CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

Clase de estudio o titulación	**Máster**
Denominación	**MÁSTER EN CIBERSEGURIDAD. RED TEAM - BLUE TEAM**

Nº EDICIÓN: 1ª

Fecha de inicio edición (mes y año):	oct-20
Fecha de finalización (mes y año):	dic-21

Fecha de aprobación en Junta de Centro (Escuela Politécnica Superior): 28/01/2020

Nota Importante:

Para la cumplimentación de este formulario, téngase en cuenta la «Normativa sobre enseñanzas propias y formación continua de la Universidad Autónoma de Madrid», aprobada por el Consejo de Gobierno de la UAM en fecha 5 de febrero de 2010, en adelante, «Normativa UAM» https://www.uam.es/ss/Satellite/es/1242648684748/contenidoFinal/Legislacion_y_Normativa.htm

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

1. DESCRIPCIÓN DEL TÍTULO

1.1. Denominación:

MÁSTER EN CIBERSEGURIDAD. READ TEAM - BLUE TEAM

1.2. Universidad/es participantes:

UNIVERSIDAD AUTÓNOMA DE MADRID

Copie y numere líneas tantas veces como necesite

1.3. Centro/s, Departamento/s o Instituto/s responsable/s del Programa:

INSTITUTO DE CIENCIAS FORENSES Y DE LA SEGURIDAD DE LA UAM

Copie y numere líneas tantas veces como necesite

1.4. Dirección académica.

Dirección: D. ÁLVARO ORTIGOSA

Categoría académica: PROFESOR CONTRATADO DOCTOR

Universidad o Centro de adscripción: ESCUELA POLITÉCNICA SUPERIOR

Correo electrónico: alvaro.ortigosa@uam.es

Número de teléfono: 919472271

Codirección: D. ÓSCAR MAQUEDA HORTELLS (EMPRESA DISRUPTIVE CONSULTING)

Categoría académica:

Universidad o Centro de adscripción:

Correo electrónico: oscar.maqueda@hotmail.com

Número de teléfono: 919474268

Codirección: MARIO GUERRA SOTO (MINISTERIO DE DEFENSA)

Categoría académica:

Universidad o Centro de adscripción:

Correo electrónico: marioguerrasoto@gmail.com

Número de teléfono: 919474268

Codirección: RAMÓN FUENTES REQUENA (GUARDIA CIVIL)

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

Categoría académica:

Universidad o Centro de adscripción:

Correo electrónico: ramonfure@gmail.com

Número de teléfono: 919474268

Subdirección: JORGE LÓPEZ DE VERGARA

Categoría académica: PROFESOR TITULAR UAM

Universidad o Centro de adscripción: EPS

Correo electrónico: jorge.lopez_vergara@uam.es

Número de teléfono: 919472246

Copie tantas veces como necesite la plantilla de Subdirección

Secretaría Académica:

Categoría académica:

Universidad o Centro de adscripción:

Correo electrónico:

Número de teléfono:

Comisión responsable, en su caso (indique los nombres, la categoría y el Centro de adscripción):

1. **ÁLVARO ORTIGOSA JUAREZ (PROFESOR CONTRATADO DOCTOR UAM (EPS) Y DIRECTOR ICFS)**
2. **ÓSCAR MAQUEDA HORTELLS (CODIRECTOR MÁSTER. EMPRESA DISRUPTIVE CONSULTING)**
3. **MARIO GUERRA SOTO (CODIRECTOR DEL MÁSTER. MCCD)**
4. **RAMÓN FUENTES (CODIRECTOR DEL MÁSTER. GUARDIA CIVIL)**
5. **JORGE LÓPEZ DE VERGARA (SUBDIRECTOR DEL MÁSTER. PROFESOR TITULAR UAM (EPS))**

Copie y numere líneas tantas veces como necesite

Persona de contacto (de entre las anteriores): ÁLVARO ORTIGOSA JUAREZ

1.5. Secretaría administrativa

Nombre: ARACELI BAILÓN GARCÍA

Procedencia: ICFS UAM

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

Experiencia en puestos de gestión administrativa: **SÍ** ☒ **NO** ☐ **Correo electrónico: araceli.bailon@inv.uam.es** **Número de teléfono:** 919474268

1.6. Tipo de enseñanza: semipresencial **Clic aquí**

1.7. Rama de conocimiento: Ingeniería y Arquitectura

1.8. Número de plazas ofertadas: 30

1.9. Número de becas ofrecidas: 3

1.10. Instituciones o empresas colaboradoras (en su caso):

Idoneidad de la colaboración propuesta [máx. 2000 caracteres o 30 líneas]:
Copie tantas veces como necesite la plantilla de Institución o Empresa colaboradora

1.11. Lugar (centro) de Impartición: EPS UAM

1.12. Tiempo de impartición:

Fecha de inicio: 02/10/2020 **Unidades temporales (periodos lectivos): CUATRIMESTRES** Clic aquí **Número de Unidades temporales (periodos lectivos): 4** Clic aquí
Primer CUATRIMESTRE: **Fechas: De oct-20 a dic-20** **Nº de semanas: 12** **Nº horas de docencia por semana: 4/8 DEPENDIENDO, PORQUE ES SEMIPRESENCIAL Y NO HAY CLASE PRESENCIAL TODAS LAS SEMANAS** **Horario: VIERNES DE 15.30 A 20.00 (30 MINUTOS DE DESCANSO) Y SÁBADOS DE 9.30 A 14.00 (30 MINUTOS DE DESCANSO)**
Segundo CUATRIMESTRE: **Fechas: De ene-21 a abr-21**

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

Nº de semanas: 16 **Nº horas de docencia por semana: 4/8 DEPENDIENDO, PORQUE ES SEMIPRESENCIAL Y NO HAY CLASE PRESENCIAL TODAS LAS SEMANAS** **Horario: VIERNES DE 15.30 A 20.00 (30 MINUTOS DE DESCANSO) Y SÁBADOS DE 9.30 A 14.00 (30 MINUTOS DE DESCANSO)**
Tercer CUATRIMESTRE : **Fechas: De may-21 a ago-21** **Nº de semanas: 10** **Nº horas de docencia por semana: 4/8 DEPENDIENDO, PORQUE ES SEMIPRESENCIAL Y NO HAY CLASE PRESENCIAL TODAS LAS SEMANAS** **Horario: VIERNES DE 15.30 A 20.00 (30 MINUTOS DE DESCANSO) Y SÁBADOS DE 9.30 A 14.00 (30 MINUTOS DE DESCANSO)**
Cuarto CUATRIMESTRE: **Fechas: De sept-21 a Clic aquí. DICIEMBRE 2021** **Nº de semanas: 16** **Nº horas de docencia por semana: 4/8 DEPENDIENDO, PORQUE ES SEMIPRESENCIAL Y NO HAY CLASE PRESENCIAL TODAS LAS SEMANAS** **Horario: VIERNES DE 15.30 A 20.00 (30 MINUTOS DE DESCANSO) Y SÁBADOS DE 9.30 A 14.00 (30 MINUTOS DE DESCANSO)**

1.13. Precios y plazos de inscripción y matrícula

Nº de créditos ECTS	Precio por crédito	Precio total
70 ECTS	128,57 €	9000 €

Plazo de inscripción	**Desde: 1 de abril**	**Hasta: 1 día antes del comienzo de la clases**
Plazo de matrícula	**Desde: 1 de abril**	**Hasta: 1 mes después del comienzo de las clases**

Auto registro de Inscripción	**Sí X**	**No ☐**
Auto registro de matrícula	**Sí X**	**No ☐**

1.14. Requisitos/Reglas de matrícula: Si el estudiante tiene que matricular obligatoriamente alguna asignatura y tiene que elegir entre alguna otra, indicar el patrón que se debe cumplir. (ejemplo: de las diez asignaturas de los que consta el estudio, el estudiante tiene que matricularse de 8 asignaturas en total. hay 6 asignaturas obligatorias de las cuales sí o sí se tiene que matricular y elegir dos de las otras cuatro que son obligatorias).

Todas son obligatorias

2. JUSTIFICACIÓN DEL TÍTULO PROPUESTO

2.1 Interés académico y/o profesional [máx. 3000 caracteres o 40 líneas]

Sin duda el mundo se mueve a través de las ondas radioeléctricas, el conocimiento de las tecnologías involucradas, los distintos estándares desde Wifi a/b/g/n/ac, Zigbee, GSM, LTE, Satélite, … y muchos más, es fundamental para cualquier profesional de la ciberseguridad, saber como los atacantes pueden sacar partido de las vulnerabilidades es critico y poder prevenirlo es muy importante. Las tecnologías de redes inalámbricas cada vez tienen más presencia en nuestros vehículos, hogares, etc. y es de ahí donde los alumnos han de aprender tanto la vertiente defensiva como la ofensiva. El alumno tiene que ser capaz de entender los distintos métodos de ataque y defensa de las redes inalámbricas: protocolos, electrónica involucrada, ataques para interceptación, ataques DDoS/DoS, ataques por inyección de datos, … en definitiva cualquier modo mediante el cual un atacante puede obtener acceso a los recursos, manipularlos o impersonarlos.

