VICERRECTORADO DE POSTGRADO, EMPLEABILIDAD Y RELACIONES CON LAS EMPRESAS E INSTITUCIONES

Fecha: 18/12/2019
Unidad Origen: Vicerrectorado de Postgrado, Empleabilidad y Relaciones con las Empresas e Instituciones
Asunto: *Petición de inclusión de asunto en orden del día del Consejo de Gobierno*

Unidad de destino:
- Secretaría General de la UAL

Por la presente le ruego proceda a incluir en el orden del día del próximo Consejo de Gobierno un punto con el siguiente enunciado:

Aprobación, si procede, del Máster Propio en Ciberseguridad. .

y cuya propuesta de acuerdo sería:

Se aprueba el Máster Propio, para su elevación al Consejo Social: - Máster en Ciberseguridad. Se adjunta documentación.

El VICERRECTOR

[firma certificado digital FNMT]

Fdo.: Juan García García

SRA. SECRETARIA GENERAL DE LA UNIVERSIDAD DE ALMERÍA

Puede verificar la autenticidad, validez e integridad de este documento en la dirección:
https://verificarfirma.ual.es/verificarfirma/code/+8Qwa2D/zQUYiyARvYAduw==

Firmado Por	Juan Garcia Garcia		Fecha	12/12/2019
ID. FIRMA	blade39adm.ual.es	+8Qwa2D/zQUYiyARvYAduw==	PÁGINA	1/1

+8Qwa2D/zQUYiyARvYAduw==

Informe favorable, si procede, del Máster Propio:

- ✓ **Máster en Ciberseguridad. (147379)**

UNIVERSIDAD DE ALMERÍA

Centro de Postgrado y Formación Continua
Universidad de Almería

Nº Expediente:	147379
Inicio Expediente:	08/11/2019
Propuesta:	08/11/2019
Informe:	08/11/2019

Curso: Master en ciberseguridad

Unidad Académica (Organizador):

Centro de Desarrollo y Transferencia de Investigación Matemática a la empresa

Título a Expedir	Duración	Plazas
Máster	**60 ECTS / 515h**	**30 Alumnos**

INFORME ACADÉMICO

1.- ADECUACIÓN A NIVEL ACADÉMICO DE LA PROPUESTA A LA NORMATIVA DE ENSEÑANZAS PROPIAS

- Adecuación correcta.

2.- OTROS ASPECTOS

- Antecedentes: Es la primera edición de este curso.

La Subdirectora
del Centro de Postgrado y Formación Continua

María Mercedes Peralta López

UNIVERSIDAD DE ALMERÍA

Centro de Postgrado y Formación Continua
Universidad de Almería

Nº Expediente:	147379
Inicio Expediente:	08/11/2019
Propuesta:	08/11/2019
Informe:	08/11/2019

Curso: Master en ciberseguridad

Unidad Académica (Organizador):

Centro de Desarrollo y Transferencia de Investigación Matemática a la empresa

Título a Expedir	Duración	Plazas
Máster	**60 ECTS / 515h**	**30 Alumnos**

INFORME TÉCNICO

1.- ADECUACIÓN A NIVEL TÉCNICO DE LA PROPUESTA A LA NORMATIVA DE ENSEÑANZAS PROPIAS
- Adecuación correcta.

2.- ADECUACIÓN DE LA PROPUESTA A LA NORMATIVA DEL CONSEJO SOCIAL
- Adecuación correcta.

2.1.- MEMORIA ENTREGADA: Sí.
2.2.- PRECIO ACORDE A NORMATIVA: Sí.
2.3.- HONORARIOS ACORDE A NORMATIVA: Sí.
2.4.- NÚMERO DE ALUMNOS POR GRUPO ACORDE A NORMATIVA: Sí.

3.- CUMPLIMIENTO DE LA NORMATIVA DE EEPP RESPECTO A LA ASIGNACIÓN DE HORAS AL PROFESORADO
- Sí.

4.- OTROS ASPECTOS

- Antecedentes: Es la primera edición de este curso.

El Jefe de Sección
Enseñanzas Propias

Sergio Altea Puertollano

Vº Bº
El Jefe del Servicio de Ordenación Docente,
Planes de Estudio y Formación Continua

Esther González Jiménez

AENOR Empresa Registrada ER 0/26/2004
IQNet

Código:	147379
Fecha:	10/12/2019
Hora:	11:35:31

PORTADA

Denominación del Curso
Master en ciberseguridad
Traducción de la Denominación al Inglés
No se ha especificado traducción al inglés

Código del curso	Edición	Curso Académico	Duración horas	Créditos ECTS	Diploma a expedir	Área de Conocimiento
147379	1	2019/20	515	60	Master	Ingeniería y Tecnología

El Director se compromete a seguir el Sistema de Verificación de Calidad

Organizadores
Centro de Desarrollo y Transferencia de Investigación Matemática a la Empresa

Dirección y Coordinación	
Director(es)	Juan Antonio López Ramos , José Antonio Álvarez Bermejo
Responsable Económico-Administrativo del Curso	Director
Correo electrónico para notificaciones	jaberme@ual.es
Teléfono de Contacto	609187507

Alumnos Totales	
Mínimo	**Óptimo**
3	30

Porcentaje Virtual	Usa el Aula Virtual del Centro de Postgrado y Formación Continua
100%	Sí

Actividades formativas no presenciales, herramientas de comunicación y utilidades propuestas
Resolución de problemas. - Entrega de actividades y trabajos. - Docencia a distancia a través de Collaborate. - Docencia / material docente multimedia. - Herramientas: herramientas de comunicación de Blackboard.

Avalado por el Centro de Gastos	
Código del Centro de Gastos	**Denominación del Centro de Gastos**
122040	Centro de Desarrollo de Transferencia de Investigación Matemática a la Empresa

Perfil de Entrada	
Número	**Perfil**
1	Graduados que hayan superado los Títulos de Experto en Ciberseguridad que componen este Master

Código:	147379
Fecha:	10/12/2019
Hora:	11:35:31

Procedimiento de Evaluación
Entrega de relaciones de ejercicios. Entrega de trabajos prácticos.

Objetivos, Proyección profesional, aspectos innovadores...
Los objetivos básicos de este master es el de proporcionar una formación en un campo tan demandado actualmente por las empresas como es la ciberseguridad, abarcando competencias en diversos campos de la misma, algunos básicos, tales como aspectos reguladores y legislativos o estándares criptográficos, y otros más técnicos, abarcando la seguridad en entornos de red, el software y el hardware. Se pretende que el estudiante tenga una formación que le haga tener una visión lo más completa posible de los aspectos a tener en cuenta a la hora de proteger todo tipo de dispositivos y sistemas de comunicación y electrónicos y que pueda ser aplicada en ambientes reales.

Justificación de la conveniencia de su implantación
La cibersegurdidad es un término de reciente creación y que hace referencia tal como se expresa en la Recomendación UITT X.1205, es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de ries- gos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno, que incluyen los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada dicho ciberentorno. La ciberseguridad vela por el mantenimiento de la disponibilidad y de los activos y usuarios, su integridad, la confidencialidad, la autenticidad y el no repudio de los mismos. Los principales hitos que afectan a la ciberseguridad en nuestro país son la Estrategia española de ciberseguridad (http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf); la Agenda Digital para España (http://www.agendadigital.gob.es/digital- agenda/Documents/digital-agenda-for-spain.pdf) y La Agenda Digital para Europa (http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=EN). En ellos se recoge la necesidad y obligación de establecer un ciberespacio seguro para un entorno que nos ofrece múltiples oportunidades en el campo comercial, el tecnológico, el científico, el cultural o el de las relaciones sociales, pero que, al mismo tiempo se enfrenta a multitud de retos y amenazas derivados de la interconectividad y el acceso a los dispositivos e información que ofrece el ciberespacio. Es por ello que son cada vez más las empresas privadas e instituciones públicas que demandan profesionales con una formación específica en el conocimiento y competencias que permitan desarrollar su actividad en el ciberespacio de un modo adecuado y que cumpla con las exigencias que demandan los hitos anteriormente citados. Actualmente la Universidad de Almería no ofrece ningún título similar de grado o master. Tan solo ciertos aspectos muy genéricos son recogidos en muy determinadas materias dentro de algunos de los títulos anteriormente citados, pero que, evidentemente no son ni mucho menos suficientes para ofrecer una formación en este campo como actualmente están demandando gobiernos, sociedad y empresas.

Gestión de Matrícula
Centro de Postgrado y Formación Continua

Propuesta Inicial de Plazos	
Plazo de Preinscripción	Matriculación sin Preinscripcion
Fecha de Publicación Listado Provisional	-
Plazo de Reclamaciones	-
Fecha de Publicación Listado Definitivo	-
Plazo de Inscripción	Del día 24/03/2020 al día 31/03/2020
Llamamiento para cubrir vacante	-
Fechas de Celebración del Curso	Del día 01/04/2020 al día 30/09/2020

Turno	**Horario**	**Lugar de realización**
Por determinar	Universidad de Almería	Del día 01/04/2020 al día 30/09/2020

¿Dónde puede solicitar el alumno información?

Página Web
http://www.ual.es/~cybersecurity

Código:	147379
Fecha:	10/12/2019
Hora:	11:35:31

Programación Docente						
Num	**Denominación del Módulo**	**Créditos ECTS**	**Horas**	**Computable**	**Trabajo Final**	**Prácticas Externas**
1	Aspectos legales y tratamiento de datos	3	22,5	No	No	No
2	Análisis de riesgos en la protección de datos y privacidad	3	22,5	No	No	No
3	Fundamentos criptográficos de la seguridad.	4	30	No	No	No
4	Seguridad en redes	6	45	No	No	No
5	Investigaciones digitales y análisis forense informático	3	22,5	No	No	No
6	Ingeniería del Software en Proyectos de Seguridad. Desarrollo seguro.	3	22,5	No	No	No
7	Seguridad de datos en sistemas electrónicos	4	30	No	No	No
8	Protección de sistemas electrónicos	2	15	No	No	No
9	Seguridad en entornos IoT	2	15	No	No	No
10	Análisis de malware	4	30	No	No	No
11	Introducción a la BIOS y RAM	2	15	No	No	No
12	Análisis de cifradores y procesos de protección de la información	2	15	No	No	No
13	Ofensiva y defensa en aplicaciones web	3	22,5	No	No	No
14	Blockchain	1	7,5	No	No	No
15	Prácticas externas	12	150	No	No	Sí
16	Trabajo Final de Máster	6	49,5	Sí	Sí	No

Código:	147379
Fecha:	10/12/2019
Hora:	11:35:31

CUADRO DE PROFESORADO

Docente	Datos Personales			Externo UAL	Id	Tipo de cotización	Horas Asignadas	
	Apellidos	Nombre	Sexo				Lectivas	Otras
Sí	Álvarez Bermejo	José Antonio	Varón	No	19575	Prof. funcionario posterior 01/01/2011	0	34,75
Departamento de Informática								
Sí	Fernández Guerrero	José María	Varón	No	19576	PAS funcionario	0	0
Responsable de Datos UAL. Funcionario.								
Sí	Gómez López	Julio	Varón	Sí	19577	Sin asignar	0	0
Experto en seguridad den redes. Profesor de ciclos superiores. Junta de Andalucía.								
Sí	López Ramos	Juan Antonio	Varón	No	19578	Prof. funcionario anterior 31/12/2010	0	34,75
Departamento de Matemáticas								
Sí	Parrilla Roure	Luis	Varón	Sí	19579	Sin asignar	0	0
Profesor Titular de Universidad. Departamento de Electrónica y Tecnología de Computadores - Universidad de Granada.								
Sí	Peralta López	Justo	Varón	No	19580	Prof. funcionario anterior 31/12/2010	0	0
Departamento de Matemáticas								
Sí	Piedra Fernández	María Ángeles	Mujer	No	19581	PAS funcionario	0	0
Asesora Jurídica de la UAL. Funcionaria								
Sí	Sánchez Cordero	Pedro	Varón	Sí	19582	Sin asignar	0	0
CIR-DFIR - Principal Forensics and Threat Hunting en Santander Global Tech.								
Sí	Castillo Morales	Encarnación	Mujer	Sí	19583	Sin asignar	0	0
Profesor Titular de Universidad. Departamento de Electrónica y Tecnología de Computadores - Universidad de Granada.								
Sí	Varela Vaca	Ángel Jesús	Varón	Sí	19592	Sin asignar	0	0
Profesor Ayudante Doctor en la Universidad de Sevilla								

Total	Docentes		No Docentes		Docentes Propios		Docentes Externos	
10	10	100 %	0	0 %	5	50 %	5	50 %

Código:	147379
Fecha:	10/12/2019
Hora:	11:35:31

RELACIÓN DE ACTIVIDADES

Actividades Académicas			Presupuesto Mínimo		Presupuesto Óptimo	
Cod	**Actividad**	**Horas**	**€ / Hora**	**Total**	**€ / Hora**	**Total**
TRIBU	Tribunal	10	4	40 €	49	490 €
TFIN	Trabajo Final	49.5	7	346,5 €	70	3465 €

Dirección y Secretaría			Presupuesto Mínimo		Presupuesto Óptimo	
Cod	**Actividad**	**Horas**	**€ / Hora**	**Total**	**€ / Hora**	**Total**
DIR	Dirección	10	7	70 €	66	660 €

Total	Horas	Presupuesto Mínimo	Presupuesto Óptimo
Total Actividades Académicas	59,5	386,5	3955
Total Dirección y Secretaría	10	70 €	660 €
TOTAL GASTOS PERSONAL:	69,5	456,5 €	4615 €

Código:	147379
Fecha:	10/12/2019
Hora:	11:35:31

CONTENIDO DE LA COLABORACIÓN

Módulo	Actividad	Cod	Profesor	Horas
16	Trabajo Final	TFIN	Álvarez Bermejo José Antonio	24,75
16	Trabajo Final	TFIN	López Ramos Juan Antonio	24,75
Sin Módulo	Tribunal	TRIBU	Álvarez Bermejo José Antonio	5
Sin Módulo	Tribunal	TRIBU	López Ramos Juan Antonio	5
Sin Módulo	Dirección	DIR	Álvarez Bermejo José Antonio	5
Sin Módulo	Dirección	DIR	López Ramos Juan Antonio	5

El porcentaje de horas en actividades docentes asignadas a Docentes Propios de la Universidad (100%) es SUPERIOR al mínimo permitido (20%).

