las pérdidas intangibles son las de mayor impacto tras una brecha de seguridad. Es por esto que el conocimiento de nuestras ciber amenazas se vuelve fundamental para enfrentar estos nuevos retos; ya no basta con contar con pistas sobre lo ocurrido en un incidente, es necesario convertir datos en información valiosa que pueda direccionar nuestras estrategias de seguridad de manera proactiva.

Inteligencia Operacional: La integración de capacidades técnicas de generación de inteligencia es el primer paso para responder ante amenazas desconocidas, pues resultaría imposible aprender de nuestros adversarios sin la experiencia previa.

Inteligencia Táctica

El conocimiento del negocio es fundamental para la generación de ciber inteligencia, ya que se requiere conocer la información que se necesita proteger y entender cuál es la operación habitual para identificar actividad inusual en nuestro entorno cibernético. Por tanto, la generación de inteligencia se vuelve un proyecto de "Seguridad o Tecnología de Información".

Inteligencia Estratégica

Es de suma importancia el involucramiento de la alta dirección en la definición de una estrategia de Ciber Seguridad; por lo tanto, el entendimiento de los riesgos tecnológicos debe ser comunicado adecuadamente desde el personal técnico hacia los altos ejecutivos, permitiendo la alineación de la estrategia con los objetivos y la visión del negocio. El conocimiento y estudio de nuestros ciber adversarios se ha vuelto fundamental para el direccionamiento de nuestros esfuerzos y capacidades de defensa contra sus ataques; sin embargo, si estos no son comprendidos por nuestros altos ejecutivos puede resultar complicado alinear los esfuerzos de Ciberseguridad y las necesidades de la organización.

5.5.1.4 OBSERVACIONES

Observaciones:

- Requisitos previos: ninguno

Actividades formativas:

Modalidad Semipresencial:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	0%
AF2	10	0%
AF3	10	25%
AF4	63	0%
AF5	20	0%
AF6	10	50%
AF7	2	100%

Modalidad a distancia:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	35	0%
AF2	10	0%
AF3	10	0%
AF4	40	0%
AF5	43	0%
AF6	10	20%
AF7	2	100%

Metodologías docentes:

Modalidad semipresencial: MD1; MD2; MD3; MD4

Modalidad a distancia: MD1; MD2; MD3; MD4

Sistemas de evaluación:

Para superar con éxito cualquier materia/asignatura, el alumno debe aprobar el examen final presencial. Esto es, en el examen final se debe alcanzar una calificación igual o superior a 5 en una escala de 0-10, siendo 0 la nota mínima y 10 la máxima.

Modalidad Presencial:

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad semipresencial

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	25	25
SE2	25	25
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

Modalidad a distancia:

Convocatoria Ordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	35	35
SE2	15	15
SE3	50	50

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE1	50	50
SE2	0	0
SE3	50	50

En todo caso, la superación de cualquier materia/asignatura está supeditada a aprobar las pruebas finales presenciales e individuales correspondientes.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG2 - El alumno debe ser capaz de entender cómo su profesión afecta a otros departamentos de la empresa o institución en el ámbito de la ciberdelincuencia.
CG3 - El alumno debe dominar las técnicas de lucha contra la ciberdelincuencia suficientes en el ámbito de la ciberdelincuencia que le permitan obtener y analizar información, evaluar su relevancia y validez, sintetizarla y adaptarla al contexto.
CG4 - El alumno debe ser capaz de tratar situaciones complejas e impredecibles de forma sistemática y creativa, con juicio crítico, con información incompleta, asumiendo riesgos, tomando decisiones y comunicándolas a una audiencia profesional del ámbito de la ciberseguridad y ciberdelincuencia
CG5 - El alumno debe ser capaz de comunicarse correctamente tanto oralmente como por escrito, utilizando la tecnología más actual, en el ámbito de la ciberseguridad y ciberdelincuencia.
CG6 - El alumno debe ser capaz de actuar de forma autónoma en la planificación e implementación de proyectos y decisiones sobre prevención y actuación frente a la ciberdelincuencia.
CG9 - El alumno debe ser capaz de actuar de forma autónoma en un marco de libertad responsable, en el ámbito de la actuación frente a la ciberdelincuencia.
CG11 - Capacidad para integrar en su actuación frente a la ciberdelincuencia, los valores y políticas de igualdad efectiva, especialmente entre mujeres y hombres y atención a la discapacidad.
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
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
5.5.1.5.2 TRANSVERSALES
No existen datos
5.5.1.5.3 ESPECÍFICAS
CE1 - Ser capaz de analizar y desarrollar sistemas de seguridad web aplicado a la prevención de la ciberdelincuencia.
CE3 - Ser capaz de planificar y aplicar medidas de prevención contra fraudes en comercio electrónico.
CE4 - Ser capaz de aplicar las propiedades biométricas al área de seguridad informática y de las comunicaciones.
CE6 - Ser capaz de programar y analizar tareas en diversos lenguajes de programación en el área de seguridad informática y de las comunicaciones.
CE7 - Ser capaz de utilizar las herramientas científico técnicas para evaluar la fiabilidad y robustez de sistemas informáticos complejos, aplicado a la prevención de la ciberdelincuencia.
CE10 - Ser capaz de diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos, aplicado a la prevención de la ciberdelincuencia.
CE11 - Ser capaz de utilizar con destreza las principales herramientas de detección y clasificación de malware y de realizar ejercicios sencillos de ingeniería inversa en el contexto de la ciberseguridad