2.2 Referentes externos nacionales e internacionales que avalan la adecuación de la propuesta (indique si existen títulos de contenido similar en Universidades u otras instituciones de prestigio nacionales o extranjeras y especifique su denominación y su enlace *web*) [máx. 2000 caracteres o 30 líneas]

En la actualidad no existe ningún programa con contenidos parecidos al que queremos ofrecer. Si hay alguno en empresas privadas, pero que se refiere únicamente a pentesting y hacking , como por ejemplo: Máster en seguridad informática y Hacking ético en CICE (https://www.cice.es/master-en-seguridad-informatica-y-hacking-etico-ec-council-msi/)

3. OBJETIVOS GENERALES DEL TÍTULO PROPUESTO

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

3.1 Objetivos [máx. 2000 caracteres o 30 líneas]

Una gestión básica de la Ciberseguridad pivota sobre los ámbitos de Protección, Detección y Respuesta, enmarcadas en un aseguramiento continuo que garantice el adecuado funcionamiento de las actividades que incluyen. De manera, que un esquema de evaluación de controles de seguridad, debería tener con una visión holística de estos tres ámbitos.

Bajo esta necesidad las operaciones Red Team se están postulando como uno de los mejores esquemas de revisión y aseguramiento por su alta capacidad para evaluar de manera holística las actividades de Protección, Detección y Respuesta; y evidenciar gaps de seguridad desconocidos (mostrar diferencias entre la seguridad supuesta y la real).

Por otra parte, el concepto Blue Team, va más allá del equipo de respuesta frente a las actividades del Red Team. Bajo este color se engloban un conjunto de actividades complejas de detección, respuesta y mitigación con ajustes finos que necesitan y deben compartir la inteligencia de ataque del Red Team. En la actualidad la Detección y Respuesta es uno de ámbitos de mayor recorrido de madurez y altamente necesario.

Es por ello que en este grado se engloben ambos enfoques Red y Blue para dar respuesta a la demanda en ciberseguridad de una visión holística tanto en pruebas (Red) como en detección y respuesta (Blue), además de la evidente Protección.

De esta manera, una clave de éxito para conseguir una mejora continua en Protección, Detección y Respuesta es disponer de un adecuado esquema Red Blue y es, en este Master, donde se proporcionan todos los elementos conceptuales y prácticos para conseguirlo.

3.2. Principales Competencias (enumere en torno a 10 competencias, distinguiendo entre competencias «generales» y «específicas»)

Competencias Generales

CG1: Comprender y aplicar tácticas, técnicas y procedimientos de ciberataque a una instalación específica.

CG2: Comprender y aplicar métodos de detección y respuesta para técnicas de ciberataque de agentes hostiles.

CG3: El alumno debe ser capaz de tratar situaciones complejas e impredecibles de forma sistemática y creativa, con j ciberdelincuencia.

CG4: Elaborar concisa, clara y razonadamente documentos de trabajo e informes en el ámbito de la Ciberseguridad.

Competencias Específicas

CE1 Ser capaz de buscar e identificar información en fuentes abiertas que le permitan explotar vulnerabilidades en e

CE2 Ser capaz de conocer y aplicar técnicas y procedimientos de ataque en todos los ámbitos de una intrusión: explo exfiltración...

CE3 Ser capaz de desplegar arquitecturas básicas SIEM (Security Information and Event Management) . El alumno será capaz de adquirir nociones y habilidades básicas de respuesta ante una investigación en entornos web,

aprovechando las características propias de todas y cada una de las fases de un pentest.

CE4 Ser capaz de modelar y desplegar alertas para la detección de potenciales incidentes de ciberseguridad.

CE5 Ser capaz de identificar y explotar potenciales vulnerabilidades de los sistemas Web de la organización

CE6 Ser capaz de identificar y explotar potenciales vulnerabilidades de arquitecturas específicas comúnes organizaci

CE7 Ser capaz de identificar y explotar potenciales vulnerabilidades de redes inalámbricas.

CE8 Ser capaz de identificar y explotar potenciales vulnerabilidades de sistemas informáticos de entornos industriale

CE9 Ser capaz de identificar y explotar potenciales vulnerabilidades mediante técnicas avanzadas o arsenal propio.

CE10 Ser capaz de detectar e identificar actividad asociada o potenciales incidentes de ciberseguridad.

CE11 Ser capaz de responder en tiempo y forma frente a potencial actividad asociada a incidentes de ciberseguridad

CE12 Ser capaz de entender y desempeñar el papel del auditor de seguridad dentro del equipo de ciberseguridad (o a

4. DIFUSIÓN, INFORMACIÓN Y CAPTACIÓN DE ESTUDIANTES

4.1. Canales específicos de difusión y captación de estudiantes. [máx. 1500 caracteres o 20 líneas]

La difusión del programa se realizará principalmente a través de los siguientes medios:

-Redes sociales (Twitter, Facebook, LinkedIn, Google+, Youtube, etc.)

- Página web oficial del ICFS.

-Canales oficiales de la UAM

- Foros de seguridad, ciberseguridad y afines.

- Jornadas oficiales fijadas en el programa de eventos de la UAM orientadas a formación y empleabilidad.

4.2. Acciones de difusión y captación previstas [máx. 1500 caracteres o 20 líneas]

- Creación y difusión de materiales publicitarios específicos del programa: carteles, dípticos, logos.
- Distribución de información del programa vía e-mail.
- Diseño de páginas específicas del programa en redes sociales.

4.3. Sistemas de información previa a la matriculación [máx. 1500 caracteres o 20 líneas]

El ICFS dispone de personal de gestión que ofrece información previa a la matriculación a través de distintos medios a los alumnos interesados. Esta labor de información se realiza a partir de los siguientes medios:

1. A través de correo electrónico.

2. A través de la página web del ICFS que contiene toda la información referente a los siguientes aspectos:

- Relación de la oferta académica del programa.
- Procedimiento y plazos de solicitud de admisión y matriculación, así como la documentación necesaria para la inscripción y solicitud de becas.
- Tasas académicas
- Normativa y procedimiento para la obtención de la homologación de títulos extranjeros.
- Información relevante para los alumnos extranjeros: alojamiento, procedimientos de renovación de permisos de estudiante y residencia, gastos medios de su estancia en España, residencias o lugares de alojamiento, etc.

3. Vía telefónica, en horario de mañana de lunes a viernes.

La solicitud de admisión de los alumnos puede realizarse a través del correo electrónico. Una vez comprobado desde la dirección del máster que la documentación presentada es adecuada, se realiza la valoración de las solicitudes que también es revisada por el Centro de Estudios de Posgrado. La comisión directiva responsable del programa es quien valora los méritos y propone la admisión en función de los criterios de admisión y requisitos generales.

5. ACCESO Y ADMISIÓN DE ESTUDIANTES

5.1. Requisitos de acceso y condiciones o pruebas especiales. [máx. 1500 caracteres o 20 líneas]

Los requisitos de acceso son aquellos que están reflejados en el artículo 28 de la Normativa de Enseñanzas Propias y Formación Continua. Para este programa, los requisitos específicos serán los siguientes:
- Ser licenciado o graduado universitario
-Alumnos que estén en último año de Grado y tengan al menos 192 créditos aprobados y estén en disposición de obtener el título.
- Aquellas personas que, aun no siendo graduados o licenciados, puedan acreditar experiencia profesional de entre 3 y 5 años en este ámbito.
- Para el resto de interesados, la admisión queda condicionada a la evaluación de la comisión del programa.

En determinados casos, se podrá solicitar una entrevista personal con el estudiante para evaluar sus competencias.

5.2. Criterios generales de selección de estudiantes. [máx. 1500 caracteres o 20 líneas]

Admisión de estudiantes:

Los alumnos del programa serán seleccionados por los directores del título atendiendo a los siguientes criterios:

1. Adecuación de la Titulación académica (30%)
2. Méritos académicos (10%)
3. Experiencia profesional relacionada con el ámbito (50%)
4. Idiomas (10%)

b) Admisión de Becarios:

Los criterios de selección de becarios son:

1. Interés institucional. Por ejemplo ser miembro de FCSE, ganador de la NCL, u otros eventos organizados del ICFS (50%)
4. Situación socio-económica (30%)
5. Expediente académico y/o experiencia profesional (20%)

La dirección del programa concederá becas por un importe mínimo correspondiente al 10% de las matrículas registradas, reservándose el derecho a dividirlas en varias becas parciales para beneficiar a un mayor número de estudiantes.

5.3. Sistemas de apoyo y orientación de los estudiantes una vez matriculados [máx. 1500 caracteres o 20 líneas]

Después del periodo de matrícula, se realiza una reunión informativa con los estudiantes para darles la bienvenida y se les presenta a los directores y coordinadores del programa. En dicho acto también se les informa de los servicios disponibles en la universidad así como su forma de disfrutarlos.