Código:	147379
Fecha:	10/12/2019
Hora:	11:35:31

PRESUPUESTO

GASTOS		
1. Personal	**Presupuesto Mínimo**	**Presupuesto Óptimo**
Profesorado	386,5 €	3955 €
Dirección / Coordinación / Secretaría	70 €	660 €
TOTAL	**456,5 €**	**4615 €**

2. Desplazamientos y Estancias	**Presupuesto Mínimo**	**Presupuesto Óptimo**
Desplazamientos	0 €	0 €
Alojamientos	0 €	0 €
Manutención	0 €	0 €
TOTAL	**0 €**	**0 €**

3. Material Fungible, Inventariable y Bibliografía	**Presupuesto Mínimo**	**Presupuesto Óptimo**
Material de Oficina	0 €	0 €
Material de Laboratorio	0 €	0 €
Reprografía	0 €	0 €
Bibliografía	0 €	0 €
Otros	0 €	0 €
Otros	0 €	0 €

4. Publicidad	**Presupuesto Mínimo**	**Presupuesto Óptimo**
TOTAL	**0 €**	**0 €**

5. Otros Gastos	**Presupuesto Mínimo**	**Presupuesto Óptimo**
Expedición de Títulos	18 €	180 €
Canon becas y otros proyectos (5 %)	30 €	300 €
Importe total de cotizaciones a la seguridad social	27,7324 €	280,361 €
Importe aula virtual	0 €	0 €
Producción Contenidos Digitales	0 €	0 €
Gastos de Gestión por Entidad Externa	0 €	0 €
Otros:	0 €	0 €
TOTAL	**75,73 €**	**760,37 €**

TOTAL DE GASTOS (1 al 5)	**532,23 €**	**5375,37 €**

6. Aportación a la Universidad de Almería	**Presupuesto Mínimo**	**Presupuesto Óptimo**
Aportación 10%	60 €	600 €

TOTAL DE GASTOS	**592,23 €**	**5975,37 €**

Código:	147379
Fecha:	10/12/2019
Hora:	11:35:31

INGRESOS		
7. Subvenciones y Otros Ingresos	**Presupuesto Mínimo**	**Presupuesto Óptimo**
1.	0 €	0 €
2.	0 €	0 €
3.	0 €	0 €
4.	0 €	0 €
TOTAL	**0 €**	**0 €**

8. Remanente Edición Anterior	**Presupuesto Mínimo**	**Presupuesto Óptimo**
TOTAL	**0 €**	**0 €**

9. Precios Públicos	**Presupuesto Mínimo**	**Presupuesto Óptimo**
Número de Alumnos	3 €	30 €
Matrícula 200 €/Alumno. Gestión: Centro de Postgrado y Formación Continua	600 €	6000 €
TOTAL	**600 €**	**6000 €**

TOTAL DE INGRESOS	**600 €**	**6000 €**

RESULTADO PRESUPUESTARIO	**Presupuesto Mínimo**	**Presupuesto Óptimo**
TOTAL	**7,77 €**	**24,63 €**

Código:	147379
Fecha:	08/11/2019
Hora:	14:12:53

PORTADA

Denominación del Curso
Master en ciberseguridad
Traducción de la Denominación al Inglés
No se ha especificado traducción al inglés

Código del curso	Edición	Curso Académico	Duración horas	Créditos ECTS	Diploma a expedir	Área de Conocimiento
147379	1	2019/20	515	60	Master	Ingeniería y Tecnología

El Director se compromete a seguir el Sistema de Verificación de Calidad

Organizadores
Dpto. Matemáticas
Organizadores
Dpto. Matemáticas
Dpto. Informática
Organizadores
Dpto. Matemáticas
Dpto. Informática
Centro de Desarrollo y Transferencia de Investigación Matemática a la Empresa

Dirección y Coordinación	
Director(es)	Juan Antonio López Ramos , José Antonio Álvarez Bermejo
Responsable Económico-Administrativo del Curso	Director
Correo electrónico para notificaciones	jaberme@ual.es
Teléfono de Contacto	609187507

Alumnos Totales	
Mínimo	**Óptimo**
3	30

Porcentaje Virtual	Usa el Aula Virtual del Centro de Postgrado y Formación Continua
100%	Sí

Actividades formativas no presenciales, herramientas de comunicación y utilidades propuestas
Resolución de problemas. - Entrega de actividades y trabajos. - Docencia a distancia a través de Collaborate. - Docencia / material docente multimedia. - Herramientas: herramientas de comunicación de Blackboard.

Código:	147379
Fecha:	08/11/2019
Hora:	14:12:53

Avalado por el Centro de Gastos	
Código del Centro de Gastos	**Denominación del Centro de Gastos**
122040	Centro de Desarrollo de Transferencia de Investigación Matemática a la Empresa

Perfil de Entrada	
Número	**Perfil**
1	Graduados que hayan superado los Títulos de Experto en Ciberseguridad que componen este Master

Procedimiento de Evaluación

Entrega de relaciones de ejercicios.
Entrega de trabajos prácticos.

Objetivos, Proyección profesional, aspectos innovadores...

Los objetivos básicos de este master es el de proporcionar una formación en un campo tan demandado actualmente por las empresas como es la ciberseguridad, abarcando competencias en diversos campos de la misma, algunos básicos, tales como aspectos reguladores y legislativos o estándares criptográficos, y otros más técnicos, abarcando la seguridad en entornos de red, el software y el hardware. Se pretende que el estudiante tenga una formación que le haga tener una visión lo más completa posible de los aspectos a tener en cuenta a la hora de proteger todo tipo de dispositivos y sistemas de comunicación y electrónicos y que pueda ser aplicada en ambientes reales.

Justificación de la conveniencia de su implantación

La cibersegurdidad es un término de reciente creación y que hace referencia tal como se expresa en la Recomendación UITT X.1205, es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de ries- gos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno, que incluyen los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada dicho ciberentorno. La ciberseguridad vela por el mantenimiento de la disponibilidad y de los activos y usuarios, su integridad, la confidencialidad, la autenticidad y el no repudio de los mismos.
Los principales hitos que afectan a la ciberseguridad en nuestro país son la Estrategia española de ciberseguridad (http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf); la Agenda Digital para España (http://www.agendadigital.gob.es/digital- agenda/Documents/digital-agenda-for-spain.pdf) y La Agenda Digital para Europa (http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=EN).
En ellos se recoge la necesidad y obligación de establecer un ciberespacio seguro para un entorno que nos ofrece múltiples oportunidades en el campo comercial, el tecnológico, el científico, el cultural o el de las relaciones sociales, pero que, al mismo tiempo se enfrenta a multitud de retos y amenazas derivados de la interconectividad y el acceso a los dispositivos e información que ofrece el ciberespacio.
Es por ello que son cada vez más las empresas privadas e instituciones públicas que demandan profesionales con una formación específica en el conocimiento y competencias que permitan desarrollar su actividad en el ciberespacio de un modo adecuado y que cumpla con las exigencias que demandan los hitos anteriormente citados.
Actualmente la Universidad de Almería no ofrece ningún título similar de grado o master. Tan solo ciertos aspectos muy genéricos son recogidos en muy determinadas materias dentro de algunos de los títulos anteriormente citados, pero que, evidentemente no son ni mucho menos suficientes para ofrecer una formación en este campo como actualmente están demandando gobiernos, sociedad y empresas.

Gestión de Matrícula

Centro de Postgrado y Formación Continua

Propuesta Inicial de Plazos		
Plazo de Preinscripción	Matriculación sin Preinscripcion	
Fecha de Publicación Listado Provisional	-	
Plazo de Reclamaciones	-	
Fecha de Publicación Listado Definitivo	-	
Plazo de Inscripción	Del día 24/03/2020 al día 31/03/2020	
Llamamiento para cubrir vacante	-	
Fechas de Celebración del Curso	Del día 01/04/2020 al día 30/09/2020	
Turno	**Horario**	**Lugar de realización**
Por determinar	Universidad de Almería	Del día 01/04/2020 al día 30/09/2020

Código:	147379
Fecha:	08/11/2019
Hora:	14:12:53

¿Dónde puede solicitar el alumno información?

Página Web
http://www.ual.es/~cybersecurity

Programación Docente

Num	Denominación del Módulo	Créditos ECTS	Horas	Computable	Trabajo Final	Prácticas Externas
1	Aspectos legales y tratamiento de datos	3	22,5	No	No	No
2	Análisis de riesgos en la protección de datos y privacidad	3	22,5	No	No	No
3	Fundamentos criptográficos de la seguridad.	4	30	No	No	No
4	Seguridad en redes	6	45	No	No	No
5	Investigaciones digitales y análisis forense informático	3	22,5	No	No	No
6	Ingeniería del Software en Proyectos de Seguridad. Desarrollo seguro.	3	22,5	No	No	No
7	Seguridad de datos en sistemas electrónicos	4	30	No	No	No
8	Protección de sistemas electrónicos	2	15	No	No	No
9	Seguridad en entornos IoT	2	15	No	No	No
10	Análisis de malware	4	30	No	No	No
11	Introducción a la BIOS y RAM	2	15	No	No	No
12	Análisis de cifradores y procesos de protección de la información	2	15	No	No	No
13	Ofensiva y defensa en aplicaciones web	3	22,5	No	No	No
14	Blockchain	1	7,5	No	No	No
15	Prácticas externas	12	150	No	No	Sí
16	Trabajo Final de Máster	6	49,5	Sí	Sí	No

Código:	147379
Fecha:	08/11/2019
Hora:	14:12:53

CUADRO DE PROFESORADO

Docente	Datos Personales			Externo UAL	Id	Tipo de cotización	Horas Asignadas	
	Apellidos	Nombre	Sexo				Lectivas	Otras
Sí	Álvarez Bermejo	José Antonio	Varón	No	19575	Prof. funcionario posterior 01/01/2011	0	34,75
Departamento de Informática								
Sí	Fernández Guerrero	José María	Varón	No	19576	PAS funcionario	0	0
Responsable de Datos UAL. Funcionario.								
Sí	Gómez López	Julio	Varón	Sí	19577	Sin asignar	0	0
Experto en seguridad den redes. Profesor de ciclos superiores. Junta de Andalucía.								
Sí	López Ramos	Juan Antonio	Varón	No	19578	Prof. funcionario anterior 31/12/2010	0	34,75
Departamento de Matemáticas								
Sí	Parrilla Roure	Luis	Varón	Sí	19579	Sin asignar	0	0
Profesor Titular de Universidad. Departamento de Electrónica y Tecnología de Computadores - Universidad de Granada.								
Sí	Peralta López	Justo	Varón	No	19580	Prof. funcionario anterior 31/12/2010	0	0
Departamento de Matemáticas								
Sí	Piedra Fernández	María Ángeles	Mujer	No	19581	PAS funcionario	0	0
Asesora Jurídica de la UAL. Funcionaria								
Sí	Sánchez Cordero	Pedro	Varón	Sí	19582	Sin asignar	0	0
CIR-DFIR - Principal Forensics and Threat Hunting en Santander Global Tech.								
Sí	Castillo Morales	Encarnación	Mujer	Sí	19583	Sin asignar	0	0
Profesor Titular de Universidad. Departamento de Electrónica y Tecnología de Computadores - Universidad de Granada.								
Sí	Varela Vaca	Ángel Jesús	Varón	Sí	19592	Sin asignar	0	0
Profesor Ayudante Doctor en la Universidad de Sevilla								

Total	Docentes		No Docentes		Docentes Propios		Docentes Externos	
10	10	100 %	0	0 %	5	50 %	5	50 %

Código:	147379
Fecha:	08/11/2019
Hora:	14:12:53

RELACIÓN DE ACTIVIDADES

Actividades Académicas			Presupuesto Mínimo		Presupuesto Óptimo	
Cod	**Actividad**	**Horas**	**€ / Hora**	**Total**	**€ / Hora**	**Total**
TRIBU	Tribunal	10	4	40 €	49	490 €
TFIN	Trabajo Final	49.5	7	346,5 €	70	3465 €

Dirección y Secretaría			Presupuesto Mínimo		Presupuesto Óptimo	
Cod	**Actividad**	**Horas**	**€ / Hora**	**Total**	**€ / Hora**	**Total**
DIR	Dirección	10	7	70 €	66	660 €

Total	Horas	Presupuesto Mínimo	Presupuesto Óptimo
Total Actividades Académicas	59,5	386,5	3955
Total Dirección y Secretaría	10	70 €	660 €
TOTAL GASTOS PERSONAL:	69,5	456,5 €	4615 €

Código:	147379
Fecha:	08/11/2019
Hora:	14:12:53

CONTENIDO DE LA COLABORACIÓN

Módulo	Actividad	Cod	Profesor	Horas
16	Trabajo Final	TFIN	Álvarez Bermejo José Antonio	24,75
16	Trabajo Final	TFIN	López Ramos Juan Antonio	24,75
Sin Módulo	Tribunal	TRIBU	Álvarez Bermejo José Antonio	5
Sin Módulo	Tribunal	TRIBU	López Ramos Juan Antonio	5
Sin Módulo	Dirección	DIR	Álvarez Bermejo José Antonio	5
Sin Módulo	Dirección	DIR	López Ramos Juan Antonio	5

El porcentaje de horas en actividades docentes asignadas a Docentes Propios de la Universidad (100%) es SUPERIOR al mínimo permitido (20%).