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Clase magistral y fundamentos teóricos	35	100
Explicación técnica para la resolución de casos relacionados con las asignaturas o materias	10	100
Tutoría	10	25
Trabajo individual del estudiante	35	0
Trabajo en grupo del estudiante	48	0

Puesta en común de resultados y procedimientos	10	100
Evaluación	2	100
5.5.1.7 METODOLOGÍAS DOCENTES		
Método del Caso		
Aprendizaje Cooperativo		
Aprendizaje Basado en Problemas (ABP)		
Clase magistral		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Desempeño del Trabajo individual	35.0	35.0
Desempeño del Trabajos grupales	15.0	15.0
Prueba final presencial	50.0	50.0
NIVEL 2: PRACTICAS PROFESIONALES		
5.5.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Prácticas Externas	
ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
NO CONSTAN ELEMENTOS DE NIVEL 3		
5.5.1.2 RESULTADOS DE APRENDIZAJE		

Resultados de aprendizaje:

La puesta en práctica de todas las competencias adquiridas a lo largo del programa, en las asignaturas anteriores.

5.5.1.3 CONTENIDOS

Contenidos :

La realización de un periodo de prácticas en empresas tiene también varios objetivos. Por una parte, intenta servir de puente al alumno entre la experiencia vital de un estudiante y la del desempeño de un puesto de trabajo en una empresa. Por otra parte, sirve de campo de experiencia para la aplicación de los conocimientos adquiridos y para observar en la realidad como se desarrolla la aplicación de dichos conocimientos por profesionales de mucha mayor experiencia. El alumno tiene un tutor en la Universidad al cual puede acudir para cualquier resolución o duda de cualquier problema que se plantee. El tutor está en contacto con los responsables de la empresa en la que el alumno desarrolla su periodo de prácticas. A la finalización de dicho periodo, la empresa emite un informe evaluatorio del desempeño del alumno, al mismo tiempo que el alumno tiene que escribir un informe sobre

su actividad durante las prácticas. La Universidad dispone de un departamento especializado denominado Departamento de Carreras Profesionales que se responsabiliza de la gestión y administración de las prácticas externas. El tutor del alumno y el coordinador de la titulación están en contacto constante con el Departamento de Carreras Profesionales para facilitar la realización del periodo de prácticas externas

5.5.1.4 OBSERVACIONES

Observaciones:

- Requisitos previos: haber cursado al menos 4 asignaturas y superado 2

Actividades formativas:

Modalidad Semipresencial:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	0	0%
AF2	10	100%
AF3	10	25%
AF4	49	100%
AF5	70	100%
AF6	10	100%
AF7	1	100%

Modalidad a distancia:

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	0	0%
AF2	10	100%
AF3	10	25%
AF4	69	100%
AF5	50	100%
AF6	10	100%
AF7	1	100%

Metodologías docentes:

Modalidad semipresencial: MD2; MD3;

Modalidad a distancia: MD2; MD3; MD4

Sistemas de evaluación:

Para superar con éxito cualquier materia/asignatura, el alumno debe aprobar el examen final presencial. Esto es, en el examen final se debe alcanzar una calificación igual o superior a 5 en una escala de 0-10, siendo 0 la nota mínima y 10 la máxima.