El personal coordinador del título desarrolla los mecanismos necesarios para que exista un sistema de apoyo permanente a los estudiantes durante sus estudios a través de los siguientes métodos:

- Atención y tutorías personales ante cuestiones planteadas directamente por parte de los alumnos.
- Responsables de comunicación entre los alumnos y la dirección del programa para asegurar que la comunicación e interacción con los alumnos es fluida y satisfactoria.

- Reuniones periódicas con los alumnos para informar sobre el desarrollo del curso y atender a aquellas inquietudes o cuestiones que puedan surgir.

Otras oficinas relevantes para los estudiantes una vez matriculados son:
- Oficina de Información y Atención al Estudiante.
- Oficina de Relaciones Internacionales.
- Oficina de Prácticas.

6. PLAN DE ESTUDIOS

6.1. Distribución de las actividades formativas por horas y por número de créditos.

TIPO DE ACTIVIDAD FORMATIVA	HORAS			CRÉDITOS ECTS	
	DOCENCIA PRESENCIAL	DOCENCIA NO PRESENCIAL	TRABAJO DEL ESTUDIAN		
Asignaturas Obligatorias	160 hs.		340 hs.		20
Asignaturas Optativas ofertadas en el título				0	
Asignaturas Optativas a cursar por el estudiante	0 hs.		0 hs.		0
Si el título es «semipresencial» indique nº de horas de actividad docente no presencial		925 hs			37
Prácticas externas	0 hs		0 hs.		0
Trabajo fin del título	0 hs.		325 hs.		13
Total Horas de docencia	**160 hs.**				
Total horas de trabajo autónomo del estudiante			**665 hs.**		

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

CRÉDITOS TOTALES DEL TÍTULO		**0 ECTS**	**70 ECTS**

6.2. Tabla-resumen de módulos y asignaturas.

[AÑADA O ELIMINE TÁBLAS DE MÓDULOS Y FILAS DE ASIGNATURA DENTRO DE CADA MÓDULO SEGÚN PROCEDA]

Módulos y asignaturas	Periodo	Créditos
Mód. I :		
Asignaturas obligatorias		
1 **Fundamentos Red Team y Blue Team**	**1**	3 ECTS
2 **Reconocimiento. Vectores de entrada y acceso.**	**1**	3 ECTS
3 **Extracción de artefactos forenses y caracterización de malware en sistemas operativos Windows**	**1**	6 ECTS
4 **Ciberinteligencia de la amezanaza**	**1**	3 ECTS
5 **Arquitecturas de Detección de SIEM (Security Information and Event Management)**	**2**	3 ECTS
6 **Modelado de Casos de Uso, reglas de correlación ya alertas en SIEM**	**2**	3 ECTS
7 **Pentesting de sistemas**	**2**	9 ECTS
8 **Pentesting web**	**2**	3 ECTS
9 **Pentesting wifi y redes inalámbricas**	**3**	3 ECTS
10 **Penteting de sistemas industriales**	**3**	3 ECTS
11 **Fuzzing. Exploiting**	**4**	6 ECTS
12 **Gestión de alertas y threat Hunting**	**4**	3 ECTS
13 **Esquemas de respuesta y Playbooks**	**4**	3 ECTS
14 **Preparación Offensive Security Certified Professional (OSCP)**	**4**	3 ECTS
15 **Bitácoras e informes técnicos y ejecutivos. Cuadros de mandos de Detección**	**4**	3 ECTS
16 **TRABAJO FINAL DE MÁSTER**	**4**	13 ECTS
«Clic aquí para añadir asignatura obligatoria en este módulo»		
Asignaturas optativas		

	0	0 ECTS
«Clic aquí para añadir asignatura optativa en este módulo»		
Mód. :		
Asignaturas obligatorias		
0	**0**	**0 ECTS**
Clic aquí para añadir asignatura		
Asignaturas optativas		
0	**0**	**0 ECTS**
Clic aquí para añadir asignatura		
«Clic aquí para añadir tabla de Módulo»		
CREDITOS TOTALES		**70 ECTS**

6.3. Número mínimo de créditos de matrícula por estudiante y Periodo lectivo : 70 ECTS por Periodo

6.4. Normas de permanencia [máx. 1000 caracteres o 15 líneas]:ok

Normativa de asistencia obligatoria al 80% de las sesiones.

6.5. En el caso de que el Título propuesto sea un Máster, ¿se ofertará alguno de sus módulos (o asignaturas) como título independiente de menor duración o como curso de corta duración?

SÍ ☐ NO ☒

En caso afirmativo:

6.5.1. Módulo/s o asignaturas que se ofertarán:

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

Ej. Mód.I (asig. 1, 2 y 3)

6.5.2. Clase de enseñanza ofertada: clic aquí

6.5.3. Número de créditos y precio

Nº de créditos ECTS	Precio por crédito	Precio total
0 ECTS	0 €	0,00 €

6.6. Contenido de las enseñanzas (FICHAS POR ASIGNATURA). [AÑADA FICHAS DE ASIGNATURA SEGÚN PROCEDA]

Asignatura Nª 1 (Mód. I) : FUNDAMENTOS RED TEAM BLUE TEAM
Número de créditos (mín. 3 ECTS): 3 **Carácter (obligatoria/optativa):** Obligatoria **Carácter (presencial/ no presencial):** No presencial **Periodo lectivo de impartición:** 1er Cuatrimestre **Requisitos previos (en su caso):**
Competencias (enumere las que correspondan conforme al apartado 3.2): CG1, CG3
Actividades formativas y competencias a las que corresponden: Clases , resolución de talleres, prácticas evaluables de la asignatura
Acciones de coordinación (en su caso):
Sistemas de evaluación y calificación: Asistencia a clase 0% Evaluación continua 80 Examen final 20 TOTAL (la suma debe ser 100%)

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

Programa de la Asignatura:

- Esquemas Red, Blue, Purple y White.
- Función Red Team. Diferencias con otros modelos de evaluación.
- Conceptos fundamentales de hacking.
- Red Teaming. Anatomía de una intrusión (Tácticas, Técnicas y Procedimientos).
- Funciones Blue Team.
- Roadmap SIEM: eventos, integración y alertas (Casos de Uso).
- Monitorización y Respuesta ante incidentes.
- Modelo de Relación Red Blue

Equipo docente de la asignatura (nombre, apellido y Centro de adscripción)

1. **ÁLVARO ORTIGOSA (EPS UAM)**
2. **FRANCISCO DAMIÁN RUIZ SORIANO (EXPERTO CIBERSEGURIDAD)**

Copie y numere líneas tantas veces como necesite

Asignatura Nº 2 (Mód.) : RECONOCIMIENTO. VECTORES DE ENTRADA Y ACCESO

Número de créditos (mín. 3 ECTS): 3

Carácter (obligatoria/optativa) : Obligatoria

Carácter (presencial/no presencial) : No presencial

Periodo lectivo de impartición: 1er Cuatrimestre

Requisitos previos (en su caso) :

Competencias (enumere las que correspondan conforme al apartado 3.2):

CG1, CG2, CG3, CE1, CE12

Actividades formativas y competencias a las que corresponden:

Clases , resolución de talleres, prácticas evaluables de la asignatura

Acciones de coordinación (en su caso):

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

Sistemas de evaluación y calificación:

Asistencia a clase	**0 %**
Evaluación continua	**80 %**
Examen final	**20 %**
TOTAL (la suma debe ser	**100%)**

Programa de la asignatura:

En esta asignatura se profundizará, desde un punto de vista teórico/práctico, en los diferentes vectores que pueden permitir el acceso a una organización sin conocimiento previo de la misma.

Inicialmente el alumno estudiará en detalle las bases sobre como mapear e identificar todos los activos sobre los cuales poder desarrollar las pruebas en busca de un vector, para posteriormente abordar los diferentes vectores que a día de hoy son más comunes. Estos vectores son los que permiten que un potencial atacante sin acceso a la organización logre el compromiso de un primer activo que le permita la interacción con redes internas, y con ello profundizar en la intrusión.

Entre los diferentes ámbitos y pruebas que serán estudiadas están la identificación de vectores a través de perímetro (activos expuestos en Internet), infraestructura y clientes Wi-Fi, uso de malware, diferentes vertientes de ingeniería social (phishing o vishing entre otros), y la intrusión física.

Programa de la asignatura:

En esta asignatura se profundizará, desde un punto de vista teórico/práctico, en los diferentes vectores que pueden permitir el acceso a una organización sin conocimiento previo de la misma.