Código:	147379
Fecha:	08/11/2019
Hora:	14:12:53

PRESUPUESTO

GASTOS		
1. Personal	**Presupuesto Mínimo**	**Presupuesto Óptimo**
Profesorado	386,5 €	3955 €
Dirección / Coordinación / Secretaría	70 €	660 €
TOTAL	**456,5 €**	**4615 €**

2. Desplazamientos y Estancias	**Presupuesto Mínimo**	**Presupuesto Óptimo**
Desplazamientos	0 €	0 €
Alojamientos	0 €	0 €
Manutención	0 €	0 €
TOTAL	**0 €**	**0 €**

3. Material Fungible, Inventariable y Bibliografía	**Presupuesto Mínimo**	**Presupuesto Óptimo**
Material de Oficina	0 €	0 €
Material de Laboratorio	0 €	0 €
Reprografía	0 €	0 €
Bibliografía	0 €	0 €
Otros	0 €	0 €
Otros	0 €	0 €

4. Publicidad	**Presupuesto Mínimo**	**Presupuesto Óptimo**
TOTAL	**0 €**	**0 €**

5. Otros Gastos	**Presupuesto Mínimo**	**Presupuesto Óptimo**
Expedición de Títulos	18 €	180 €
Canon becas y otros proyectos (5 %)	30 €	300 €
Importe total de cotizaciones a la seguridad social	27,7324 €	280,361 €
Importe aula virtual	0 €	0 €
Producción Contenidos Digitales	0 €	0 €
Gastos de Gestión por Entidad Externa	0 €	0 €
Otros:	0 €	0 €
TOTAL	**75,73 €**	**760,37 €**

TOTAL DE GASTOS (1 al 5)	**532,23 €**	**5375,37 €**

6. Aportación a la Universidad de Almería	**Presupuesto Mínimo**	**Presupuesto Óptimo**
Aportación 10%	60 €	600 €

TOTAL DE GASTOS	**592,23 €**	**5975,37 €**

Código:	147379
Fecha:	08/11/2019
Hora:	14:12:53

INGRESOS		
7. Subvenciones y Otros Ingresos	**Presupuesto Mínimo**	**Presupuesto Óptimo**
1.	0 €	0 €
2.	0 €	0 €
3.	0 €	0 €
4.	0 €	0 €
TOTAL	**0 €**	**0 €**

8. Remanente Edición Anterior	**Presupuesto Mínimo**	**Presupuesto Óptimo**
TOTAL	**0 €**	**0 €**

9. Precios Públicos	**Presupuesto Mínimo**	**Presupuesto Óptimo**
Número de Alumnos	3 €	30 €
Matrícula 200 €/Alumno. Gestión: Centro de Postgrado y Formación Continua	600 €	6000 €
TOTAL	**600 €**	**6000 €**

TOTAL DE INGRESOS	**600 €**	**6000 €**

RESULTADO PRESUPUESTARIO	**Presupuesto Mínimo**	**Presupuesto Óptimo**
TOTAL	**7,77 €**	**24,63 €**

UNIVERSIDAD DE ALMERÍA

Centro de Formación Continua y Enseñanzas Propias

Denominación del Curso

Master en ciberseguridad

Edición

1

Solicitud de Implantación

Solicito la autorización para la Celebración de la Actividad de Enseñanzas Propias que se acompaña

El Director del Curso

Firma

Juan Antonio López Ramos

Este Centro/Departamento/Vicerrectorado ha acordado dar el visto bueno a la propuesta de organización presentada

Vº Bº Departamento/Centro Organizador

Firma y Sello

RECHE LORITE FERNANDO - 27522012M

Firmado digitalmente por RECHE LORITE FERNANDO - 27522012M
Fecha: 2019.11.08 12:46:17 +01'00'

Fdo: **Fernando Reche Lorite**

Centro/Dpto: **Centro de Desarrollo y Transferencia de I**

Autorizado por el órgano colegiado del Departamento/Centro responsable en sesión de:

Aval de Financiación

Como responsable del Centro de Gastos que se indica a continuación, CERTIFICO que, el mismo se hará cargo de los déficit que pudieran ocasionarse por la actividad (*) caso de que la misma no pueda desarrollarse, o en su defecto, si una vez llegada a su término, ésta resultara deficitaria.

Centro de Gastos: **Centro de Desarrollo de Transferencia de Investigación I**

Número del C.G.: **122040**

Firma y Sello

RECHE LORITE FERNANDO - 27522012M

Firmado digitalmente por RECHE LORITE FERNANDO - 27522012M
Fecha: 2019.11.08 12:46:44 +01'00'

08/11/2019

Fdo: El Responsable C.G.: **Fernando Reche Lorite**

**Si el Curso tuviera excedente económico éste se aplicará al Centro de Gastos que avaló (hasta un 10% del presupuesto).*

SOLICITUD DIRIGIDA AL EXCMO. SR. RECTOR DE LA UNIVERSIDAD DE ALMERÍA

Presentar en el Centro de Formación Continua

PLAN DOCENTE

1.-Descripción del título de Máster propuesto

DENOMINACIÓN	
Máster en ciberseguridad	
Denominación en inglés	
Master in Cybersecurity	
Especialidades/Itinerarios	
Ramas de conocimiento	Ingeniería y Arquitectura

RESPONSABLES DEL TÍTULO			
Unidad Académica Responsable	CDTIME (Centro de) /Departamento de Matemáticas / Departamento de Informática		
Persona de contacto	Juan Antonio López Ramos/José Antonio Álvarez Bermejo		
Correo electrónico	jlopez@ual.es/jaberme@ual.es	**Teléfono**	85722/84439

Tipo de enseñanza (presencial, semipresencial, a distancia; Idioma de Impartición, etc.)
La enseñanza se lleva a cabo de modo semipresencial en idioma español.

Entidades participantes
Departamento de Matemáticas, Departamento de Informática, Centro de Desarrollo y Transferencia de Investigación Matemática a la Empresa (CDTIME)

2.-Justificación del título propuesto

En este apartado se debe incluir información que justifique la relevancia del título conforme a las experiencias formativas o investigadoras del ámbito académico al que hace referencia y/o la consonancia con estudios similares existentes, así como a la adecuación a la demanda social que se realiza desde el entorno cultural, productivo y empresarial y a la demanda de los estudiantes.

2.1 Interés académico, científico o profesional del mismo

La ciberseguridad es un término de reciente creación y que hace referencia tal como se expresa en la recomendación UIT–T X.1205, es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno, que incluyen los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada dicho ciberentorno. La ciberseguridad vela por el mantenimiento de la disponibilidad y de los activos y usuarios, su integridad, la confidencialidad, la autenticidad y el no repudio de los mismos.
Los principales hitos que afectan a la ciberseguridad en nuestro país son la Estrategia española de ciberseguridad (http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf); la Agenda Digital para España (http://www.agendadigital.gob.es/digital- agenda/Documents/digital-agenda-for-spain.pdf) y La Agenda Digital para Europa (http://eur- lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=EN).
En ellos se recoge la necesidad y obligación de establecer un ciberespacio seguro para un entorno que nos ofrece múltiples oportunidades en campos tan diversos como el comercial, el tecnológico, el científico, el cultural o el de las relaciones sociales, pero que, al mismo tiempo se enfrenta a multitud de retos y amenazas derivados de la interconectividad y el acceso a los dispositivos e información que ofrece el ciberespacio.
Es por ello por lo que son cada vez más las empresas privadas e instituciones públicas que demandan profesionales con una formación específica en el conocimiento y competencias que permitan desarrollar su actividad en el ciberespacio de un modo adecuado y que cumpla con las exigencias que demandan los hitos anteriormente citados.
Actualmente la Universidad de Almería no ofrece ningún título similar de grado o máster. Tan solo ciertos aspectos muy genéricos son recogidos en muy determinadas materias dentro de algunos de los títulos anteriormente citados, tales como el grado en Ingeniería Informática, o el máster interuniversitario en Matemáticas, pero que, evidentemente no son ni mucho menos suficientes para ofrecer una formación en este campo como actualmente están demandando gobiernos, sociedad y empresas.
En el aspecto científico, la creación de un máster propio de la temática como la que se propone en esta solicitud tiene también indudables consecuencias. El hecho de disponer de estudiantes con una formación amplia en diversos aspectos de la ciberseguridad repercutirá sin duda en la potenciación de algunos grupos de investigación de la Universidad de Almería, tales como "Categorías, Computación y Teoría de Anillos", grupo al que pertenecen las personas responsables de esta solicitud o "Informática Aplicada", ambos incluidos en el mapa I+D+I en ciberseguridad de la Red de Excelencia Nacional de Investigación en Ciberseguridad, que podrán aprovecharse de esta formación para incluir nuevos miembros, fortalecer la formación de los mismos y explorar nuevas vías de investigación resultantes del trabajo llevado a cabo, así como participar en los numerosísimos eventos sobre ciberseguridad que durante los últimos años se vienen celebrando en nuestro país, cuyo listado puede ser accesible en gran parte a través de la agenda del Instituto Nacional de Ciberseguridad en https://www.incibe.es/agenda o en https://www.elevenpaths.com/es/noticias-y-eventos/eventos/index.html, algunos de los cuales se han convertido ya eventos regulares y de referencia para investigadores y estudiantes en ciberseguridad, como las Jornadas Nacionales de Investigación en Ciberseguridad (https://www.incibe.es/red-excelencia-idi-ciberseguridad/jnic), Cybercamp (https://www.incibe.es/agenda/cybercamp-2019) o la Reunión Española sobre Criptología y Seguridad de la Información (https://nesg.ugr.es/recsi2018/).

2.2 Antecedentes

Juan Antonio López Ramos ha sido miembro del comité coordinador de la Red de Excelencia Nacional "Matemáticas en la Sociedad de la Información, MatSI" entre 2015 y 2018. Además, tal y como se ha puesto de manifiesto anteriormente, las personas responsables de esta solicitud son, ambos, miembros del grupo de investigación "Categorías, Computación y Teoría de Anillos", en el cual vienen desarrollando su principal línea de investigación en áreas concretas de la ciberseguridad, en concreto, en la protección física de datos y sistemas de información, lo que les ha llevado a un amplio catálogo de publicaciones científicas en revistas con índice de impacto en la base de datos Journal Citation Reports (JCR) y actas de congresos nacionales e internacionales, así como la organización de varios congresos y sesiones especiales en congresos internacionales, como "I Congreso Nacional sobre Desarrollo de Software Seguro, SuperSec 2018", en Almería en 2018; "Mathematics in the Information Society", sesión especial dentro del congreso internacional CMMSE 2017 en Cádiz en 2017; "Crypto and Codes", sesión especial dentro del congreso internacional CMMSE 2013 en Almería en 2013; "Crypto and Codes", sesión especial dentro del congreso internacional CMMSE 2012 en Murcia en 2012; "Applications of Algebra to Coding Theory and Cryptography", sesión especial dentro del congreso internacional CMMSE 2010 en Almería en 2010. Del mismo modo, ambos solicitantes han participado como miembros del comité científico de diversos congresos y eventos internacionales, así como revisores expertos para publicaciones científicas internacionales con impacto JCR.