Modalidad Presencial; Modalidad semipresencial y Modalidad a distancia

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE4	75	75
SE5	25	25

En todo caso, la superación de cualquier materia/asignatura está supeditada a aprobar las pruebas finales presenciales e individuales correspondientes.

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - El alumno debe adquirir aquellos conocimientos sobre recursos humanos que le permitan trabajar en un equipo de ciberdelincuencia

CG2 - El alumno debe ser capaz de entender cómo su profesión afecta a otros departamentos de la empresa o institución en el ámbito de la ciberdelincuencia.

CG3 - El alumno debe dominar las técnicas de lucha contra la ciberdelincuencia suficientes en el ámbito de la ciberdelincuencia que le permitan obtener y analizar información, evaluar su relevancia y validez, sintetizarla y adaptarla al contexto.

CG4 - El alumno debe ser capaz de tratar situaciones complejas e impredecibles de forma sistemática y creativa, con juicio crítico, con información incompleta, asumiendo riesgos, tomando decisiones y comunicándolas a una audiencia profesional del ámbito de la ciberseguridad y ciberdelincuencia

CG5 - El alumno debe ser capaz de comunicarse correctamente tanto oralmente como por escrito, utilizando la tecnología más actual, en el ámbito de la ciberseguridad y ciberdelincuencia.

CG6 - El alumno debe ser capaz de actuar de forma autónoma en la planificación e implementación de proyectos y decisiones sobre prevención y actuación frente a la ciberdelincuencia.

CG7 - El alumno debe ser capaz de desempeñar diferentes roles dentro de un equipo de la ciberseguridad y ciberdelincuencia, en particular el de líder.

CG8 - El alumno, en el ámbito de la actuación frente a la ciberdelincuencia, debe ser capaz de reconocer la necesidad del cambio y debe tener la habilidad necesaria para gestionarlo.

CG9 - El alumno debe ser capaz de actuar de forma autónoma en un marco de libertad responsable, en el ámbito de la actuación frente a la ciberdelincuencia.

CG10 - El alumno debe ser capaz de aportar valor a la empresa o institución mediante su creatividad y participación en la actuación frente a la ciberdelincuencia

CG11 - Capacidad para integrar en su actuación frente a la ciberdelincuencia, los valores y políticas de igualdad efectiva, especialmente entre mujeres y hombres y atención a la discapacidad.

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

CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

5.5.1.5.2 TRANSVERSALES

No existen datos

5.5.1.5.3 ESPECÍFICAS

CE1 - Ser capaz de analizar y desarrollar sistemas de seguridad web aplicado a la prevención de la ciberdelincuencia.

CE2 - Ser capaz de asesorar sobre el cumplimiento de la legislación reguladora de la protección de datos en materia de seguridad

CE3 - Ser capaz de planificar y aplicar medidas de prevención contra fraudes en comercio electrónico.
CE4 - Ser capaz de aplicar las propiedades biométricas al área de seguridad informática y de las comunicaciones.
CE5 - Ser capaz de distinguir los diferentes agentes implicados en seguridad informática, y saber asesorarlos de forma integrada permitiendo la colaboración con otros departamentos de la entidad.
CE6 - Ser capaz de programar y analizar tareas en diversos lenguajes de programación en el área de seguridad informática y de las comunicaciones.
CE7 - Ser capaz de utilizar las herramientas científico técnicas para evaluar la fiabilidad y robustez de sistemas informáticos complejos, aplicado a la prevención de la ciberdelincuencia.
CE10 - Ser capaz de diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos, aplicado a la prevención de la ciberdelincuencia.
CE11 - Ser capaz de utilizar con destreza las principales herramientas de detección y clasificación de malware y de realizar ejercicios sencillos de ingeniería inversa en el contexto de la ciberseguridad

5.5.1.6 ACTIVIDADES FORMATIVAS		
ACTIVIDAD FORMATIVA	**HORAS**	**PRESENCIALIDAD**
Clase magistral y fundamentos teóricos	0	0
Explicación técnica para la resolución de casos relacionados con las asignaturas o materias	10	100
Tutoría	10	25
Trabajo individual del estudiante	60	100
Trabajo en grupo del estudiante	59	100
Puesta en común de resultados y procedimientos	10	100
Evaluación	1	100