- Introducción al reconocimiento externo de infraestructuras
- Identificación y mapeo de los activos a explorar
- Exploración de activos en busca de los vectores actualmente conocidos.
  * Identificación de vectores en el perímetro
  * Identificación en infraestructura y clientes Wi-Fi
  * Uso de malware
  * Ingeniería social (Phishing, Vishing, etc)
  * Intrusión Física
- Análisis de los pasos a seguir para profundizar la intrusión

Universidad Autónoma de Madrid

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

Equipo docente de la asignatura (nombre, apellido y Centro de adscripción):

ÁLVARO ORTIGOSA (EPS UAM) Y EDUARDO ARRIOLS (PROFESIONAL CIBERSEGURIDAD)

Asignatura Nº 3 (Mód.) : EXTRACCIÓN DE ARTEFACTOS FORENSES Y CARACTERIZACIÓN DE MALWARE EN SISTEMAS OPERATIVOS WINDOWS.

Número de créditos (mín. 3 ECTS): 6

Carácter (obligatoria/optativa) : Obligatoria

Carácter (presencial/no presencial) : No presencial

Periodo lectivo de impartición: 1er Cuatrimestre

Requisitos previos (en su caso) :

Competencias (enumere las que correspondan conforme al apartado 3.2):

CG2, CG3, CG4

Actividades formativas y competencias a las que corresponden:

Clases , resolución de talleres, prácticas evaluables de la asignatura

Acciones de coordinación (en su caso):

Sistemas de evaluación y calificación:

Asistencia a clase	**0 %**
Evaluación continua	**80 %**
Examen final	**20 %**
TOTAL (la suma debe ser	**100%)**

Programa de la asignatura:

Extracción y análisis de artefactos forenses

Herramientas para la obtención y análisis de artefactos forenses

Generalidades

WMIC

- PowerShell
- Kansa
- KAPE
- DeepBlueCLI
- Sysinternals Sysmon
- Volatility Framework
- Google Rekall Framework
- Bash

Detección de actividad maliciosa en un sistema

- Detección de malware en un sistema víctima
- Detección de sistemas comprometidos sin presencia de malware activo
- Actividad maliciosa escondida a simple vista
- Técnicas evasivas empleadas por el malware
- Código firmado empleando certificados digitales de confianza
- Distinguiendo el comportamiento normal del malicioso
- Procesos legítimos de Microsoft Windows
- Detección de comportamiento anómalo
- Detección de persistencia en el arranque de Windows
- Detección de servicios maliciosos
- Detección de Tareas Programadas maliciosas
- Seguimiento de la actividad de las cuentas de usuario
- Seguimiento de movimiento lateral
- Detección de instalación de aplicaciones en el sistema
- Detección de manipulación de logs de eventos
- Evidencias de ejecución de malware
- Seguimiento de procesos y captura de la línea de comandos
- Ejecución maliciosa de PowerShell
- Utilización maliciosa de .NET

Investigando ataques WMI

- Introducción
- Arquitectura WMI
- Clases WMI y namespaces
- Consultas WMI
- Interacción con WMI
- WMI en remoto
- Eventos WMI
- Ataques WMI
- Defensa WMI

Ataques de movimiento lateral en entornos Windows

- Introducción
- Etapas de un ataque de movimiento lateral
- RID Hijacking
- Captura de credenciales
- Detección de robo de credenciales
- Técnicas maliciosas de paso de credenciales a un AD

Mitigación de robo de credenciales
Ataques explotando el protocolo RDP
Ataques empleando la herramienta WinSCP
Explotación de shares de administrador
Ejecución de comandos y/o malware en el sistema remoto con PsExec
Herramientas de gestión remota de Windows
Movimiento lateral empleando WMI
Movimiento lateral empleando PowerShell
Movimiento lateral empleando el software de despliegue de actualizaciones del objetivo
Movimiento lateral manipulando el servicio WSUS
Explotación de vulnerabilidades
Ataque PTH
Detección y mitigación de ataques PTH
Ataques contra el protocolo Kerberos y AD
Técnicas de movimiento lateral con DCOM
Detección de movimientos laterales en entornos Windows

Caracterización de malware

Introducción
Motivos para realizar un análisis de malware
Vectores de infección de un sistema
Propagación de malware
Distribución de malware a través de la Web
Capacidades del malware
Virus y gusanos
Troyanos (Trojan horses)
Adware/spyware
Scareware
Wiper
Ransomware
Downloaders y launchers
Puertas traseras (backdoors)
Rootkits
Malware de exfiltración de información
Robo de credenciales
Malware a nivel BIOS/firmare
Identificación y extracción del malware
Introducción
Detección de la configuración
Modelado
Indicadores
Comportamiento de la amenaza
Comparación de las diferentes aproximaciones de detección de la amenaza
Indicadores de que se ha producido una brecha de seguridad

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

Etapas del análisis de malware
- Introducción
- Análisis completamente automatizado
- Análisis estático de propiedades
- Análisis interactivo de comportamiento
- Ingeniería inversa manual del código
- Combinando las etapas de análisis de malware

Técnicas básicas de análisis estático de malware
- Empleo de herramientas antivirus
- Resúmenes como huella digital de malware
- Búsqueda de cadenas de texto
- Búsqueda de mutexes
- Búsqueda de patrones con YARA
- Identificación de las dependencias de archivos
- Atoms y tablas atom
- Malware empaquetado y ofuscado
- Búsqueda de la información de PE
- Desensamblado de código

Técnicas básicas de análisis dinámico de malware
- Introducción
- Monitorización de instalación de aplicaciones
- Monitorización de procesos
- Monitorización de archivos y carpetas
- Monitorización del Registro de Windows
- Monitorización del tráfico de red de las Capas de Red y Transporte
- Monitorización/resolución DNS
- Monitorización de tráfico de red en la Capa Aplicación
- Monitorización de las llamadas a la API de Microsoft Windows
- Monitorización de controladores de dispositivos
- Monitorización de programas al iniciarse Microsoft Windows
- Monitorización de servicios en Microsoft Windows

Equipo docente de la asignatura (nombre, apellido y Centro de adscripción):

MARIO GUERRA SOTO (MINISTERIO DE DEFENSA)

Asignatura Nº 4 (Mód.) : CIBERINTELIGENCIA DE LA AMENAZA

Número de créditos (mín. 3 ECTS): 3

Carácter (obligatoria/optativa) : Obligatoria

Carácter (presencial/no presencial) : No presencial

Periodo lectivo de impartición: 1er Cuatrimestre

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

Requisitos previos (en su caso) :

Competencias (enumere las que correspondan conforme al apartado 3.2):

CG1, CG2, CG3, C32, CE9, CE10, CE12

Actividades formativas y competencias a las que corresponden:

Clases , resolución de talleres, prácticas evaluables de la asignatura

Acciones de coordinación (en su caso):

Sistemas de evaluación y calificación:

Asistencia a clase	**0 %**
Evaluación continua	**80 %**
Examen final	**20 %**
TOTAL (la suma debe ser	**100%)**

Programa de la asignatura:

Introducción a la ciberinteligencia
- Agentes de la amenaza
  - Cibercriminales
  - Hacktivistas
  - Atacantes con apoyo estatal
  - La amenaza interna (insider threat)
  - Otras posibles clasificaciones
- Categorización de la ciberamenaza
- Ciberguerra y ciberoperaciones
- Defensa de red basada en inteligencia
- Pasos para la ejecución de un ciberataque (Cyber Kill Chain)
  - Reconocimiento (Reconnaissance)
  - Preparación de la operación (Weaponize)
  - Envío (Deliver)
  - Explotación (Exploit)
  - Instalación en la víctima (Installation)
  - Control remoto del malware (Command and Control)
  - Acciones sobre los objetivos (Actions on objectives)
- Cursos de acción
- Reconstrucción de una intrusión

- Análisis de campaña

Modelos en CTI

- Modelo en Diamante de Análisis de Intrusión
- Modelo ATT&CK for Enterprise
- Modelo de FireEye para el ciclo de vida de un ciberataque

Inteligencia de la amenaza

- Definiciones básicas
  - Dato, información e inteligencia
  - Inteligencia de la amenaza
  - Decepción y cibercontrainteligencia
  - Plataformas de inteligencia de la amenaza
- Planificación de inteligencia de la amenaza
- Tipologías de inteligencia de la amenaza
  - Según el modo de procesar los datos
  - Inteligencia de la amenaza funcional
  - Requisitos para disponer de capacidad propia de CTI
  - Valoración de la inteligencia de la amenaza
- Identificando las TTP de las potenciales amenazas
  - OSINT
  - Darknets
  - Escaneo e indexación
  - Procesado de código malicioso
  - Ingeniería social
- Seleccionando las fuentes de inteligencia
- Destinatarios de la inteligencia de la amenaza
  - Equipos de defensa de las redes corporativas
  - Equipos de gestión de vulnerabilidades
  - Analistas de la ciberamenaza
  - Gestión de la seguridad de la información
  - Junta directiva de la organización
- Integrando la inteligencia de la amenaza en la respuesta a incidentes
  - Fase de planificación previa
  - Fase de generación de eventos
  - Fase de respuesta a incidentes
  - Fase de respuesta a intrusiones
- Compartición de la ciberinteligencia
- Estándares para la compartición de IOC
- Estándares para la compartición de CTI
  - Introducción
  - STIX
  - TAXII
- MISP Y REYES
  - MISP
  - REYES
- Fuentes abiertas de CTI