En el apartado docente, Juan Antonio López Ramos ha sido docente en las asignaturas de grado "Criptografía", "Teoría de Códigos y Criptografía" y "Seguridad TIC", impartidas en diversos estudios en la Universidad de Almería y, como miembro coordinador de la red de excelencia MatSI durante el periodo anteriormente citado, ha organizado diversas escuelas de verano y de doctorado para estudiantes con la protección de la información como temática principal en diversas universidades españolas.

Además de contar con una amplia experiencia investigadora, José Antonio Álvarez Bermejo, ostenta el premio NordicIOT 2015 por desarrollo de firmware seguro y tiene en su haber el mérito de haber formado a las FF.CC.S.E. (Guardia Civil y Policía Nacional) en la búsqueda de perfiles en redes a partir de información de inteligencia extraída de las darknets.

2.3 Potenciales interesados (demanda de los estudiantes)

La oferta educativa que se pretende ofrecer es un complemento natural para estudiantes con un grado en Ingeniería Informática o en Ingeniería Electrónica, dado que el estudiante que curse este master tendrá una amplia visión de todos los aspectos que cubre la ciberseguridad, desde el software, a los dispositivos hardware y a las redes de comunicación entre dichos dispositivos. Del mismo modo puede ser de interés para un graduado en Matemáticas con suficientes conocimientos sobre sistemas de información, dado su amplia formación en técnicas matemáticas aplicables tanto a la protección de la información, como al análisis de posibles defectos en el diseño de los sistemas y técnicas de protección.

Por otro lado, profesionales cualificados en áreas afines a la seguridad, como policías, militares o administradores de sistemas de información de empresas pueden ver igualmente en esta oferta docente una oportunidad para ampliar conocimientos, perfeccionar sus competencias y/o mantenerse al día en los últimos desarrollos en el ámbito de la ciberseguridad.

2.4 Adecuación a la demanda social que se realiza desde el entorno cultural, productivo y empresarial

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales regula en nuestro país el tratamiento de cualquier tipo de información personal en lo que respecta a todos los ámbitos de nuestra vida, tanto privados, como profesionales. Una sociedad basada en la interconectividad y el intercambio de información que ofrece el cada vez más extendido ciberespacio, hace necesaria una estrategia que permita el desarrollo de la actividad de una forma segura, es decir, estrategias para la ciberseguridad.

Tal y como ya se ha señalado anteriormente, los principales hitos que afectan a la ciberseguridad en nuestro país , son la Estrategia española de ciberseguridad (http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf); la Agenda Digital para España (http://www.agendadigital.gob.es/digital- agenda/Documents/digital-agenda-for-spain.pdf) y La Agenda Digital para Europa (http://eur- lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=EN), además. En ellos se recoge la necesidad y obligación de establecer un ciberespacio seguro.

Cabe destacar la gran campaña de concienciación a nivel particular y empresarial que están llevando a cabo organismos oficiales como el INCIBE y el Centro Criptológico Nacional (CCN) sobre la necesidad de la formación en ciberseguridad. En este contexto, podemos citar el encuentro llevado a cabo el pasado 28 de marzo de 2019 en el Parque Industrial y Tecnológico de Almería, al que los solicitantes pudieron asistir como invitados, y en el que un asesor del CCN y un consultor experto de IBM intervinieron para concienciar a las empresas más importantes del tejido empresarial almeriense de la necesidad de profundizar en este aspecto clave para el futuro desarrollo económico de nuestra provincia, quedando de manifiesto por parte de estas empresas sus necesidades para formar y contratar personal en el ámbito de la ciberseguridad.

2.5 Objetivos formativos

Los objetivos formativos que se pretenden mediante esta oferta docente son:

- Ofrecer una formación general sobre los distintos ámbitos que se ven afectados por la ciberseguridad, tanto en la parte técnica, como en el marco regulador.
- Comprender los retos de implantación y las vulnerabilidades a las que se enfrenta el profesional en el ciberespacio.
- Tener una visión actual sobre las últimas técnicas y avances en ciberseguridad.

En definitiva, proporcionar al estudiante o profesional de la ciberseguridad los conocimientos y técnicas más actuales que le permitan el desarrollo de su actividad de un modo profesional y ajustado a la legislación.

3.-Competencias

3.1. Competencias Básicas y Generales

Básicas

1.Poseer y comprender conocimientos.
2.Aplicación de conocimientos.
3.Capacidad de emitir juicios.
4.Capacidad de comunicar y aptitud social.
5.Habilidad para el aprendizaje.

Generales

Las competencias genéricas incluidas en el Real Decreto 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales

3.2. Competencias Transversales

Conocimientos básicos de la profesión.
Habilidad en el uso de las TIC.
Capacidad para resolver problemas.
Comunicación oral y escrita en la propia lengua.
Capacidad de crítica y autocrítica.
Trabajo en equipo.
Conocimiento de una segunda lengua.
Compromiso ético.
Capacidad para aprender a trabajar de forma autónoma.
Competencia social y ciudadanía global.

3.3. Competencias Específicas

- Conocimiento marco legal en el tratamiento de datos.
- Conocimiento del marco de gestión de datos en una organización.
- Conocimiento de la figura, papel y función del Delegado de Protección de Datos de una empresa o institución.
- Ser capaz de analizar riesgos y brechas de seguridad en el tratamiento de la información.
- Conocimiento y uso de técnica avanzadas para la gestión y la protección de la información.
- Conocimiento y uso de técnicas avanzadas para la autenticación de la información.
- Conocimiento y uso de técnicas avanzadas para el control de acceso a servicios de información.
- Conocimiento y uso de técnicas avanzadas para la gestión y la protección de redes de comunicaciones.
- Conocimiento y uso de técnicas de comunicación en grupos.
- Conocimiento y uso de técnicas avanzadas para la gestión de la información.
- Conocimiento y uso de técnicas de inteligencia artificial y sistemas basados en conocimiento.
- Conocimiento y uso de técnicas informáticas avanzadas para la investigación y el análisis en el entorno industrial.
- Conocimiento y uso de técnicas avanzadas para la programación y control de dispositivos hardware.
- Conocimiento y uso de técnicas de optimización en problemas de ingeniería
- Conocimiento y uso de técnicas avanzadas para la gestión y la protección de dispositivos hardware.

4.-Requisitos de Acceso y Admisión de estudiantes

Títulos de experto de la UAL en Ciberseguridad y Ciberseguridad Avanzada y Protección de Datos .

5.-Sistema de reconocimientos y Transferencia de Créditos

Ambos títulos de experto suponen el reconocimiento de los 42 créditos lectivos correspondientes a los módulos docentes además de 12 créditos de prácticas en empresa.

6.- Planificación de las enseñanzas

6.1. Actividades Formativas

6.2. Metodologías docentes

Clases magistrales. Supuestos prácticos y Trabajo en Grupo.
Respecto al Trabajo en Grupo se procederá a la elaboración de resoluciones de los supuestos prácticos que se planteen, siendo posteriormente expuestos en debate.

6.3. Sistemas de evaluación

Casos prácticos y debate sobre los mismos.
Participación en el aula virtual y en los foros para cada caso práctico.
Trabajo individual que consistirá en la resolución de un caso práctico que será facilitado por el profesor de las materias objeto de la asignatura.

7.-Distribución de Créditos

CARGA LECTIVA	ECTS	Itinerario 1	Itinerario 2
Básicas			
Obligatorias	42		
Optativas			
Prácticas externas	12		
Trabajo de fin de Grado / Máster	6		
Total			

El máster propio debe tener de 60 a 120 ECTS. 60 ECTS por curso y 30 ECTS por cuatrimestre.
Los contenidos del máster que den lugar a una especialidad deben ser tratados como optativos.
El título tendrá un único trabajo final de entre 6 y 30 ECTS. Para los másteres con perfil investigador es recomendable que tenga una duración de 12 ECTS.

8.-Estructura del Título.

Describa la Estructura del Título: Módulos que lo compondrían, créditos a superar en cada uno de ellos. Detalle el itinerario que seguiría el estudiante para alcanzar el título, diferenciando los módulos que lo componen y, especialmente, las componentes optativas que existan en el título.

El curso se compone de diecisiete módulos, que suponen un total de 42 créditos más 12 créditos de prácticas en empresas y seis créditos de trabajo fin de máster.

9.- Descripción del Título

***Para cada uno de los módulos** que componen el título deberá especificar los datos generales, resultado del aprendizaje, enumeración de los contenidos del módulo, competencias, actividades formativas, metodologías docentes, el sistema de evaluación a aplicar y bibliografía.*

DENOMINACIÓN DEL MÓDULO					
Aspectos legales y tratamiento de datos.					
DENOMINACIÓN EN INGLÉS					
Legal aspects and data processing.					
CRÉDITOS ECTS:	3	**CUATRIMESTRE**	1	**CARÁCTER** (Obligatoria/ Optativa)	Obligatorio
DISTRIBUCIÓN DE CRÉDITOS					
	Presenciales		**OnLine**		
Teóricos			1.5		
Prácticos			1.5		

RESULTADOS DEL APRENDIZAJE

El principal objetivo de este módulo es que el estudiante conozca las normas que componen el marco jurídico en materia de Protección de Datos que están vigentes en la Unión Europea (RGPD) y en el ámbito nacional (LOPDgdd).

Así mismo, se abordará el sistema de garantía de los derechos digitales que, inequívocamente, encuentra su anclaje en el mandato impuesto por el artículo 18.4 de la Constitución Española, que establece: “La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”.

Por ello, siendo evidente que Internet se ha convertido en una realidad omnipresente tanto en nuestra vida personal como colectiva, toda vez que gran parte de nuestra actividad profesional, económica y privada se desarrolla en la Red y adquiere una importancia fundamental tanto para la comunicación humana como para el desarrollo de nuestra vida en sociedad, es básico que el estudiante sepa identificar con claridad los riesgos y oportunidades que el mundo de las redes ofrece, al objeto de poder ejercer los derechos que le asisten.

Especial consideración se hará a la nueva figura del Delegado de Protección de Datos, nuevo perfil profesional cuyas funciones, entre otras, serán informar y asesorar al responsable o, en su caso, al encargado del tratamiento y a los empleados de sus obligaciones y supervisar el cumplimiento en la protección de datos dentro de la organización o empresa.

En definitiva, en esta asignatura se pretende que el alumno tenga una visión general sobre los conceptos relacionados con la privacidad, abordando en profundidad el estudio de la Protección de Datos.

CONTENIDOS

Tema 1. El Derecho Fundamental a la Protección de Datos. Principios de protección. Especial consideración al consentimiento.

Tema 2. Derechos de los interesados y ejercicio de los derechos. Derechos digitales.

Tema 3. Disposiciones aplicables a tratamiento concretos. Obligaciones del Responsable y del Encargado del Tratamiento.

Tema 4. Medidas de Seguridad en la Protección de Datos Personales.

Tema 5 Gestión de las Organizaciones. Evaluaciones de impacto y análisis de riesgos.

Tema 6. Brechas de seguridad.

Tema 7. El Delegado de Protección de Datos. Perfil y responsabilidades.

OBSERVACIONES

COMPETENCIAS

Competencias básicas y generales

1. Poseer y comprender conocimientos.
2. Aplicación de conocimientos.
3. Capacidad de emitir juicios.
4. Capacidad de comunicar y aptitud social.
5. Habilidad para el aprendizaje.

Competencias transversales

1. Conocimientos básicos de la profesión.
2. Compromiso ético.

Competencias específicas

1. Conocimiento marco legal en el tratamiento de datos.
2. Conocimiento del marco de gestión de datos en una organización.
3. Ser capaz de analizar riesgos y brechas de seguridad en el tratamiento de la información.

ACTIVIDADES FORMATIVAS

METODOLOGÍAS DOCENTES

Clases magistrales. Supuestos prácticos y Trabajo en Grupo.
Respecto al Trabajo en Grupo se procederá a la elaboración de resoluciones de los supuestos prácticos que se planteen, siendo posteriormente expuestos en debate.

SISTEMAS DE EVALUACIÓN DE COMPETENCIAS

1. Casos prácticos y debate sobre los mismos.
2. Participación en el aula virtual y en los foros para cada caso práctico.
3. Trabajo individual que consistirá en la resolución de un caso práctico que será facilitado por el profesor de las materias objeto de la asignatura.