5.5.1.7 METODOLOGÍAS DOCENTES
Aprendizaje Cooperativo
Aprendizaje Basado en Problemas (ABP)

5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Informe de autoevaluación del alumno	75.0	75.0
Certificado empresarial e Informe de la empresa	25.0	25.0

NIVEL 2: TRABAJO FIN DE MASTER	
5.5.1.1 Datos Básicos del Nivel 2	
CARÁCTER	Trabajo Fin de Grado / Máster
ECTS NIVEL 2	6

DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**

LENGUAS EN LAS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**

No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	
LISTADO DE ESPECIALIDADES		
No existen datos		
NO CONSTAN ELEMENTOS DE NIVEL 3		

5.5.1.2 RESULTADOS DE APRENDIZAJE

Resultados de aprendizaje: Evaluar la adecuada adquisición de todas las competencias del programa mediante la exposición de un trabajo pautado, que muestre la adquisición de dichas competencias.

5.5.1.3 CONTENIDOS

Contenidos Con el Trabajo se pretende conseguir una integración vertical de todos los conocimientos y desarrollo de capacidades de todas las materias de la titulación de forma que se ayude a conseguir un perfil de capacidades coherente con los objetivos del Máster. El objetivo del Trabajo Fin de Máster es crear una situación en la que el alumno se vea obligado a ejercitarse en procesos de tomas de decisiones bajo presión, tiempo limitado y escasez de información, lo más semejante que sea posible a las situaciones que tiene que afrontar quien dirige una empresa. Al mismo tiempo, es la ocasión para que el alumno tenga que ejercitarse en el trabajo en equipo, liderazgo, debate y aceptación de conclusiones, etc. En este supuesto, el Trabajo está dirigido por un Tutor, se concreta en un documento que tiene que ser defendido en una presentación profesional ante un Tribunal formado por profesores y profesionales de prestigio y relevancia en el mundo empresarial. Dicho documento escrito puede ser un elemento utilizable posteriormente como herramienta en una entrevista de selección de empleo.

5.5.1.4 OBSERVACIONES

Observaciones:

- Requisitos previos: Haber cursado o estar cursando las restantes materias.

Actividades formativas:

Modalidad semipresencial

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	0	0%
AF2	10	0%
AF3	10	10%
AF4	98	0%
AF5	20	0%
AF6	10	0%
AF7	2	100%

Modalidad a distancia

Actividad formativa	Horas	Porcentaje de presencialidad de la AF
AF1	0	0%
AF2	10	0%

AF3	10	0%
AF4	88	0%
AF5	30	0%
AF6	10	0%
AF7	2	100%

Metodologías docentes:

Modalidad semipresencial: MD2; MD3; MD4

Modalidad a distancia: MD2; MD3; MD4

Sistemas de evaluación:

Para superar con éxito cualquier materia/asignatura, el alumno debe aprobar el examen final presencial. Esto es, en el examen final se debe alcanzar una calificación igual o superior a 5 en una escala de 0-10, siendo 0 la nota mínima y 10 la máxima.

Modalidad presencial; modalidad semipresencial; modalidad a distancia

Convocatoria Extraordinaria

Sistema de Evaluación	Ponderación mínima %	Ponderación máxima %
SE6 Defensa ante tribunal		
Aspectos metodológicos: Fuentes bibliográficas y/o documentales consultadas, corrección y adecuación de la metodología.	25 %	25 %
Aportaciones del trabajo: Pertinencia, originalidad, interés y fundamentación de las aportaciones del trabajo.	25 %	25 %
Aspectos formales del documento escrito: Estructura, claridad en la exposición de las ideas y corrección del lenguaje.	25 %	25 %
Exposición del trabajo y defensa oral ante el tribunal: Claridad de la exposición y defensa oral ante el tribunal, capacidad de síntesis y de transmisión.	25 %	25 %
TOTAL	100%	100%

El Tribunal estará formado por al menos tres profesores que ejercen como Presidente, Vocal y Secretario.

El profesor que ejerza como Presidente del Tribunal deberá ser Doctor. Si el Departamento o Facultad así lo aprueba, el vocal podrá ser un experto de reconocido prestigio en el campo. Además, podrá invitar a otros expertos del sector. En ningún caso podrá estar incluido el tutor- Director del Trabajo Fin de Máster. Para establecer la composición del tribunal se ha atendido a los criterios indicados en la Normativa Universitaria de Trabajo Fin de Máster de la Universidad Nebrija

5.5.1.5 COMPETENCIAS

5.5.1.5.1 BÁSICAS Y GENERALES

CG1 - El alumno debe adquirir aquellos conocimientos sobre recursos humanos que le permitan trabajar en un equipo de ciberdelincuencia

CG2 - El alumno debe ser capaz de entender cómo su profesión afecta a otros departamentos de la empresa o institución en el ámbito de la ciberdelincuencia.