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

Análisis de datos
- Introducción
- Contextualización de los datos
- Tipos de análisis de datos
- Técnicas de análisis de datos

Atribución
- Introducción
- Búsqueda de huellas humanas en muestras de malware

Equipo docente de la asignatura (nombre, apellido y Centro de adscripción):

MARIO GUERRA SOTO (MINISTERIO DE DEFENSA)

Asignatura Nº 5 (Mód.) : ARQUITECTURA DE DETECCIÓN DE SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT)

Número de créditos (mín. 3 ECTS): 3

Carácter (obligatoria/optativa) : Obligatoria

Carácter (presencial/no presencial) : No presencial

Periodo lectivo de impartición: 2ndo Cuatrimestre

Requisitos previos (en su caso) :

Competencias (enumere las que correspondan conforme al apartado 3.2):

CG2, CE3

Actividades formativas y competencias a las que corresponden:

Clases , resolución de talleres, prácticas evaluables de la asignatura

Acciones de coordinación (en su caso):

Sistemas de evaluación y calificación:

Asistencia a clase	**0 %**
Evaluación continua	**80 %**
Examen final	**20 %**

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

TOTAL (la suma debe ser 100%)

Programa de la asignatura:

En esta asignatura se abordará qué es y como funciona un sistema de gestión y eventos de seguridad (en inglés, SIEM), herramienta fundamental para la detección y gestión de incidentes de seguridad en los SOC (Security Operation Center).

Los alumnos aprenderan inicialmente cuales son los conceptos básicos, evolución y arquitectura de los SIEM, incluyendo un estudio detallado de todas las capas que los componen.

Posteriormente, se abordará el proceso de la gestión de logs/eventos de seguridad e integración de las principales fuentes de información, de la telemetría interna de la organización a monitorizar, en la tecnología SIEM.

Además, se abordará cuales son las principales fases en el diseño y despliegue de un SIEM y pondrán en práctica el conocimiento adquirido a través de casos prácticos con herramientas SIEM open source y con la herramienta comercial emasSOM (licencia cedida por S2Grupo).

PROGRAMA ACADÉMICO

1. Introducción a las tecnologías SIEM
    a. SOC (Security Operation Center)
    b. Conceptos y arquitecturas de SIEM
        - Capa de recolección
            1. Arquitecturas distribuidas de sensores de recolección
                a. Syslog
                b. Otros mecanismos de recopilación de logs
            2. Integración y normalización de logs
        - Reglas de agregación y correlación
        - Dashboards
    c. Evolución de la tecnología
        - SIEM Intelligence
            1. Detección por comportamiento (Behavioral Analysis)
            2. Machine Learning

2. Telemetría interna
    a. Endpoint
        - HIDS y Sistemas Antivirus
        - Sistemas EDR
        - Casos prácticos: CLAUDIA (Herramienta desarrollada por el CCN-CERT y S2Grupo. Licencia cedida por S2Grupo)
        - Casos prácticos : OSSEC (Open Source)
    b. Red
        - Principales fuentes de información

- Sistemas de Detección y Prevención de Intrusos
  1. Ejemplos prácticos: Snort/Suricata (Open Source)
- Detección basada en patrones vs basada en anomalías
  1. Casos prácticos: CARMEN (Herramienta desarrollada por el CCN-CERT y S2Grupo. Licencia cedida por S2Grupo)

c. Sistemas de Deception o Contrainteligencia

3. Telemetría externa
- **a.** Feeds de inteligencia
- **b.** OSINT

4. Introducción al modelado de casos de uso

5. Diseño y despliegue de un SIEM
- **a.** Estudio de la plataforma tecnológica objeto de la monitorización
- **b.** Fuentes de información a integrar en el SIEM
  - Análisis y procesado de los logs/registros
- **c.** Dimensionado del SIEM
- **d.** Retención de Logs
- **e.** Arquitectura de Red
- **f.** Solución final

6. Tipos de prestación de servicios
- **a.** As A service
- **b.** On premise
- **c.** Normativa
- **d.** Ventajas vs Inconvenientes

7. SIEM Fabricantes
- **a.** Caso de estudio: Splunk (Free License)
- **b.** Caso de estudio: emasSOM (Licencia cedida por S2Grupo)
- **c.** Otros

Equipo docente de la asignatura (nombre, apellido y Centro de adscripción):

MAITE MORENO (S2 GROUP)

Asignatura Nº 6 (Mód.) : MODELADO DE CASOS DE USO, REGLAS DE CORRELACIÓN Y ALERTAS EN SIEM

Número de créditos (mín. 3 ECTS): 3

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

Carácter (obligatoria/optativa) : Obligatoria

Carácter (presencial/no presencial) : No presencial

Periodo lectivo de impartición: 2ndo Cuatrimestre

Requisitos previos (en su caso) :

Competencias (enumere las que correspondan conforme al apartado 3.2):

CG2, CG3, CE4

Actividades formativas y competencias a las que corresponden:

Clases , resolución de talleres, prácticas evaluables de la asignatura

Acciones de coordinación (en su caso):

Sistemas de evaluación y calificación:

Asistencia a clase	**0 %**
Evaluación continua	**80 %**
Examen final	**20 %**
TOTAL (la suma debe ser	**100%)**

Programa de la asignatura:

Con los conocimientos adquiridos en el resto de asignaturas, vamos a aprender a identificar los tipos de amenazas más conocidas en nuestros SIEM a través de los diferentes casos de uso así como su codificación lógica en forma de regla dependiendo de cada fabricante. Se utilizarán las reglas Sigma para la explicación lógica del modelado de datos.

- Diferencias entre casos de uso y reglas de correlación.
- Sigma y los despliegues de casos de uso.
- Clasificaciones de casos de uso:
    - Categorías:
        - Ataques internos / externos
        - DoS
        - DLPs
    - Tecnologías:

- IPS / IDS / FW / DA / VPN / Correlación
- Afectación:
  - Confidecialidad
  - Integridad
  - Disponibilidad
- Seguimiento de usuarios
- Equipos comprometidos
- Cambios en el sistema
- IPS/IDS/EDR/AV
- Anomalías de red
- WAFs / DMZ
- Cloud
- DLPs
- Threats intelligence feeds
- Tipos de cierre de los incidentes. Escalado a cliente o IR.

Equipo docente de la asignatura (nombre, apellido y Centro de adscripción):

MARTA LÓPEZ PARDAL (ElevenPaths)

Asignatura Nº 7 (Mód.) : PENTESTING DE SISTEMAS

Número de créditos (mín. 3 ECTS): 9

Carácter (obligatoria/optativa) : Obligatoria

Carácter (presencial/no presencial) : No presencial

Periodo lectivo de impartición: 2ndo Cuatrimestre

Requisitos previos (en su caso) :

Competencias (enumere las que correspondan conforme al apartado 3.2):

CEG1, CG3, CE6, CE12

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

Actividades formativas y competencias a las que corresponden:

Clases , resolución de talleres, prácticas evaluables de la asignatura

Acciones de coordinación (en su caso):

Sistemas de evaluación y calificación:

Asistencia a clase	**0 %**
Evaluación continua	**80 %**
Examen final	**20 %**
TOTAL (la suma debe ser	**100%)**

Programa de la asignatura:

En la asignatura se tratará de manera fundamentalmente práctica la secuencia de un ataque que realizaría un atacante real, centrándose fundamentalmente en las acciones que se llevarían para aprovechar vulnerabilidades y malas configuraciones existentes en servicios expuestos a Internet, sin olvidar aquellas que presentan los equipos de cliente y las posibles acciones llevadas a cabo por los usuarios de los mismos, tanto en entornos Windows como Linux. Antes de comenzar con la parte práctica, en la que se estudiarán y se practicará con distintas herramientas que podría utilizar un atacante, es imprescindible proporcionar una base teórica para identificar las diferencias entre un análisis de vulnerabilidades y un pentesting, así como identificar las particularidades de un Red Team. Asimismo, se estudiará cómo tomar notas de una manera eficaz, fundamental a la hora de mantener un registro de las acciones realizadas y los resultados obtenidos, que toma más importancia si cabe cuando se trata de las acciones realizadas como parte de un equipo.