BIBLIOGRAFÍA

Reglamento General de Protección de Datos: Contiene introducción al Reglamento, concordancias e índice analítico. Colex; Edición: 1 (25 de julio de 2018). 978-8417135799

DENOMINACIÓN DEL MÓDULO					
Fundamentos criptográficos de la ciberseguridad					
DENOMINACIÓN EN INGLÉS					
Cryptographic basics of Cybersecurity					
CRÉDITOS ECTS:	4	**CUATRIMESTRE**	1	**CARÁCTER** (Obligatoria/ Optativa)	Obligatorio

DISTRIBUCIÓN DE CRÉDITOS		
	Presenciales	**OnLine**
Teóricos		2
Prácticos		2

RESULTADOS DEL APRENDIZAJE

Con este módulo se pretende que el estudiante conozca las distintas aplicaciones de la Criptografía en Ciberseguridad; sea capaz de distinguir de cifrados en bloque simétricos y de clave pública, conociendo los estándares actuales recomendados, y sea capaz de decidir la conveniencia del uso de unos u otros dependiendo del contexto e infraestructura en los que serán usados, así como el conocimiento de los distintos modos de cifrado en bloque.
Además, el estudiante conocerá la construcción de las firmas digitales y su uso en Criptografía, para lo cual se hace necesario además el concepto de infraestructura de clave pública: construcción de certificados digitales y su uso en Ciberseguridad para el acceso a servicios o comunicaciones punto a punto o en grupo. Finalmente, el alumno tendrá una visión general del futuro de la ciberseguridad con el avance de la computación cuántica.

CONTENIDOS

1. Cifrados de clave simétrica.
2. El estándar AES.
3. Otros cifrados simétricos: IDEA, Feal, Skipjack, RC6.
4. Modos de cifrado: ECB, CBC, CFB, OFB.
5. Funciones de una sola vía.
6. Cifrados de clave pública.
7. Los estándares RSA y ECC.
8. Autenticación y firmas digitales.
9. Funciones Hash.
10. Distribución de claves públicas.
11. Certificados digitales.
12. Pretty Good Privacy.
13. El estándar X.509.
14. Almacenamiento de claves.
15. Identificación y autenticación de entidades.
16. Distribución de claves en grupos.
17. Amenazas y retos para la criptografía postcuantica.

OBSERVACIONES

Nociones básicas de conceptos matemáticos sobre Teoría de Números y Cuerpos Finitos pueden ayudar a una mejor asimilación de los contenidos, aunque no de un modo determinante.
Se hará uso de software gratuito.

COMPETENCIAS

Competencias básicas y generales

1. Poseer y comprender conocimientos.
2. Aplicación de conocimientos.
3. Capacidad de emitir juicios.
4. Capacidad de comunicar y aptitud social.
5. Habilidad para el aprendizaje.

Competencias transversales

1. Conocimientos básicos de la profesión.
2. Capacidad para resolver problemas.

Competencias específicas

1. Conocimiento y uso de técnica avanzadas para la gestión y la protección de la información.
2. Conocimiento y uso de técnicas avanzadas para la autenticación de la información.
3. Conocimiento y uso de técnicas avanzadas para el control de acceso a servicios de información.

ACTIVIDADES FORMATIVAS

METODOLOGÍAS DOCENTES

Los contenidos teóricos serán desarrollados a partir de material docente preparado por el profesorado para tal efecto y complementado con un sistema de tutorías online para resolver cualquier duda o cuestión al respecto del material docente.

En el apartado práctico se realizarán una serie de guiones prácticos preparados por el profesorado, que permitirán asimilar adecuadamente los contenidos teóricos y poner en una situación real de aplicación al estudiante.

SISTEMAS DE EVALUACIÓN DE COMPETENCIAS

La evaluación del estudiante se llevará a cabo atendiendo a tres apartados:

1. Realización de actividades individuales. Cada alumno deberá ser capaz de plantear y resolver situaciones o escenarios concretos en diversos apartados del curso. Las actividades se realizarán de forma individualizada, con el apoyo del material del curso.
2. Realización de algún caso práctico propuesto que se llevará a cabo con los recursos recomendados por el profesorado.
3. Participación en el aula virtual de forma activa en los diversos foros de comunicación.

BIBLIOGRAFÍA

Bruce Schneier. Applied Cryptography. Wiley & Sons. 1996.

Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone. Handbook of Applied Criptography. CRC Press. 1997.

Wade Trappe, Lawernce C. Washington. Introduction to criptography with coding theory. Prentice-Hall, Inc.. 2004.

Christof Paar, Jan Pelzl. Understanding Cryptography: A Textbook for Students and Practitioners. Springer. 2008.

Amparo Fuster Sabater, Luis Hernández Encinas, Fausto Montoya Vitini, Jaime Muñoz Masque. Criptografía, protección de datos y aplicaciones. Una guía para estudiantes y profesionales. Ra-Ma. 2012

DENOMINACIÓN DEL MÓDULO					
Introducción a la seguridad en redes					
DENOMINACIÓN EN INGLÉS					
Introduction to network security					
CRÉDITOS ECTS:	3	**CUATRIMESTRE**	2	**CARÁCTER** (Obligatoria/ Optativa)	Obligatorio

DISTRIBUCIÓN DE CRÉDITOS		
	Presenciales	**OnLine**
Teóricos		1.5
Prácticos		1.5

RESULTADOS DEL APRENDIZAJE

El objetivo de este módulo es que el alumnado conozca los fundamentos de la seguridad en redes de datos, así como entender su estructura y funcionamiento para crear una red que conecte de forma eficiente y segura los equipos de usuario, servidores y la red externa (Internet).

CONTENIDOS

1. Esquemas de red.
2. Seguridad en redes cableadas.
3. Seguridad en redes inalámbricas.
4. Seguridad en las comunicaciones.
5. Hacking ético y test de penetración. Introducción
    1. Hacking ético en la auditoría de seguridad
    2. Black hat y white hat
6. Hacking ético en acción
    1. Footprinting
        1. Shodan
        2. Google Hacking Database
        3. OSINT
    2. Fingerprinting
        1. Nmap
    3. Escaneo de vulnerabilidades
        1. CVE
        2. NVD
7. Conclusiones

OBSERVACIONES

COMPETENCIAS

Competencias básicas y generales

1. Poseer y comprender conocimientos.
2. Aplicación de conocimientos.
3. Capacidad de emitir juicios.
4. Capacidad de comunicar y aptitud social.
5. Habilidad para el aprendizaje.

Competencias transversales

1. Habilidad en el uso de las TIC.
2. Capacidad para resolver problemas.
3. Capacidad para trabajar de forma autónoma.

Competencias específicas

1. Conocimiento y uso de técnicas avanzadas para la gestión y la protección de redes de comunicaciones.
2. Conocimiento y uso de técnicas de comunicación en grupos.

ACTIVIDADES FORMATIVAS

METODOLOGÍAS DOCENTES

Los contenidos teóricos serán desarrollados a partir de material docente preparado por el profesorado para tal efecto y complementado con un sistema de tutorías online para resolver cualquier duda o cuestión al respecto del material docente.

En el apartado práctico se realizarán una serie de guiones prácticos preparados por el profesorado, que permitirán asimilar adecuadamente los contenidos teóricos y poner en una situación real de aplicación al estudiante.

SISTEMAS DE EVALUACIÓN DE COMPETENCIAS

1. Realización de actividades individuales. Cada alumno deberá ser capaz de plantear y resolver situaciones o escenarios concretos en diversos apartados del curso. Las actividades se realizarán de forma individualizada, con el apoyo del material del curso.

2. Realización de algún caso práctico propuesto que se llevará a cabo con los recursos recomendados por el profesorado.
3. Participación en el aula virtual de forma activa en los diversos foros de comunicación.

BIBLIOGRAFÍA

José Manuel Huidobro Moya, David Roldán Martínez. Seguridad en redes y sistemas informáticos. Thomson Paraninfo S.A.. 2005.

Andrew S. Tanenbaum. Redes de computadores. Prentice-Hall, Pearson, Addison Wesley. 1997.

DENOMINACIÓN DEL MÓDULO					
Investigaciones digitales y análisis forense informático					
DENOMINACIÓN EN INGLÉS					
Digital Investigations and Computer Forensics					
CRÉDITOS ECTS:	3	**CUATRIMESTRE**	2	**CARÁCTER** (Obligatoria/ Optativa)	Obligatoria

DISTRIBUCIÓN DE CRÉDITOS		
	Presenciales	**OnLine**
Teóricos		1.5
Prácticos		1.5

RESULTADOS DEL APRENDIZAJE

Se pretende que el alumno sea capaz de analizar el entorno tras un incidente. No sólo de dar una respuesta a qué elemento ha sido el causante y cual el vector de ataque sino además de tratar de dar una respuesta al incidente. De la rápida actuación de los profesionales DFIR depende evitar la propagación de una infección que pueda causar males mayores. Además de tratar de atribuirla a una organización o individuo.

CONTENIDOS

1-INTRODUCCION
2-METODOLOGIA
3-ADQUISICION-CLONADO
4-ARTEFACTOS
5- ARQUITECTURA-WINDOWS
6-ATAQUES_LATERALES
7-DETECTANDO ROOTKITS

8-AUDIT-POWERSHELL
9-INDICADORES COMPROMISOs
10-ANALISIS_DE_MEMORIA_RAM
11-AUTOPSY
12-ANALISIS DE RED
13-SISTEMA_DE_FICHEROS
14-IR-Tools - SYSMON
15-IR-Tools - LOKI

OBSERVACIONES

COMPETENCIAS

Competencias básicas y generales

1. Poseer y comprender conocimientos.
2. Aplicación de conocimientos.
3. Capacidad de emitir juicios.
4. Capacidad de comunicar y aptitud social.
5. Habilidad para el aprendizaje.

Competencias transversales

1. Habilidad en el uso de las TIC.
2. Capacidad para resolver problemas.
3. Capacidad para trabajar de forma autónoma.

Competencias específicas

1. Conocimiento y uso de técnicas avanzadas para la gestión de incidentes relacionados con la información.
2. Resolución de problemas relacionados con hardware.

ACTIVIDADES FORMATIVAS

METODOLOGÍAS DOCENTES

Los contenidos teóricos serán desarrollados a partir de material docente preparado por el profesorado para tal efecto y complementado con un sistema de tutorías online para resolver cualquier duda o cuestión al respecto del material docente.

En el apartado práctico se realizarán una serie de guiones prácticos preparados por el profesorado, que permitirán asimilar adecuadamente los contenidos teóricos y poner en una situación real de aplicación al estudiante.

SISTEMAS DE EVALUACIÓN DE COMPETENCIAS

1.Realización de actividades individuales. Cada alumno deberá ser capaz de plantear y resolver situaciones o escenarios concretos en diversos apartados del curso. Las actividades se realizarán de forma individualizada, con el apoyo del material del curso.
2.Realización de algún caso práctico propuesto que se llevará a cabo con los recursos recomendados por el profesorado.
3.Participación en el aula virtual de forma activa en los diversos foros de comunicación.

BIBLIOGRAFÍA

Ultimate DFIR Cheats! Windows Forensic Environment.Independently published (5 de febrero de 2019) Ultimate DFIR Cheats! ISBN-13: 978-1790322787

DENOMINACIÓN DEL MÓDULO					
Ingeniería del Software en Proyectos de Seguridad. Desarrollo seguro.					
DENOMINACIÓN EN INGLÉS					
Software engineering in Security Projects. Secure Development					
CRÉDITOS ECTS:	3	**CUATRIMESTRE**	2	**CARÁCTER** (Obligatoria/ Optativa)	Obligatoria

DISTRIBUCIÓN DE CRÉDITOS		
	Presenciales	**OnLine**
Teóricos	1.5	
Prácticos		1.5

RESULTADOS DEL APRENDIZAJE

El alumno debe ser capaz de establecer las relaciones entre el software que desarrolla y el hardware que estará a su disposición. Esta relación implica potenciales vulnerabilidades. Que pueden acentuarse si el software no contempla unos requisitos mínimos de seguridad.

El alumno será expuesto a las técnicas de control de software con las que podrá determinar si el software que ha desarrollado puede ser vulnerable a buffers overflows o a otros ataques, como por ejemplo a los que se expone con la incorporación de librerías de terceros no controladas.

CONTENIDOS

- Introducción al desarrollo seguro.
  - Principios de seguridad.
  - Modelado de amenazas.
- Técnicas de codificación segura.
- Appropriate Access Control (ACL). Ejecución bajo el menor privilegio.
- Problemas generados al no prestar atención a la criptografía. Protección de datos.
- Análisis de Riesgos
- Introducción
  - Conceptos principales
  - Evaluación de vulnerabilidades
- Análisis y gestión de riesgos
  - Fundamentos de ISO 27005:2018
  - Identificación del contexto y activos
  - Análisis y valoración de riesgos
  - Evaluación y gestión de riesgos
- Conclusiones

OBSERVACIONES

COMPETENCIAS

Competencias básicas y generales

1. Poseer y comprender conocimientos.
2. Aplicación de conocimientos.
3. Capacidad de emitir juicios.
4. Capacidad de comunicar y aptitud social.
5. Habilidad para el aprendizaje.

Competencias transversales

1. Habilidad en el uso de las TIC.
2. Capacidad para resolver problemas.
3. Capacidad para trabajar de forma autónoma.

Competencias específicas

Conocimiento y uso de técnicas avanzadas para la gestión de la información

Conocimiento y uso de técnicas de inteligencia artificial y sistemas basados en conocimiento

Conocimiento y uso de técnicas informáticas avanzadas para la investigación y el análisis en el entorno industrial.