CG3 - El alumno debe dominar las técnicas de lucha contra la ciberdelincuencia suficientes en el ámbito de la ciberdelincuencia que le permitan obtener y analizar información, evaluar su relevancia y validez, sintetizarla y adaptarla al contexto.

CG4 - El alumno debe ser capaz de tratar situaciones complejas e impredecibles de forma sistemática y creativa, con juicio crítico, con información incompleta, asumiendo riesgos, tomando decisiones y comunicándolas a una audiencia profesional del ámbito de la ciberseguridad y ciberdelincuencia

CG5 - El alumno debe ser capaz de comunicarse correctamente tanto oralmente como por escrito, utilizando la tecnología más actual, en el ámbito de la ciberseguridad y ciberdelincuencia.

CG6 - El alumno debe ser capaz de actuar de forma autónoma en la planificación e implementación de proyectos y decisiones sobre prevención y actuación frente a la ciberdelincuencia.
CG7 - El alumno debe ser capaz de desempeñar diferentes roles dentro de un equipo de la ciberseguridad y ciberdelincuencia, en particular el de líder.
CG8 - El alumno, en el ámbito de la actuación frente a la ciberdelincuencia, debe ser capaz de reconocer la necesidad del cambio y debe tener la habilidad necesaria para gestionarlo.
CG9 - El alumno debe ser capaz de actuar de forma autónoma en un marco de libertad responsable, en el ámbito de la actuación frente a la ciberdelincuencia.
CG10 - El alumno debe ser capaz de aportar valor a la empresa o institución mediante su creatividad y participación en la actuación frente a la ciberdelincuencia
CG11 - Capacidad para integrar en su actuación frente a la ciberdelincuencia, los valores y políticas de igualdad efectiva, especialmente entre mujeres y hombres y atención a la discapacidad.
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
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
5.5.1.5.2 TRANSVERSALES
No existen datos
5.5.1.5.3 ESPECÍFICAS
CE1 - Ser capaz de analizar y desarrollar sistemas de seguridad web aplicado a la prevención de la ciberdelincuencia.
CE2 - Ser capaz de asesorar sobre el cumplimiento de la legislación reguladora de la protección de datos en materia de seguridad
CE3 - Ser capaz de planificar y aplicar medidas de prevención contra fraudes en comercio electrónico.
CE4 - Ser capaz de aplicar las propiedades biométricas al área de seguridad informática y de las comunicaciones.
CE5 - Ser capaz de distinguir los diferentes agentes implicados en seguridad informática, y saber asesorarlos de forma integrada permitiendo la colaboración con otros departamentos de la entidad.
CE6 - Ser capaz de programar y analizar tareas en diversos lenguajes de programación en el área de seguridad informática y de las comunicaciones.
CE7 - Ser capaz de utilizar las herramientas científico técnicas para evaluar la fiabilidad y robustez de sistemas informáticos complejos, aplicado a la prevención de la ciberdelincuencia.
CE10 - Ser capaz de diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos, aplicado a la prevención de la ciberdelincuencia.
CE11 - Ser capaz de utilizar con destreza las principales herramientas de detección y clasificación de malware y de realizar ejercicios sencillos de ingeniería inversa en el contexto de la ciberseguridad
CE12 - Ser capaz de realizar, presentar y defender, una vez obtenidos todos los créditos del plan de estudios, un ejercicio original ante un tribunal universitario, consistente en un proyecto de investigación en el campo de la ciberdelincuencia en el que se sinteticen las competencias adquiridas en las enseñanzas.