1. Introducción al Pentesting

1.1. Conceptos y definiciones.

1.2. Diferencias entre análisis de vulnerabilidades, pentesting, Red Team.

1.3. Vectores de ataque.

1.4. Secuencia típica de un ataque.

1.5. Documentación del proceso.

2. Reconocimiento

2.1. Identificación de objetivos.

2.2. Obtención de información.

3. Enumeración

3.1. Enumeración de redes y escaneo de servicios.

3.2. Identificación de vulnerabilidades

4. Explotación

4.1. Explotación de servicios y malas configuraciones

4.2. Ataques a cliente

4.3. Técnicas de evasión

5. Post- Explotación

5.1. Escalada de privilegios.

5.2. Persistencia.

5.3. Movimiento lateral.

Partiendo de los conocimientos adquiridos durante la asignatura "2. Reconocimiento. Vectores de entrada y acceso" se pasará a la enumeración de vulnerabilidades en los servicios expuestos. A continuación, se verán las posibles vías de explotación de estas vulnerabilidades para ganar acceso al primer equipo de la red, y las acciones de post-explotación posteriores, tendentes a ganar privilegios en el sistema, así como identificar otros equipos internos y el movimiento lateral por la red atacada y la persistencia en la misma, disminuyendo las posibilidades de detección. También se analizarán distintas formas de atacar directamente a un usuario logrando que este ejecute de código que permita el acceso a su equipo.

Equipo docente de la asignatura (nombre, apellido y Centro de adscripción):

JORGE LÓPEZ DE VERGARA (EPS UAM), ROBERTO LATORRE CAMINO (EPS UAM), MIGUEL ÁNGEL MORA RINCÓN (EPS UAM), LUIS HERRERO PÉREZ (MINISTERIO DEFENSA)

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

Asignatura Nº 8 (Mód.) : PENTESTING WEB

Número de créditos (mín. 3 ECTS): 3

Carácter (obligatoria/optativa) : Obligatoria

Carácter (presencial/no presencial) : No presencial

Periodo lectivo de impartición: 2ndo Cuatrimestre

Requisitos previos (en su caso) :

Competencias (enumere las que correspondan conforme al apartado 3.2):

CE3, CE5

Actividades formativas y competencias a las que corresponden:

Clases , resolución de talleres, prácticas evaluables de la asignatura

Acciones de coordinación (en su caso):

Sistemas de evaluación y calificación:

Asistencia a clase	**0 %**
Evaluación continua	**80 %**
Examen final	**20 %**
TOTAL (la suma debe ser	**100%)**

Programa de la asignatura:

- Introducción al Pentesting Web: Fases de un test de penetración de aplicaciones web; Contexto actual, herramientas más utilizadas y metodologías de trabajo más utilizadas; Vulnerabilidades más comunes, arquitectura web, servidores de aplicaciones más usados; Importancia del desarrollo seguro y una introducción al software de análisis de código estático.
- Fases de Gathering – Fingerprinting: Conceptos básicos de métodos HTTP, tipos de autenticación y codificación; Fingerprinting, frameworks más utilizados, arquitectura web y métodos de ataque de ataque; Fase de gathering, terminología y herramientas más utilizadas; Introducción al manejo de Burp Suite

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

- Controles del Lado Cliente: Análisis del contenido que se esconde al otro lado de una aplicación web; Vulnerabilidades desde el lado del cliente; Captura de tráfico, reconocimiento y análisis posterior; Serialización Java, Flash y Silverlight
- Manejo de Sesiones: Vulnerabilidades desde el lado del cliente; Captura de tráfico, reconocimiento y análisis posterior; Serialización Java, Flash y Silverlight
- Inyecciones: Tipos de inyecciones más comunes, detección y prevención; Inyecciones avanzadas en Microsoft SQL, MySQL y Oracle; Inyecciones XPath e Inyecciones LDAP
- Explotación de Servicios Backend: Fase de explotación de un pentest web; Inyecciones que permiten interactuar directamente con los servicios de back-end ; Inyección de comandos de sistema, manipulación de path, inyecciones XML y la manera de prevenirlas
- Ataques a Usuarios: Análisis y manejo de datos recopilados en fases anteriores; Ataques a sistemas y evaluación de su estado de seguridad; Detección y prevención de Cross-Site Scripting; Cross-Site Scripting: Reflejado, Almacenado y DOM
- Ataques a la Insfraestructura Web: Técnicas de ataque a servidores de aplicaciones; Vulnerabilidades más comunes dentro de la infraestructura de un servidor web; Ataques mediante buffer overflows; Pruebas de concepto, vídeos y ejercicios prácticos

Equipo docente de la asignatura (nombre, apellido y Centro de adscripción):

RAMÓN FUENTES REQUENA (GUARDIA CIVIL)

Asignatura Nº 9 (Mód.) : PENTESTING WIFI Y REDES INALÁMBRICAS

Número de créditos (mín. 3 ECTS): 3

Carácter (obligatoria/optativa) : Obligatoria

Carácter (presencial/no presencial) : No presencial

Periodo lectivo de impartición: 3er Cuatrimestre

Requisitos previos (en su caso) :

Competencias (enumere las que correspondan conforme al apartado 3.2):

CG1, CG3, CE7, CE12

Actividades formativas y competencias a las que corresponden:

Clases , resolución de talleres, prácticas evaluables de la asignatura

Acciones de coordinación (en su caso):

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

Sistemas de evaluación y calificación:

Asistencia a clase	**0 %**
Evaluación continua	**80 %**
Examen final	**20 %**
TOTAL (la suma debe ser	**100%)**

Programa de la asignatura:

1. Arquitecturas de redes inalámbricas
2. Esquemas de seguridad en redes inalámbricas
3. Pentesting para los distintos esquemas de seguridad
4. Obtención de información en redes inalámbricas

Equipo docente de la asignatura (nombre, apellido y Centro de adscripción):

JORGE LÓPEZ DE VERGARA (EPS UAM)

Asignatura Nº 10 (Mód.) : PENTESTING DE SISTEMAS INDUSTRIALES

Número de créditos (mín. 3 ECTS): 3

Carácter (obligatoria/optativa) : Obligatoria

Carácter (presencial/no presencial) : No presencial

Periodo lectivo de impartición: 3er Cuatrimestre

Requisitos previos (en su caso) :

Competencias (enumere las que correspondan conforme al apartado 3.2):

CG1, CG3, C38, CE12

Actividades formativas y competencias a las que corresponden:

Clases , resolución de talleres, prácticas evaluables de la asignatura

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

Acciones de coordinación (en su caso):

Sistemas de evaluación y calificación:

Asistencia a clase	**0 %**
Evaluación continua	**80 %**
Examen final	**20 %**
TOTAL (la suma debe ser	**100%)**

Programa de la asignatura:

Durante las clases el alumno adquirirá el conocimiento necesario comenzar con el análisis de sistemas embebidos:

- Aprenderá a identificar los componentes físicos que contienen, con qué protocolos de comunicación interactúan entre ellos y cómo pueden ser manipulados mediante ejemplos prácticos.
- Aprenderá a utilizar herramientas hardware para investigar los buses de datos de los dispositivos, así como para la extracción de firmware.
- Una vez dominada la parte física pasaremos a analizar firmware mediante la extracción, modificación, emulación y búsqueda de vulnerabilidades entre otras tareas.
- Aprenderá la metodología y fases necesarias para llevar a cabo un test de penetración en Sistemas de Control Industrial y a cómo utilizar herramientas open source más comunes para esta tarea.
- Se tratarán los conceptos y definiciones que engloban a los sistemas de control industrial (Industrial Control System I.C.S.) así como su catalogación y securización. A su vez se entregará, a cada alumno partícipe de la asignatura, una **licencia profesional, válida por un periodo de 365 días, del software de Ingeniaría TIA Portal en su versión 15_x,** para su uso.
- Durante las clases presenciales, se mostrará instrumentación real involucrada en los procesos industriales (firewall industrial, autómatas programables de la serie PLC 1200, dispositivos de conexión inalámbrica y 4G etc).

Temario:

Sección 1: Introducción y conceptos básicos

Definición y objetivos del Hardware Hacking

Definición de Sistema Embebido

Definición de Dispositivo IoT

Laboratorio y herramientas de trabajo

Preparación del entorno de Laboratorio

Sección 2: Análisis de Sistemas Embebidos

Análisis de Hardware

Recolección de información

Identificación de componentes

Lectura y análisis de buses de datos UART

Interacción con buses de datos UART

Identificación de pines JTAG

Interacción con JTAG

Extracción del contenido de una memoria vía SPI

Extracción del contenido de una memoria vía I2C

Extracción del contenido de una memoria vía JTAG

Extracción del contenido de una memoria eMMC vía Chip-Off

Medidas de protección Anti Tampering

Sección 3: Análisis y Ataques a Firmware

OWASP Firmware Security Testing Methodology

Extracción y análisis de firmware

Modificación y emulación de firmware

Explotación de firmware

Medidas de protección para firmware

Sección 4: Ataques a Sistemas Embebidos

Mapa de amenazas y ataques en Sistemas Embebidos

Introducción a Jupyter Notebooks y Jupyer Labs
Automatización de tareas de análisis con Jupyter Notebooks
Ejemplo práctico de ataque sobre STM32 con Jupyter Notebooks

Sección 5: Ataques a Sistemas Industriales

Introducción a los sistemas de control industrial (ICS / SCADA) con descripción de categorías y evolución histórica.

Conceptos base en sistemas de control industrial.

Particularidades de la configuración de la seguridad industrial.

Vulnerabilidades y Amenazas Sistemas Control Industrial.

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

Safety / Security.