ACTIVIDADES FORMATIVAS

METODOLOGÍAS DOCENTES

Los contenidos teóricos serán desarrollados a partir de material docente preparado por el profesorado para tal efecto y complementado con un sistema de tutorías online para resolver cualquier duda o cuestión al respecto del material docente.

En el apartado práctico se realizarán una serie de guiones prácticos preparados por el profesorado, que permitirán asimilar adecuadamente los contenidos teóricos y poner en una situación real de aplicación al estudiante.

SISTEMAS DE EVALUACIÓN DE COMPETENCIAS

1. Realización de actividades individuales. Cada alumno deberá ser capaz de plantear y resolver situaciones o escenarios concretos en diversos apartados del curso. Las actividades se realizarán de forma individualizada, con el apoyo del material del curso.
2. Realización de algún caso práctico propuesto que se llevará a cabo con los recursos recomendados por el profesorado.

3. Participación en el aula virtual de forma activa en los diversos foros de comunicación.

BIBLIOGRAFÍA
Writing Secure Code. Microsoft Press; ISBN-13: 978-0735617223 Secure Programming with Static Analysis. Addison-Wesley Professional (July 9, 2007). ISBN-13: 978-0321424778 Secure Coding in C and C++ (2nd Edition) (SEI Series in Software Engineering) 2nd Edition

DENOMINACIÓN DEL MÓDULO					
Seguridad de datos en sistemas electrónicos					
DENOMINACIÓN EN INGLÉS					
Data security in electronic devices					
CRÉDITOS ECTS:	4	**CUATRIMESTRE**	2	**CARÁCTER** (Obligatoria/ Optativa)	Obligatorio
DISTRIBUCIÓN DE CRÉDITOS					
	Presenciales		**OnLine**		
Teóricos			2		
Prácticos			2		

RESULTADOS DEL APRENDIZAJE

El estudiante ha de ser capaz de dar proveer soluciones para el problema de la integridad de los datos procesados y/o comunicados en un contexto de interconexión global de sistemas electrónicos para comunicaciones, tele-control y gestión remota.

CONTENIDOS

6. Autentificación de dispositivos: Physically Unclonable Functions (PUFs).
7. Procesadores criptográficos.

OBSERVACIONES

Conocimientos sobre algoritmos y protocolos criptográficos son necesarios para una buena comprensión de los conceptos tratados en el módulo.

COMPETENCIAS

Competencias básicas y generales

8. Poseer y comprender conocimientos.
9. Aplicación de conocimientos.
10. Capacidad de emitir juicios.
11. Capacidad de comunicar y aptitud social.
12. Habilidad para el aprendizaje.

Competencias transversales

1. Habilidad en el uso de las TIC.
2. Capacidad para resolver problemas.
3. Capacidad para trabajar de forma autónoma.

Competencias específicas

1. Conocimiento y uso de técnicas avanzadas para la gestión y la protección de la información.
2. Conocimiento y uso de técnicas avanzadas para la autenticación de la información.
3. Conocimiento y uso de técnicas avanzadas para la programación y control de dispositivos hardware.
4. Conocimiento y uso de técnicas de optimización en problemas de ingeniería

ACTIVIDADES FORMATIVAS

METODOLOGÍAS DOCENTES

Los contenidos teóricos serán desarrollados a partir de material docente preparado por el profesorado para tal efecto y complementado con un sistema de tutorías online para resolver cualquier duda o cuestión al respecto del material docente.

En el apartado práctico se realizarán una serie de guiones prácticos preparados por el profesorado, que permitirán asimilar adecuadamente los contenidos teóricos y poner en una situación real de aplicación al estudiante.

SISTEMAS DE EVALUACIÓN DE COMPETENCIAS

1. Realización de actividades individuales. Cada alumno deberá ser capaz de plantear y resolver situaciones o escenarios concretos en diversos apartados del curso. Las actividades se realizarán de forma individualizada, con el apoyo del material del curso.
2. Realización de algún caso práctico propuesto que se llevará a cabo con los recursos recomendados por el profesorado.
3. Participación en el aula virtual de forma activa en los diversos foros de comunicación.

BIBLIOGRAFÍA

Christof Paar, Jan Pelzl. Understanding Cryptography: A Textbook for Students and Practitioners. Springer. 2008.

Mohammad Tehranipoor, Cliff Wang. Introduction to hardware security and trust. Springer Science & Business Media. 2012.

Lilian Bossuet, Lionel Torres. Foundations of Hardware IP Protection. Springer. 2017.

DENOMINACIÓN DEL MÓDULO					
Protección de sistemas electrónicos					
DENOMINACIÓN EN INGLÉS					
Protection of electronic devices					
CRÉDITOS ECTS:	2	**CUATRIMESTRE**	2	**CARÁCTER** (Obligatoria/ Optativa)	Obligatorio

DISTRIBUCIÓN DE CRÉDITOS		
	Presenciales	**OnLine**
Teóricos		1
Prácticos		1

RESULTADOS DEL APRENDIZAJE

En el contexto actual de interconexión global de sistemas electrónicos para comunicaciones, tele-control y gestión remota se hace imprescindible el garantizar la seguridad de los mismos frente a intentos de modificación maliciosa del funcionamiento. El objeto fundamental de aprendizaje es que el estudiante aborde forma exitosa el problema de la seguridad hardware desde el punto de vista de la protección del funcionamiento.

CONTENIDOS

1. Protección ante ataques laterales.
2. Protección ante troyanos hardware.
3. Técnicas de activación hardware.

OBSERVACIONES

COMPETENCIAS

Competencias básicas y generales

1. Poseer y comprender conocimientos.
2. Aplicación de conocimientos.
3. Capacidad de emitir juicios.
4. Capacidad de comunicar y aptitud social.
5. Habilidad para el aprendizaje.

Competencias transversales

1. Habilidad en el uso de las TIC.
2. Capacidad para resolver problemas.
3. Capacidad para trabajar de forma autónoma.

Competencias específicas

1. Conocimiento y uso de técnicas avanzadas para la gestión y la protección de la dispositivos hardware.
2. Conocimiento y uso de técnicas avanzadas para la programación y control de dispositivos hardware.
3. Conocimiento y uso de técnicas de optimización en problemas de ingeniería.

ACTIVIDADES FORMATIVAS

METODOLOGÍAS DOCENTES

Los contenidos teóricos serán desarrollados a partir de material docente preparado por el profesorado para tal efecto y complementado con un sistema de tutorías online para resolver cualquier duda o cuestión al respecto del material docente.

En el apartado práctico se realizarán una serie de guiones prácticos preparados por el profesorado, que permitirán asimilar adecuadamente los contenidos teóricos y poner en una situación real de aplicación al estudiante.

SISTEMAS DE EVALUACIÓN DE COMPETENCIAS

1. Realización de actividades individuales. Cada alumno deberá ser capaz de plantear y resolver situaciones o escenarios concretos en diversos apartados del curso. Las actividades se realizarán de forma individualizada, con el apoyo del material del curso.
2. Realización de algún caso práctico propuesto que se llevará a cabo con los recursos recomendados por el profesorado.
3. Participación en el aula virtual de forma activa en los diversos foros de comunicación.

BIBLIOGRAFÍA

Christof Paar, Jan Pelzl. Understanding Cryptography: A Textbook for Students and Practitioners. Springer. 2008.

Mohammad Tehranipoor, Cliff Wang. Introduction to hardware security and trust. Springer Science & Business Media. 2012.

Lilian Bossuet, Lionel Torres. Foundations of Hardware IP Protection. Springer. 2017.

Domenic Forte, Swarup Bhunia, Mohammad Tehranipoor. Hardware Protection through Obfuscation. Springer, *2017.*

DENOMINACIÓN DEL MÓDULO					
Fundamentos del análisis de malware					
DENOMINACIÓN EN INGLÉS					
Malware análisis foundations					
CRÉDITOS ECTS:	3	**CUATRIMESTRE**	2	**CARÁCTER** (Obligatoria/ Optativa)	Obligatoria

DISTRIBUCIÓN DE CRÉDITOS		
	Presenciales	**OnLine**
Teóricos	1.5	
Prácticos		1.5

RESULTADOS DEL APRENDIZAJE

El alumno aprenderá detalles sobre la arquitectura de los sistemas computacionales que son objetivos repetidos y comunes en los despliegues de malware. Así mismo, aprenderá cómo funciona el malware más básico. Y qué mecanismos de ocultación suele usarse.

CONTENIDOS

1. Introducción : arquitectura de Computadores.
2. Programación a bajo nivel.
3. Análisis estático y dinámico en Windows. Vulnerabilidades PE/MZ
4. Ejemplo de un ataque por malware.
5. Análisis de las técnicas que emplean para ocultarse.

OBSERVACIONES

COMPETENCIAS

Competencias básicas y generales

1. Poseer y comprender conocimientos.
2. Aplicación de conocimientos.
3. Capacidad de emitir juicios.
4. Capacidad de comunicar y aptitud social.
5. Habilidad para el aprendizaje.

Competencias transversales

1. Habilidad en el uso de las TIC.
2. Capacidad para resolver problemas.

3. Capacidad para trabajar de forma autónoma.
Competencias específicas
1. Conocimiento y uso de técnicas avanzadas para la gestión y la protección de la dispositivos hardware. 2. Conocimiento y uso de técnicas avanzadas para la gestión de la información

ACTIVIDADES FORMATIVAS

METODOLOGÍAS DOCENTES

Los contenidos teóricos serán desarrollados a partir de material docente preparado por el profesorado para tal efecto y complementado con un sistema de tutorías online para resolver cualquier duda o cuestión al respecto del material docente.

En el apartado práctico se realizarán una serie de guiones prácticos preparados por el profesorado, que permitirán asimilar adecuadamente los contenidos teóricos y poner en una situación real de aplicación al estudiante.

SISTEMAS DE EVALUACIÓN DE COMPETENCIAS

4. Realización de actividades individuales. Cada alumno deberá ser capaz de plantear y resolver situaciones o escenarios concretos en diversos apartados del curso. Las actividades se realizarán de forma individualizada, con el apoyo del material del curso.
5. Realización de algún caso práctico propuesto que se llevará a cabo con los recursos recomendados por el profesorado.
6. Participación en el aula virtual de forma activa en los diversos foros de comunicación.

BIBLIOGRAFÍA

Malware Data Science: Attack Detection and Attribution (Inglés)

Practical Binary Analysis: Build Your Own Linux Tools for Binary Instrumentation, Analysis, and Disassembly (Inglés)

DENOMINACIÓN DEL MÓDULO					
Análisis de riesgos en la protección de datos y privacidad.					
DENOMINACIÓN EN INGLÉS					
Risk analysis in data protection and privacy.					
CRÉDITOS ECTS:	3	**CUATRIMESTRE**	1	**CARÁCTER** (Obligatoria/ Optativa)	Obligatorio
DISTRIBUCIÓN DE CRÉDITOS					
	Presenciales		**OnLine**		
Teóricos			1.5		
Prácticos			1.5		

RESULTADOS DEL APRENDIZAJE

El estudiante tendrá un conocimiento profundo en los análisis de riesgos, las evaluaciones de impacto y la importancia de la figura del Delegado de Protección de Datos ante estos eventos. Mantener la seguridad y evitar que los tratamientos de datos infrinjan lo dispuesto en el Reglamento General de Protección de Datos, son tareas de los responsables y/o encargados de tratamientos, que deben evaluar los riesgos inherentes a los tratamientos y aplicar medidas para mitigarlos. Garantizando un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deben protegerse.

Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

El estudiante será capaz de analizar el origen, la naturaleza, la particularidad y la gravedad del riesgo, para determinar el alcance, planificación y preparación de una evaluación de impacto, para el cumplimiento del Reglamento General de Protección de Datos, en los casos en que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas.

El estudiante conocerá la nueva figura del Delegado de Protección de Datos su función primordial, su papel e intervención en los análisis de riesgos, las evaluaciones de impacto y las brechas de seguridad, supervisando el cumplimiento y asesorando a la organización o empresa en la protección de datos.

CONTENIDOS

Tema 1. El Delegado de Protección de Datos. La figura del DPO como asesor del riesgo en protección de datos. El DPO en la rendición de cuentas. Posición. Recursos. Competencias y habilidades profesionales. Interlocutor con las Autoridades de Control.

Tema 2.Gestión de riesgos en privacidad. Estándares internacionales.

Tema 3. Análisis de riesgos y Evaluaciones de Impacto en protección de datos. Determinación del alcance, planificación y preparación de una EIPD.

Tema 4. Evaluación de impacto. Identificación, análisis, evaluación, tratamiento de riesgos y como evitarlos.

OBSERVACIONES

COMPETENCIAS

Competencias básicas y generales

1. Poseer y comprender conocimientos.
2. Aplicación de conocimientos.
3. Capacidad de emitir juicios.
4. Capacidad de comunicar y aptitud social.
5. Habilidad para el aprendizaje.