5.5.1.6 ACTIVIDADES FORMATIVAS

ACTIVIDAD FORMATIVA	HORAS	PRESENCIALIDAD
Clase magistral y fundamentos teóricos	0	0
Explicación técnica para la resolución de casos relacionados con las asignaturas o materias	10	0
Tutoría	10	20

Trabajo individual del estudiante	58	0
Trabajo en grupo del estudiante	60	0
Puesta en común de resultados y procedimientos	10	100
Evaluación	2	100
5.5.1.7 METODOLOGÍAS DOCENTES		
Aprendizaje Cooperativo		
Aprendizaje Basado en Problemas (ABP)		
Clase magistral		
5.5.1.8 SISTEMAS DE EVALUACIÓN		
SISTEMA DE EVALUACIÓN	**PONDERACIÓN MÍNIMA**	**PONDERACIÓN MÁXIMA**
Defensa ante tribunal	100.0	100.0

6. PERSONAL ACADÉMICO

6.1 PROFESORADO Y OTROS RECURSOS HUMANOS				
Universidad	**Categoría**	**Total %**	**Doctores %**	**Horas %**
Universidad Antonio de Nebrija	Profesor Adjunto	34.6	88	28,5
Universidad Antonio de Nebrija	Profesor Director	1.9	100	1
Universidad Antonio de Nebrija	Profesor Asociado (incluye profesor asociado de C.C.: de Salud)	34.6	67	41
Universidad Antonio de Nebrija	Ayudante	28	75	29,3

PERSONAL ACADÉMICO
Ver Apartado 6: Anexo 1.

6.2 OTROS RECURSOS HUMANOS
Ver Apartado 6: Anexo 2.

7. RECURSOS MATERIALES Y SERVICIOS

Justificación de que los medios materiales disponibles son adecuados: Ver Apartado 7: Anexo 1.

8. RESULTADOS PREVISTOS

8.1 ESTIMACIÓN DE VALORES CUANTITATIVOS		
TASA DE GRADUACIÓN %	**TASA DE ABANDONO %**	**TASA DE EFICIENCIA %**
75	22	80
CODIGO	**TASA**	**VALOR %**
No existen datos		
Justificación de los Indicadores Propuestos:		
Ver Apartado 8: Anexo 1.		

8.2 PROCEDIMIENTO GENERAL PARA VALORAR EL PROCESO Y LOS RESULTADOS

8.2.- Progreso y resultados del aprendizaje

Los procesos generales que se emplean en la Universidad Antonio de Nebrija para valorar el progreso y los resultados del aprendizaje de los estudiantes son los siguientes:

- **A lo largo del curso:** Una reunión antes de comenzar el curso y otra al finalizar el mismo, con todos los profesores. En ellas se informa de la marcha general y de sus dificultades referidas a planificación, cumplimiento de los programas, repeticiones o lagunas en las materias si fuera el caso, etc. También de los estudiantes que presenten especiales dificultades en su rendimiento o de excepcionales condiciones. Normalmente serán los resultados de las pruebas realizadas hasta el momento, los indicadores más inmediatos de estos aspectos; aunque también los tutores podrán completar la información cuando sea oportuno. El/la director/a de la titulación pondrán en marcha los mecanismos oportunos para remediar las dificultades cuanto antes y aprovechar la experiencia para la reorientación del alumno.
- **A final de cada curso:** El/la director/a de la titulación valorará los resultados con los profesores. Ambos responsables redactarán un breve informe ejecutivo sobre los resultados académicos y de investigación con los objetivos de mejora para el próximo curso. Los que estén en su órbita de atribuciones los comentará al profesorado en una reunión; los que le excedan los presentará al decanato.

Con carácter adicional al sistema de evaluación general, el Máster Universitario en Ciberdelincuencia contará con la figura del Director/a y Gestor/a por parte del departamento on line del Máster, que tendrán entre sus funciones la de hacer un seguimiento permanente y personalizado del estudiante y de sus resultados académicos, de soporte técnico sobre Blackboard y de practicum, tal y como se ha indicado en el apartado 5.3. El alumno tiene contacto directo con ellos cuando lo necesita y además, una entrevista personal cuando el alumno lo requiera. Cuando se encuentre en la fase de realización del Trabajo Fin de Máster cuenta con el asesoramiento continúo de su tutor, mediante una comunicación fluida y constante por diferentes medios electrónicos y entrevistas personales.

Después de pasar las pruebas del proceso de admisión, y de incorporarse al curso académico, la evaluación de las asignaturas se realiza de acuerdo a lo establecido en las fichas de cada asignatura, donde se contemplan detalladamente las acciones formativas y los aspectos integrados en la docencia.