Competencias transversales

1. Conocimientos básicos de la profesión.
2. Compromiso ético.
3. Capacidad de crítica y autocrítica.

Competencias específicas

1. Conocimiento marco legal en el tratamiento de datos.
2. Conocimiento del marco de gestión de datos en una organización.
3. Ser capaz de analizar riesgos y brechas de seguridad en el tratamiento de la información.
4. Conocimiento de la figura, papel y función del Delegado de Protección de Datos de una empresa o institución.

ACTIVIDADES FORMATIVAS

METODOLOGÍAS DOCENTES

Clases magistrales. Supuestos prácticos y Trabajo en Grupo.
Respecto al Trabajo en Grupo se procederá a la elaboración de resoluciones de los supuestos prácticos que se planteen, siendo posteriormente expuestos en debate.

SISTEMAS DE EVALUACIÓN DE COMPETENCIAS

4. Casos prácticos y debate sobre los mismos.
5. Participación en el aula virtual y en los foros para cada caso práctico.
6. Trabajo individual que consistirá en la resolución de un caso práctico que será facilitado por el profesor de las materias objeto de la asignatura.

BIBLIOGRAFÍA

Gestión Proactiva de la PROTECCIÓN DE DATOS: Cómo implantar Privacidad por Diseño y Evaluación de Impacto en la Privacidad en la Empresa. ISBN: 978-1549567001

DENOMINACIÓN DEL MÓDULO					
Seguridad avanzada en redes					
DENOMINACIÓN EN INGLÉS					
Advanced Network Security.					
CRÉDITOS ECTS:	3	**CUATRIMESTRE**	2	**CARÁCTER** (Obligatoria/ Optativa)	Obligatorio

DISTRIBUCIÓN DE CRÉDITOS		
	Presenciales	**OnLine**
Teóricos	1.5	
Prácticos		1.5

RESULTADOS DEL APRENDIZAJE

El estudiante conocerá los elementos básicos para la seguridad perimetral, en concreto routers, proxies y sistemas de detección de intrusos en red; conocerá los distintos protocolos de rutado para redes WAN/LAN, políticas de gestión de calidad de la red (QoS) y la creación de túneles VPN.

CONTENIDOS

1. Seguridad perimetral: Firewall, proxy, sistemas de detección de intrusos en red (NIDS).
2. Servicios de redes seguras: calidad de servicio (QoS), redes LAN virtuales (VLAN), Simple Network Management Protocol (SNMP), redes privadas virtuales (VPN).
3. Distribuciones GNU/Linux para enrutamiento avanzado: Vyatta, m0n0wall, pfSense.

OBSERVACIONES

COMPETENCIAS

Competencias básicas y generales

1. Poseer y comprender conocimientos.
2. Aplicación de conocimientos.
3. Capacidad de emitir juicios.
4. Capacidad de comunicar y aptitud social.
5. Habilidad para el aprendizaje.

Competencias transversales

1. Conocimientos básicos de la profesión.
2. Capacidad para resolver problemas.
3. Capacidad para trabajar de forma autónoma.

Competencias específicas

1. Conocimiento y uso de técnicas avanzadas para la gestión y la protección de redes de comunicaciones.
2. Conocimiento y uso de técnicas de comunicación en grupos.

ACTIVIDADES FORMATIVAS

METODOLOGÍAS DOCENTES

Los contenidos teóricos serán desarrollados a partir de material docente preparado por el profesorado para tal efecto y complementado con un sistema de tutorías online para resolver cualquier duda o cuestión al respecto del material docente.

En el apartado práctico se realizarán una serie de guiones prácticos preparados por el profesorado, que permitirán asimilar adecuadamente los contenidos teóricos y poner en una situación real de aplicación al estudiante.

SISTEMAS DE EVALUACIÓN DE COMPETENCIAS

1. Realización de actividades individuales. Cada alumno deberá ser capaz de plantear y resolver situaciones o escenarios concretos en diversos apartados del curso. Las actividades se realizarán de forma individualizada, con el apoyo del material del curso.
2. Realización de algún caso práctico propuesto que se llevará a cabo con los recursos recomendados por el profesorado.
3. Participación en el aula virtual de forma activa en los diversos foros de comunicación.

BIBLIOGRAFÍA

José Manuel Huidobro Moya, David Roldán Martínez. Seguridad en redes y sistemas informáticos. Thomson Paraninfo S.A.. 2005.

Andrew S. Tanenbaum. Redes de computadores. Prentice-Hall, Pearson, Addison Wesley. 1997.

Mohan Krishnamurthi. Seguridad en Linux. Anaya Multimedia 2008.

Scott Mann, Ellen L. Mitchel, Mitchell Krell. Linux System Security. Prentice Hall International. 2004.

Julio Gómez López, Eugenio Villar Fernández, Alfredo Alcayde García. Seguridad en sistemas operativos Windows y Linux (2ª edición). Editorial Ra-Ma. 2011.

DENOMINACIÓN DEL MÓDULO					
Seguridad en entornos IoT					
DENOMINACIÓN EN INGLÉS					
Security in IoT environments					
CRÉDITOS ECTS:	2	**CUATRIMESTRE**	2	**CARÁCTER** (Obligatoria/ Optativa)	Obligatorio

DISTRIBUCIÓN DE CRÉDITOS		
	Presenciales	**OnLine**
Teóricos	1	
Prácticos		1

RESULTADOS DEL APRENDIZAJE

Dada la especial relevancia que los dispositivos electrónicos comienzan a tomar en lo relativo al envío de información que permite hacer un seguimiento en tiempo real de aquellos sistemas de los cuales forman parte y que permiten controlar y gestionar de modo remoto a través de lo que se conoce como internet de las cosas (IoT), el estudiante será capaz de garantizar la protección del funcionamiento de tales dispositivos y la información que almacenan y/o envían, teniendo en cuenta los limitados recursos con lo que estos cuentan para realizar dichas labores de seguridad.

CONTENIDOS

1. Encriptación y autenticación interna de los datos.
2. Encriptación, intercambio y autenticación de los datos transmitidos/recibidos.
3. Distribución de claves en sistemas con multitud de nodos.

OBSERVACIONES

COMPETENCIAS

Competencias básicas y generales

1. Poseer y comprender conocimientos.
2. Aplicación de conocimientos.
3. Capacidad de emitir juicios.
4. Capacidad de comunicar y aptitud social.

5. Habilidad para el aprendizaje.

Competencias transversales

1. Habilidad en el uso de las TIC.
2. Capacidad para resolver problemas.
3. Capacidad para trabajar de forma autónoma.

Competencias específicas

1. Conocimiento y uso de técnicas avanzadas para la gestión y la protección de la dispositivos hardware.
2. Conocimiento y uso de técnicas avanzadas para la programación y control de dispositivos hardware.
3. Conocimiento y uso de técnicas de optimización en problemas de ingeniería.
4. Conocimiento y uso de técnicas de comunicación en grupos.

ACTIVIDADES FORMATIVAS

METODOLOGÍAS DOCENTES

Los contenidos teóricos serán desarrollados a partir de material docente preparado por el profesorado para tal efecto y complementado con un sistema de tutorías online para resolver cualquier duda o cuestión al respecto del material docente.

En el apartado práctico se realizarán una serie de guiones prácticos preparados por el profesorado, que permitirán asimilar adecuadamente los contenidos teóricos y poner en una situación real de aplicación al estudiante.

SISTEMAS DE EVALUACIÓN DE COMPETENCIAS

1. Realización de actividades individuales. Cada alumno deberá ser capaz de plantear y resolver situaciones o escenarios concretos en diversos apartados del curso. Las actividades se realizarán de forma individualizada, con el apoyo del material del curso.
2. Realización de algún caso práctico propuesto que se llevará a cabo con los recursos recomendados por el profesorado.
3. Participación en el aula virtual de forma activa en los diversos foros de comunicación

BIBLIOGRAFÍA

Christof Paar, Jan Pelzl. Understanding Cryptography: A Textbook for Students and Practitioners. Springer. 2008.

Dimitrios Serpanos, Wayne Wolf. Internet-of-Things (IoT) Systems. Springer 2018.

N. Jeyanthi, Ajith Abraham, Hamid Mcheick. Ubiquitous Computing and Computing Security of IoS. 2019.

DENOMINACIÓN DEL MÓDULO					
Introducción a la BIOS y a la RAM					
DENOMINACIÓN EN INGLÉS					
BIOS and RAM memory system foundations.					
CRÉDITOS ECTS:	2	**CUATRIMESTRE**	2	**CARÁCTER** (Obligatoria/ Optativa)	Obligatoria

DISTRIBUCIÓN DE CRÉDITOS		
	Presenciales	**OnLine**
Teóricos	1	
Prácticos		1

RESULTADOS DEL APRENDIZAJE

El alumno aprenderá a manejar los términos de backdoor (pueta trasera) y de troyano. Así como la relación de estos con los términos rootkit y bootkit. Cuando se hable de rootkits ya deberán estar familiarizados pues se debieron formar en técnicas básicas de malware. Además, en este módulo se mostrará cómo se emplean técnicas avanzadas para incluir malware en el firmware (bios, uefi..) del sistema computacional.

CONTENIDOS

1. Puertas traseras.
2. Uso de la red para el establecimiento de puertas traseras.
3. Rootkits: TDL3 y Festi Rootkit. Infección a través de Rootkits.
4. Bootkits. Arranque de un sistema operativo. Seguridad en el arranque
5.Técnicas de defensa y protección.

OBSERVACIONES

COMPETENCIAS

Competencias básicas y generales

1.Poseer y comprender conocimientos.
2.Aplicación de conocimientos.
3.Capacidad de emitir juicios.
4.Capacidad de comunicar y aptitud social.
5.Habilidad para el aprendizaje.

Competencias transversales

4. Habilidad en el uso de las TIC.
5. Capacidad para resolver problemas.
6. Capacidad para trabajar de forma autónoma.

Competencias específicas

Conocimiento y uso de técnicas avanzadas para la gestión y la protección de dispositivos hardware.
Conocimiento y uso de técnicas avanzadas para la protección de la información.

ACTIVIDADES FORMATIVAS

METODOLOGÍAS DOCENTES

Los contenidos teóricos serán desarrollados a partir de material docente preparado por el profesorado para tal efecto y complementado con un sistema de tutorías online para resolver cualquier duda o cuestión al respecto del material docente.

En el apartado práctico se realizarán una serie de guiones prácticos preparados por el profesorado, que permitirán asimilar adecuadamente los contenidos teóricos y poner en una situación real de aplicación al estudiante.

SISTEMAS DE EVALUACIÓN DE COMPETENCIAS

1. Realización de actividades individuales. Cada alumno deberá ser capaz de plantear y resolver situaciones o escenarios concretos en diversos apartados del curso. Las actividades se realizarán de forma individualizada, con el apoyo del material del curso.
2. Realización de algún caso práctico propuesto que se llevará a cabo con los recursos recomendados por el profesorado.
3. Participación en el aula virtual de forma activa en los diversos foros de comunicación

BIBLIOGRAFÍA

Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats.

DENOMINACIÓN DEL MÓDULO					
Análisis de cifradores y procesos de protección de la información					
DENOMINACIÓN EN INGLÉS					
Encryption analysis and information protection processes					
CRÉDITOS ECTS:	2	**CUATRIMESTRE**	2	**CARÁCTER** (Obligatoria/ Optativa)	Obligatorio

DISTRIBUCIÓN DE CRÉDITOS		
	Presenciales	**OnLine**
Teóricos	1	
Prácticos		1

RESULTADOS DEL APRENDIZAJE

Con este módulo se pretende que el estudiante sea capaz de analizar correcta implementación de un cifrador que utilice alguno de los estándares criptográficos recomendados. Será capaz de llevar a cabo ataques que exploten un error de implementación en dichos cifradores. Del mismo modo será capaz de comprender y evaluar determinados riesgos provocados por los factores físicos que determinan la implementación, pudiendo recomendar o desaconsejar su posible uso, dependiendo del caso práctico.

CONTENIDOS

1. Fallos de implementación de una infraestructura de clave pública RSA.
2. Fallos de implementación de una infraestructura de clave pública basada en el problema del logaritmo en distintos grupos.
3. Generación y uso de números aleatorios en cifradores.
4. Ataques a sistemas de distribución de claves en grupos.

OBSERVACIONES

Nociones básicas de conceptos matemáticos sobre Teoría de Números y Cuerpos Finitos pueden ayudar a una mejor asimilación de los contenidos, aunque no de un modo determinante.
Se hará uso de software gratuito.

COMPETENCIAS

Competencias básicas y generales

1. Poseer y comprender conocimientos.
2. Aplicación de conocimientos.
3. Capacidad de emitir juicios.

4. Capacidad de comunicar y aptitud social.
5. Habilidad para el aprendizaje

Competencias transversales

1. Conocimientos básicos de la profesión.
2. Capacidad para resolver problemas.
3. Capacidad de crítica y autocrítica.

Competencias específicas

1. Conocimiento y uso de técnicas avanzadas para la gestión y la protección de la información.
2. Conocimiento y uso de técnicas avanzadas para la autenticación de la información.
3. Conocimiento y uso de técnicas avanzadas para el control de acceso a servicios de información.

ACTIVIDADES FORMATIVAS

METODOLOGÍAS DOCENTES

Los contenidos teóricos serán desarrollados a partir de material docente preparado por el profesorado para tal efecto y complementado con un sistema de tutorías online para resolver cualquier duda o cuestión al respecto del material docente.

En el apartado práctico se realizarán una serie de guiones prácticos preparados por el profesorado, que permitirán asimilar adecuadamente los contenidos teóricos y poner en una situación real de aplicación al estudiante.

SISTEMAS DE EVALUACIÓN DE COMPETENCIAS

1. Realización de actividades individuales. Cada alumno deberá ser capaz de plantear y resolver situaciones o escenarios concretos en diversos apartados del curso. Las actividades se realizarán de forma individualizada, con el apoyo del material del curso.
2. Realización de algún caso práctico propuesto que se llevará a cabo con los recursos recomendados por el profesorado.
3. Participación en el aula virtual de forma activa en los diversos foros de comunicación.

BIBLIOGRAFÍA

Bruce Schneier. Applied Cryptography. Wiley & Sons. 1996.

Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone. Handbook of Applied Criptography. CRC Press. 1997.

Wade Trappe, Lawernce C. Washington. Introduction to criptography with coding theory. Prentice-Hall, Inc.. 2004.

Christof Paar, Jan Pelzl. Understanding Cryptography: A Textbook for Students and Practitioners. Springer. 2008.

Amparo Fuster Sabater, Luis Hernández Encinas, Fausto Montoya Vitini, Jaime Muñoz Masque. Criptografía, protección de datos y aplicaciones. Una guía para estudiantes y profesionales. Ra-Ma. 2012.

DENOMINACIÓN DEL MÓDULO					
Análisis avanzado de malware					
DENOMINACIÓN EN INGLÉS					
Advanced malware analysis					
CRÉDITOS ECTS:	1	**CUATRIMESTRE**	2	**CARÁCTER** (Obligatoria/ Optativa)	Obligatoria

DISTRIBUCIÓN DE CRÉDITOS		
	Presenciales	**OnLine**
Teóricos	0.5	
Prácticos		0.5

RESULTADOS DEL APRENDIZAJE

El alumno aprenderá las técnicas de análisis de malware (tanto dinámicas como estáticas) que es frecuente usar en entornos Linux y entornos Windows ante la presencia de una infección o ataque.

CONTENIDOS

1. Shellcodes y vulnerabilidades
2. Contramedidas (NX, ASLR,…)
3. Evasión de contramedidas.
4. Técnicas de reversing y exploiting.

OBSERVACIONES

COMPETENCIAS

Competencias básicas y generales

1. Poseer y comprender conocimientos.
2. Aplicación de conocimientos.
3. Capacidad de emitir juicios.
4. Capacidad de comunicar y aptitud social.
5. Habilidad para el aprendizaje.

Competencias transversales

1. Habilidad en el uso de las TIC.
2. Capacidad para resolver problemas.

3. Capacidad para trabajar de forma autónoma.
Competencias específicas
5. Conocimiento y uso de técnicas avanzadas para la gestión y la protección de sistemas.

ACTIVIDADES FORMATIVAS
METODOLOGÍAS DOCENTES
Los contenidos teóricos serán desarrollados a partir de material docente preparado por el profesorado para tal efecto y complementado con un sistema de tutorías online para resolver cualquier duda o cuestión al respecto del material docente. En el apartado práctico se realizarán una serie de guiones prácticos preparados por el profesorado, que permitirán asimilar adecuadamente los contenidos teóricos y poner en una situación real de aplicación al estudiante.

SISTEMAS DE EVALUACIÓN DE COMPETENCIAS
1. Realización de actividades individuales. Cada alumno deberá ser capaz de plantear y resolver situaciones o escenarios concretos en diversos apartados del curso. Las actividades se realizarán de forma individualizada, con el apoyo del material del curso. 2. Realización de algún caso práctico propuesto que se llevará a cabo con los recursos recomendados por el profesorado. 3. Participación en el aula virtual de forma activa en los diversos foros de comunicación

BIBLIOGRAFÍA
Malware Data Science: Attack Detection and Attribution (Inglés) Practical Binary Analysis: Build Your Own Linux Tools for Binary Instrumentation, Analysis, and Disassembly (Inglés)

DENOMINACIÓN DEL MÓDULO					
Ofensiva y defensa en aplicaciones web.					
DENOMINACIÓN EN INGLÉS					
Web applications: defense and offense techniques.					
CRÉDITOS ECTS:	3	**CUATRIMESTRE**	2	**CARÁCTER** (Obligatoria/ Optativa)	Obligatoria

DISTRIBUCIÓN DE CRÉDITOS		
	Presenciales	**OnLine**
Teóricos	1.5	
Prácticos		1.5

RESULTADOS DEL APRENDIZAJE

Las aplicaciones web son muy comunes en el ecosistema digital e hiperconectado. Los perfiles profesionales que se dedican a construir estos sistemas están muy demandados y extendidos, pero apenas se forma en seguridad. Los alumnos aprenderán a contener los ataques elementales a las aplicaciones web que diseñen y construyan. Estarán capacitados para conocer dónde su aplicación web puede presentar vulnerabilidades y ser capaces de hacer tests de penetración elementales para comprobar la consistencia, tanto de la aplicación web como de las protecciones que se han empleado.

CONTENIDOS

01_INTRODUCCIÓN
02_METODOLOGÍA
03_LABORATORIO DE PRUEBAS
04_SQL INYECTION
05_CROSS-SITE SCRIPTING
06_ATAQUES_DE LOGIN
07_ATAQUES CON WEBSHELL
08_ATAQUES FILE UPLOAD
09_LOCAL FILE INCLUSION
10_BRUTE FORCE
11_PARAMETER TAMPERING
12_CONTROL INSEGURO DE ROLES
13_DETECCIÓN DE ATAQUES
14_MONITORIZACIÓN DE SITIOS WEB
15_INTRODUCCIÓN A LOS WAF

OBSERVACIONES

COMPETENCIAS

Competencias básicas y generales

6. Poseer y comprender conocimientos.
7. Aplicación de conocimientos.
8. Capacidad de emitir juicios.
9. Capacidad de comunicar y aptitud social.
10. Habilidad para el aprendizaje.

Competencias transversales

4. Habilidad en el uso de las TIC.
5. Capacidad para resolver problemas.
6. Capacidad para trabajar de forma autónoma.

Competencias específicas

6. Conocimiento y uso de técnicas avanzadas para la gestión y la protección de la dispositivos hardware.
7. Conocimiento y uso de técnicas avanzadas para la programación y control de dispositivos hardware.
8. Conocimiento y uso de técnicas de optimización en problemas de ingeniería.
9. Conocimiento y uso de técnicas de comunicación en grupos.

ACTIVIDADES FORMATIVAS

METODOLOGÍAS DOCENTES

Los contenidos teóricos serán desarrollados a partir de material docente preparado por el profesorado para tal efecto y complementado con un sistema de tutorías online para resolver cualquier duda o cuestión al respecto del material docente.

En el apartado práctico se realizarán una serie de guiones prácticos preparados por el profesorado, que permitirán asimilar adecuadamente los contenidos teóricos y poner en una situación real de aplicación al estudiante.

SISTEMAS DE EVALUACIÓN DE COMPETENCIAS

4. Realización de actividades individuales. Cada alumno deberá ser capaz de plantear y resolver situaciones o escenarios concretos en diversos apartados del curso. Las actividades se realizarán de forma individualizada, con el apoyo del material del curso.
5. Realización de algún caso práctico propuesto que se llevará a cabo con los recursos recomendados por el profesorado.
6. Participación en el aula virtual de forma activa en los diversos foros de comunicación

BIBLIOGRAFÍA
Web Application Security, A Beginner's Guide. McGraw-Hill Education; ISBN-13: 978 0071776165 The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. Publisher: Wiley; 2 editionISBN-13: 978-1118026472

DENOMINACIÓN DEL MÓDULO					
Blockchain					
DENOMINACIÓN EN INGLÉS					
Blockchain					
CRÉDITOS ECTS:	1	**CUATRIMESTRE**	2	**CARÁCTER** (Obligatoria/ Optativa)	Obligatoria

DISTRIBUCIÓN DE CRÉDITOS		
	Presenciales	**OnLine**
Teóricos	0.5	
Prácticos		0.5

RESULTADOS DEL APRENDIZAJE

El alumno conocerá el sistema de “federación” de entidades pares para el mantenimiento de una red de confianza que permita compartir y mantener históricos de transferencias.
Aprenderá las bases de bitcoin y de sus fortalezas y debilidades.

CONTENIDOS

1. Qué es block-chain.
2. El pilar financiero. Conceptos fundamentales de bitcoin como ejemplo de blockchain
3. Libro de registro distribuido: tecnología.
4. Los bloques, su creación y la seguridad de blockchain.
5. Redes peer to peer. Hashing. etc
6. Aplicaciones a la cadena de valor
7. Hyperledger

OBSERVACIONES

COMPETENCIAS

Competencias básicas y generales

11. Poseer y comprender conocimientos.
12. Aplicación de conocimientos.
13. Capacidad de emitir juicios.
14. Capacidad de comunicar y aptitud social.
15. Habilidad para el aprendizaje.

Competencias transversales

7. Habilidad en el uso de las TIC.
8. Capacidad para resolver problemas.
9. Capacidad para trabajar de forma autónoma.

Competencias específicas

10. Conocimiento y uso de técnicas de optimización en problemas de ingeniería.
11. Conocimiento y uso de técnicas de comunicación en grupos.
12. Conocimiento y uso de técnicas de protección de la información.

ACTIVIDADES FORMATIVAS

METODOLOGÍAS DOCENTES

Los contenidos teóricos serán desarrollados a partir de material docente preparado por el profesorado para tal efecto y complementado con un sistema de tutorías online para resolver cualquier duda o cuestión al respecto del material docente.

En el apartado práctico se realizarán una serie de guiones prácticos preparados por el profesorado, que permitirán asimilar adecuadamente los contenidos teóricos y poner en una situación real de aplicación al estudiante.

SISTEMAS DE EVALUACIÓN DE COMPETENCIAS

7. Realización de actividades individuales. Cada alumno deberá ser capaz de plantear y resolver situaciones o escenarios concretos en diversos apartados del curso. Las actividades se realizarán de forma individualizada, con el apoyo del material del curso.
8. Realización de algún caso práctico propuesto que se llevará a cabo con los recursos recomendados por el profesorado.
9. Participación en el aula virtual de forma activa en los diversos foros de comunicación

BIBLIOGRAFÍA

Todo sobre Tecnología Blockchain: La Guía Definitiva para Principiantes Sobre Monederos Blockchain.

10.- Prácticas Externas

Este apartado deberá ser cumplimentado en el caso de contemplar la realización de prácticas externas

Empresas	*Nombre de las empresas*	*Convenio vigente (si/no)*
	TECNOBIT (Grupo OESÍA)	No
	CAJAMAR	Si
	JCARRIÓN	Si
	HISPATEC	SI
	MEDGAZ (Pendiente)	SI
Días de la semana y horario	Pendiente	
Número de días de prácticas de cada alumno	Pendiente	
Número de alumnos simultáneos	Pendiente	
Carga docente de las prácticas en horas presenciales por alumno	12 créditos (150 horas)	

PROYECTO FORMATIVO

Competencias que deben adquirir las y los estudiantes en estas prácticas
Conocimientos básicos de la profesión. Habilidad en el uso de las TIC. Capacidad para resolver problemas. Comunicación oral y escrita en la propia lengua. Capacidad de crítica y autocrítica. Trabajo en equipo. Compromiso ético. Capacidad para aprender a trabajar de forma autónoma.
Resultados esperados del aprendizaje práctico
Que el alumno sea capaz de desenvolverse y aplicar las competencias adquiridas, en cada uno de los módulos, en un entorno y situación real.
Metodología de la evaluación prevista
¿Cómo tiene previsto la Universidad que las personas tutoras de prácticas evalúen al alumnado? A través de la plataforma ícaro, mediante la emisión de un informe por parte del tutor de la empresa e informe o valoración emitida por el tutor académico a partir de la memoria redactada por el alumno al finalizar el periodo de prácticas.

¿Cómo tiene previsto la Universidad que el alumnado evalúe a las personas tutoras de prácticas? A través de la plataforma ícaro.
¿Cómo tiene previsto la Universidad evaluar la satisfacción del alumnado respecto a las prácticas? A través de la plataforma ícaro.

11.- Recursos Necesarios

Localidad		**FERNANDO RECHE LORITE**
Fecha		
Firma		**Fdo. Decano / Director de Centro responsable**