Y para garantizar el seguimiento integral de los progresos de los estudiantes del Máster, se realizarán reuniones de evaluación entre el Director del Máster y el profesor de la asignatura del programa y de los alumnos, tratados individualmente. Tras la finalización de los exámenes o la entrega de los trabajos asignados, y una vez introducidos las calificaciones en el sistema, se realizarán reuniones de evaluación en las que participarán el claustro de profesores del semestre, el Gestor/a, el Director/a del Máster, y la secretaría del departamento. En estas reuniones se revisa la evolución académica del grupo, rendimiento de los alumnos, posibles incidencias de cualquier tipo, alumnos que están en situaciones particulares, grado de cumplimiento de programas, etc. Si es necesario, se acuerdan acciones de seguimiento y atención personalizada a algunos alumnos.

8.2.1.- Aspectos metodológicos de la evaluación para el seguimiento del aprendizaje, específicos de la modalidad semipresencial y a distancia

Evaluación más continuada y frecuente

Con carácter general, la evaluación en la modalidad semipresencial, debe ser más continuada y frecuente en el número de trabajos que debe entregar el estudiante. De esta forma se podrá realizar un seguimiento más cercano y continuo del progreso y resultados del aprendizaje, que compense la no presencialidad.

Uso de herramientas tecnológicas para el seguimiento del aprendizaje.

Hay que señalar que la plataforma virtual utilizada, dispone de herramientas de seguimiento de la entrega de trabajos y del tiempo de conexión a la misma por el alumno, de forma que se dispare una alarma si ha transcurrido un cierto número umbral de días sin ninguna conexión por parte del alumno. Este umbral se puede configurar a voluntad.

Recíprocamente el interfaz que el alumno ve, presenta cuando se abre, unos iconos que identifican de inmediato si se han añadido nuevos contenidos o intervenciones en la asignatura en concreto por parte del profesor. De esta forma se facilita por ambas partes, profesor y alumno la identificación del avance en su aportación al Campus, sea esta cual sea.

Compartición activa de conocimiento

Adicionalmente, el uso de los foros permite una puesta en común de dudas académicas que todos los alumnos ven y el profesor responde para todos, de forma que se pueda hacer un seguimiento próximo del progreso a medida que avanzan los capítulos. Se debe tener en cuenta que precisamente por estar los alumnos a distancia, hacen un uso intensivo de la comunicación con los profesores a través de los foros, muy superior al de los alumnos presenciales que también tienen esa herramienta disponible, esto permite tener una realimentación del progreso de cada alumno. Además, y de forma progresiva, la sociedad en su conjunto y los jóvenes especialmente, se han implicado y familiarizado en la comunicación a través de foros y redes sociales virtuales, con un grado de intensidad muy notable en los últimos años y que también puede ser explotado favorablemente para la enseñanza.

Seguimiento personalizado telefónico

El personal administrativo de seguimiento de los cursos, se pone en contacto telefónico inmediato con aquellos alumnos que pueden dar síntoma, por cualquier vía de abandono, distanciamiento o demora de las actividades formativas o de evaluación por parte de cualquier alumno. Este seguimiento telefónico es un factor de calidad docente muy importante, tal como se ha puesto de manifiesto en la experiencia de la universidad Nebrija en los programas impartidos hasta la fecha en la metodología a distancia.

Aprendizaje activo

Como criterio metodológico general que garantice un aprendizaje correcto en la modalidad a distancia, se debe promover el aprendizaje activo, esto incluirá la búsqueda de información y soporte, en situaciones y casos no totalmente cerrados en la información de la que disponen, de manera que el alumno deba esforzarse en esa búsqueda de información e integrar criterios, experiencias y conocimiento de varias fuentes.

El profesor como diseñador de experiencias de aprendizaje

Emana de los principios de los planteamientos docentes y pedagógicos del EEES y es común a la enseñanza presencial, pero requiere más imaginación en la modalidad a distancia, las actividades formativas deben convertirse en auténticas experiencias de aprendizaje para que el alumno mantenga su interés y motivación en grado máximo. Esto hará que participe a medida que evoluciona la asignatura y el profesor pueda observar mejor esa participación, implicación creativa orientada y en definitiva pueda evaluar y comprobar el resultado final de lo aprendido por el alumno.

Planificación y seguimiento síncrono del aprendizaje

Otro factor metodológico importante que facilita el seguimiento del progreso en el caso de modalidad a distancia, es la propia secuencia síncrona de los itinerarios formativos. Se van subiendo al campus virtual los contenidos y se van exigiendo la entrega de trabajos de forma secuenciada coordinada y planificada, de manera que se pueda hacer un seguimiento del progreso de aprendizaje de forma organizada, de forma similar al avance de las clases en la modalidad presencial, pero con una entrega de trabajos por parte del alumno más frecuente.

Los test de autoevaluación, son también una herramienta específica para esta modalidad y sirven para que el alumno pueda evaluarse a sí mismo, facilitando su propio seguimiento del aprendizaje.

El Trabajo fin de Máster como ejercicio de síntesis.

La elaboración, presentación y defensa del Trabajo Fin de Máster (o TFM) es una excelente ocasión para valorar la adquisición de las competencias en su conjunto por parte del alumno, todas ellas, los conocimientos, las capacidades de autoaprendizaje, la aptitud para comunicar argumentar y convencer, la capacidad para emitir juicios y aplicar criterios a cada problema que se analice. Durante el proceso de elaboración la distancia del alumno debe ser resuelta por el Director del TFM utilizando las herramientas de comunicación y reunión telepresencial ya descritas.

Evaluación a distancia

Para medir los resultados de aprendizaje en la modalidad a distancia, se evaluará a los alumnos conforme a los siguientes procedimientos:

1. Elaboración de trabajos individuales y en grupo.
2. Evaluación de lecturas complementarias.
3. Resolución de casos prácticos, ejercicios, análisis de recursos, resolución de problemas, etc.
4. Pruebas escritas a distancia: Pruebas de conocimiento. Ejercicios evaluables que el alumno debe resolver y enviar al profesor en un plazo determinado. El profesor puede solicitar que estas pruebas sean resueltas individualmente o en grupo. Una vez evaluadas, sus resultados se publicarán en la plataforma.
5. Participación en foros a distancia, sesiones telepresenciales, y otros medios colaborativos, y participación en las sesiones lectivas a distancia.

Los test de autoevaluación, si se requieren, que el alumno puede realizar solamente sirven para su propia evaluación, pero no son evaluados por el profesor y no se tienen en cuenta en la nota final.

En todos los ejercicios y trabajos a distancia y, en general en todo el uso de la plataforma informática a distancia, la suplantación de personalidad está radicalmente prohibida. Los profesores comprobarán la diferencia de los trabajos de cada alumno o grupo de alumnos con los trabajos de los demás alumnos una vez entregados. Adicionalmente, los alumnos deben estar preparados para la personalización de los trabajos propuestos, de forma que cada alumno tenga que entregar un trabajo diferente, aunque se garantice la adquisición común de competencias.

En las fichas de asignaturas que se incluyen en el presente documento aparece reflejado el procedimiento de evaluación para cada una de las asignaturas, indicando claramente la naturaleza del examen final presencial.

En todo caso, la superación de cualquier materia/asignatura está supeditada a aprobar las pruebas finales presenciales correspondientes.

9. SISTEMA DE GARANTÍA DE CALIDAD

ENLACE	http://www.nebrija.com/unidad-tecnica-de-calidad-nebrija/documentos-sistema.php

10. CALENDARIO DE IMPLANTACIÓN

10.1 CRONOGRAMA DE IMPLANTACIÓN	
CURSO DE INICIO	2018

Ver Apartado 10: Anexo 1.

10.2 PROCEDIMIENTO DE ADAPTACIÓN

10. Calendario de Implantación

Justificación

De Octubre a Junio - De Marzo a Febrero

Curso de implantación

2018/2019 para las tres modalidades solicitadas: presencial, semipresencial y a distancia

Procedimiento de adaptación en su caso de los estudiantes de los estudios existentes al nuevo plan de estudios

No procede

Enseñanzas que se extinguen por la implantación del siguiente título propuesto

Se extinguen las enseñanzas del título propio ¿Máster en ciberdelincuencia¿ por la Universidad Antonio de Nebrija. Dicho título, impartido en la Universidad Antonio de Nebrija, coincide en objetivos, competencias, criterios de evaluación, criterios de calificación y obtención de la nota media del expediente, trabajo final de Máster como se detalla en el punto 4.4. de la presente memoria, para aquellos módulos y materias para los que se plantea reconocimiento.

10.3 ENSEÑANZAS QUE SE EXTINGUEN

CÓDIGO	**ESTUDIO - CENTRO**