¿Por qué es diferente la seguridad respecto a otros elementos de las tecnologías de la información?

Aspectos básicos de Seguridad de Redes.

Iniciativas, buenas prácticas y soluciones de seguridad.

Descubrimiento de riesgos en los sistemas SCADA.

Vulnerabilidades SCADA.

Contra medidas.

Ingeniería social específica para ataques a SCADA.

Recomendaciones de seguridad específicas para SCADA.

Equipo docente de la asignatura (nombre, apellido y Centro de adscripción):

MARTINA MATARI GONZÁLEZ (TELEFÓNICA) Y SANTIAGO GONZÁLEZ GONZÁLEZ (CNPIC)

Asignatura Nº 11 (Mód.) : FUZZING. EXPLOITING

Número de créditos (mín. 3 ECTS): 6

Carácter (obligatoria/optativa) : Obligatoria

Carácter (presencial/no presencial) : Presencial

Periodo lectivo de impartición: 4º Cuatrimestre

Requisitos previos (en su caso) :

Competencias (enumere las que correspondan conforme al apartado 3.2):

GC1, GC3, GC9

Actividades formativas y competencias a las que corresponden:

Clases , resolución de talleres, prácticas evaluables de la asignatura

Acciones de coordinación (en su caso):

Sistemas de evaluación y calificación:

Asistencia a clase 0 %

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

Evaluación continua	**80 %**
Examen final	**20 %**
TOTAL (la suma debe ser	**100%)**

Programa de la asignatura:

Para todo buen pentester o red teamer es importante conocer distintas técnicas de explotación, si se quiere llegar a un nivel avanzado. Por lo que, lo primero de todo, es básico conocer a fondo cómo funciona la memoria del sistema desde el punto de vista de *exploiting*, además de ensamblador x86, *linking* y *loading*. Una vez encontramos una vulnerabilidad, a través de técnicas de *fuzzing*, se utiliza un desesamblador para conseguir ejecución remota de código o elevación de privilegios. Comenzaremos por un básico *stack buffer overflow* y llegaremos a evadir distintas técnicas de protección en sistemas Windows y Linux.

1. Fuzzing
    1. Introducción a Fuzzing
    2. Técnicas de Fuzzing
    3. Crear tu propio fuzzer
    4. Fuzzing Block Coverage Measurement
    5. Source-assisted fuzzing con AFL

2. Exploiting en Linux
    1. Introducción a la memoria
    2. Lenguaje ensamblador x86
    3. Linkers y Loaders
    4. Introducción a shellcodes
    5. Técnicas de exploiting en Linux
    6. Técnicas avanzadas para la evasión de protección de memoria

3. Exploiting en Windows
    1. Introducción a exploiting en Windows
    2. Protecciones de memoria en Windows
    3. Windows Overflows
    4. Técnicas avanzadas para la evasión de protección de memoria
    5. Windows shellcodes

Equipo docente de la asignatura (nombre, apellido y Centro de adscripción):

SANDRA BARDÓN MORAL (MINISTERIO DE DEFENSA)

Asignatura Nº 12 (Mód.) : GESTIÓN DE ALERTAS Y THREAT HUNTING

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

Número de créditos (mín. 3 ECTS): 3

Carácter (obligatoria/optativa) : Obligatoria

Carácter (presencial/no presencial) : No presencial

Periodo lectivo de impartición: 4º Cuatrimestre

Requisitos previos (en su caso) :

Competencias (enumere las que correspondan conforme al apartado 3.2):

CG1, CG2, CE10

Actividades formativas y competencias a las que corresponden:

Clases , resolución de talleres, prácticas evaluables de la asignatura

Acciones de coordinación (en su caso):

Sistemas de evaluación y calificación:

Asistencia a clase	**0 %**
Evaluación continua	**80 %**
Examen final	**20 %**
TOTAL (la suma debe ser	**100%)**

Programa de la asignatura:

Gestión de Alertas

- Introducción
- Capacidad de respuesta a ciberincidentes
  - Eventos e incidentes
  - Respuesta a los ciberincidentes
  - Política de seguridad de la información y gestión de ciberincidentes
  - Personal responsable de la gestión de incidentes
- Gestión de ciberincidentes
  - Fases de la gestión de incidentes
  - Clasificación de ciberincidentes
  - Detección de ciberincidentes
  - Determinación de la peligrosidad de un ciberincidente
  - Documentación de los ciberincidentes

Nivel de impacto del ciberincidente en la organización
Seguimiento del ciberincidente
Documentación del ciberincidente
Tipificación de causas y hechos del ciberincidente
Recolección y custodia de evidencias digitales
Intercambio de información y comunicación de ciberincidentes
Elementos para el cierre del ciberincidente
Integrando la inteligencia de la amenaza en la respuesta a incidentes
Fase de planificación previa
Fase de generación de eventos
Fase de respuesta a incidentes
Fase de respuesta a intrusiones

Threat hunting
Introducción
El proceso de threat hunting
Requisitos para poder realizar threat hunting
Recurso humano
Colectores de datos
Plan de threat hunting
Modelo de madurez de threat hunting

Equipo docente de la asignatura (nombre, apellido y Centro de adscripción):

ÁLVARO ORTIGOSA JUÁREZ (EPS UAM) Y MARIO GUERRA SOTO (MINISTERIO DE DEFENSA)

Asignatura Nº 13 (Mód.) : ESQUEMA DE RESPUESTA Y PLAYBOOKS

Número de créditos (mín. 3 ECTS): 3

Carácter (obligatoria/optativa) : Obligatoria

Carácter (presencial/no presencial) : No presencial

Periodo lectivo de impartición: 4º Cuatrimestre

Requisitos previos (en su caso) :

Competencias (enumere las que correspondan conforme al apartado 3.2):

CG1, CG2, CE11

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

Actividades formativas y competencias a las que corresponden:

Clases , resolución de talleres, prácticas evaluables de la asignatura

Acciones de coordinación (en su caso):

Sistemas de evaluación y calificación:

Asistencia a clase	**0 %**
Evaluación continua	**80 %**
Examen final	**20 %**
TOTAL (la suma debe ser	**100%)**

Programa de la asignatura:

- Respuestas a Incidentes: objetivos y metodologías.
- Equipo de respuesta a incidentes: posición, competencias y autoridad dentro de la organización. Definición de roles y responsabilidades de cada unidad.
- Responsabilidades departamentales y personales. Procedimientos operativos de seguridad: mecanismos y medios de notificación.
- Plan de respuesta a incidentes: el playbook. Estudio del ciclo de vida del Playbook: Preparación, Identificación, Contención, Erradicación, Recuperación, Repercusiones y Mejora Continua.
- Ejemplos prácticos:
- Malware:
- Gusanos (Específicos)
- Ransomware (Específicos)
- Dispositivos móviles (Específicos)
- Detección de intrusiones
- Windows (Específicos)
- Linux (Específicos)
- DDoS
- Chantaje
- Defacement
- Ingeniería social
- Fugas de información
- Insider
- Phishing
- Estafas (fraude al CEO)
- Daño de marca

Universidad Autónoma de Madrid

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

Equipo docente de la asignatura (nombre, apellido y Centro de adscripción):

Marta López Pardal (ElevenPaths)

Asignatura Nº 14 (Mód.) : PREPARACIÓN OFFENSIVE SECURITY CERTIFIED PROFESSIONAL (OSCP)

Número de créditos (mín. 3 ECTS): 3

Carácter (obligatoria/optativa) : Obligatoria

Carácter (presencial/no presencial) : No presencial

Periodo lectivo de impartición: 4º Cuatrimestre

Requisitos previos (en su caso) :

Competencias (enumere las que correspondan conforme al apartado 3.2):

CG1, CG3, CG4, CE2

Actividades formativas y competencias a las que corresponden:

Clases , resolución de talleres, prácticas evaluables de la asignatura

Acciones de coordinación (en su caso):

Sistemas de evaluación y calificación:

Asistencia a clase	**0 %**
Evaluación continua	**80 %**
Examen final	**20 %**
TOTAL (la suma debe ser	**100%)**

Programa de la asignatura:

OSCP es la certificación más reconocida en temas de pentesting, durante estos días de clase os mostraremos cual es el contenido, como es el examen y veremos en detalle todos los topics de la certificación:

- Recopilación pasiva de información
- Recopilación activa de información

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

- Análisis de vulnerabilidades
- Desbordamientos de búfer
- Win32 Buffer Overflow Exploitation
- Explotación de desbordamiento de búfer de Linux
- Trabajar con Exploits
- Transferencias de archivos
- Escalada de privilegios
- Ataques del lado del cliente
- Ataques a aplicaciones web
- Ataques con contraseña
- Redirección de puertos y túneles
- El Marco Metasploit
- Pasar por alto el software antivirus
- Montaje de las piezas: Desglose de la prueba de penetración

Esta certificación te proporcionará las siguientes competencias:

- Uso de técnicas de recopilación de información para identificar y enumerar objetivos que ejecutan diversos sistemas operativos y servicios
- Escribir scripts y herramientas básicas para ayudar en el proceso de prueba de penetración
- Analizar, corregir, modificar, compilar y portar código de explotación público
- Llevar a cabo ataques remotos y del lado del cliente
- Identificación y explotación de vulnerabilidades XSS, inyección SQL e inclusión de archivos en aplicaciones web
- Implementación de técnicas de tunelización para evitar cortafuegos
- Soluciones creativas de problemas y habilidades de pensamiento lateral

Equipo docente de la asignatura (nombre, apellido y Centro de adscripción):

ÓSCAR MAQUEDA HORTELLS (PROFESIONAL DE CIBERSEGURIDAD. EMPRESA DISRUPTIVE CONSULTING)

Asignatura Nº 15 (Mód.) : BITÁCORAS E INFORMES TÉCNICOS Y EJECUTIVOS. CUADROS DE MANDOS DE DETECCIÓN

Número de créditos (mín. 3 ECTS): 3

Carácter (obligatoria/optativa) : Obligatoria

Carácter (presencial/no presencial) : No presencial

Periodo lectivo de impartición: 4º Cuatrimestre

Requisitos previos (en su caso) :

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

Competencias (enumere las que correspondan conforme al apartado 3.2):

CG1, CG2, CG4, CE12

Actividades formativas y competencias a las que corresponden:

Clases , resolución de talleres, prácticas evaluables de la asignatura

Acciones de coordinación (en su caso):

Sistemas de evaluación y calificación:

Asistencia a clase	**0 %**
Evaluación continua	**80 %**
Examen final	**20 %**
TOTAL (la suma debe ser	**100%)**

Programa de la asignatura:

La gestión de básica de la Ciberseguridad no se asienta única y exclusivamente en pilares técnicos o procedimentales. Requiere una alta dosis de síntesis y evaluación continua que permita obtener los mejores resultados. Desarrollar un procedimiento elaborado de documentación técnica es esencial para dar solidez y consistencia al trabajo de campo elaborado por el equipo de Red Team. Tener afianzado un conocimiento previo sobre técnicas de documentación resulta esencial para el trabajo de cualquier pentester.

El desarrollo programático de las TTPs plasmadas en una bitácora será una técnica que jamás abandonará a los especialistas en Red Team, de ahí su importancia. Por otro lado, la capacidad de Protección, Detección y Respuesta debe imperiosamente estar reflejada en una documentación detallada que permita dar cobijo a todo el ámbito técnico sobre el cual oscilará el trabajo del Redteamer.

En este Máster el alumno podrá adquirir todas aquellas técnicas y competencias necesarias para cumplimentar una documentación técnica y ejecutiva que le permita en su posterior desempeño, poner en valor es trabajo realizado.

Índice programático de la asignatura

UD.1 - Introducción.

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

1.1 - Objetivo general. 1.2 - Objetivos específicos. 1.3 - Fundamentación teórica y estado del arte. UD.2 - Tipología documental. 2.1 - Bitácoras. 2.2 - Diagramas de flujo de información aplicado a Redteam. 2.3 - Documentación aplicada a informes ejecutivos. UD.3 - Recopilación de la información útil. 3.1 - Logs, categorización y observación. 3.2 - Herramientas de documentación. 3.3 - Narrativa del ataque. 3.4 - Referencias y bibliografía. Un paso esencial. UD.4 - Esquemas de Respuesta y Playbooks. 4.1 - Detección del flujo de datos y diagramas de flujo de ataques. 4.2 - Playbooks adaptados y demostrativos. 4.3 - Elaboración de informes ejecutivos. UD.5 - Desarrollo práctico. 5.1 - Proyecto: Documentación adaptativa de un proyecto único. 5.2 - Proyecto: Documentación ejecutiva de un proyecto general.
Equipo docente de la asignatura (nombre, apellido y Centro de adscripción): RAMÓN FUENTES REQUENA (GUARDIA CIVIL)
«Doble clic aquí para añadir ficha de asignatura»

Módulo de Prácticas Externas (en su caso):
Número de créditos: 0 ECTS
Descripción de las prácticas [máx. 750 caracteres o 10 líneas]:

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

Entidades colaboradoras para las prácticas externas: **1.** *Copie y numere líneas tantas veces como necesite*
Sistemas de evaluación y calificación de las prácticas [máx. 500 caracteres u 8 líneas]:

Trabajo Fin de Título:
Número de créditos (máx. 18 ECTS): 13 ECTS
Descripción del Trabajo Fin de Título [máx. 750 caracteres o 10 líneas]: **En el Trabajo Fin de Máster (12ECTS/ 300 horas) el estudiante desarrollará un trabajo original realizado individualmente por él, bajo la dirección y supervisión de un tutor. Se trata de un proyecto integral de naturaleza profesional. Su desarrollo debe involucrar la articulación de los conocimientos, habilidades y destrezas adquiridos a lo largo de la formación en el máster.** **Se fomentará y facilitará la realización del proyecto correspondiente al trabajo de fin de máster en el entorno profesional del estudiante, que requiera la aplicación de los conocimientos y competencias asociados al título y que permita comprobar que el estudiante ha logrado obtener las capacidades necesarias para analizar problemas com**
Sistema de evaluación del trabajo fin de Título [máx. 500 caracteres u 8 líneas]: **El TFM será tutorizado por un profesor del máster. En el caso que el estudiante desarrolle el TFM en su entorno profesional, el trabajo podrá ser tutorizado por una persona externa al máster, en cuyo caso deberá contar con un profesor del máster en el papel de ponente.** **La defensa del Trabajo Fin de Máster se realizará una vez aprobadas el resto de asignaturas necesarias para finalizar los estudios de Máster.**

7. PERSONAL ACADÉMICO

7.1. Profesorado UAM.

APELLIDOS	NOMBRE	FACULTAD /CENTRO	CATEGORÍA ACADÉMICA	DOCENCIA IMPARTIDA		
				Menos de 1 ECTS	Entre 1 y 3 ECTS	Más de 3 ECTS
ORTIGOSA JUÁREZ	ÁLVARO	EPS	Profesor Contratado Doctor	☐	☐	☒
LÓPEZ DE VERGARA	JORGE	EPS	Profesor Titular	☐	☒	☐
LATORRE CAMINO	ROBERTO	EPS	Profesor Contratado Doctor	☐	☒	☐
MORA RINCÓN	MIGUEL ÁNGEL	EPS	Profesor Contratado Doctor	☐	☒	☐
ANDRÉS SÁEZ	JUAN ANTONIO	EPS	Profesor Asociado	☐	☒	☐
Doble clic aquí						

7.2 Profesorado EXTERNO a la UAM

APELLIDOS	NOMBRE	FACULTAD /CENTRO	CATEGORÍA ACADÉMICA	DOCENCIA IMPARTIDA		
				Menos de 1 ECTS	Entre 1 y 3 ECTS	Más de 3 ECTS
RUIZ SORIANO	FRANCISCO DAMIÁN	Singular Bank		☐	☒	X☐
MAQUEDA HORTELLS	ÓSCAR	Disruptive Consulting		☐	☒	☐
GUERRA SOTOS	MARIO	Ministerio de Defensa		☐	☐	☒
FUENTES REQUENA	RAMÓN	Guardia Civil		☐	☐	☒

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

BARDÓN MORAL	**SANDRA**	**Ministerio de Defensa**		☐	☐	☒
MORENO GARCÍA	**MAITE**	**S2Group**		☐	☒	☐
LÓPEZ PARDAL	**MARTA**	**ElevenPath - Telefónica**		☐	☐	X☐
MATARI GONZÁLEZ	**MARTINA**	**Telefónica**		☐	☒	☐
ARRIOLS NUÑEZ	**EDUARDO**	**RootPointer**		☐	☒	☐
GONZÁLEZ GONZÁLEZ	**SANTIAGO**	**CNPIC**		☐	☒	☐
HERRERO PÉREZ	**LUIS**	**MINISTERIO DE DEFENSA**		☐	☒	☐
				☐	☐	☐
				☐	☐	☐
Doble clic aquí						

***Deberá adjuntarse *currículum vitae* de los profesores externos**

7.3. Recursos Humanos: apoyo administrativo o técnico previsto [máx. 500 caracteres u 8 líneas]

El apoyo administrativo será ofrecido por el ICFS y el técnico por la EPS de la UAM

8. RECURSOS MATERIALES Y SERVICIOS

8.1 Justificación de la adecuación de los medios materiales y servicios disponibles para el Título en el Centro previsto como lugar de impartición [máx. 1000 caracteres o 15 líneas]

El máster contará con aula en la Escuela Politécnica Superior. La Secretaría administrativa se encuentra en un espacio compartido del Instituto de Ciencias Forenses y de la Seguridad en el edificio C de la Escuela Politécnica Superior de la UAM.
Teléfonos:

Dirección: Ciudad Universitaria de Cantoblanco
C/ Francisco Tomás y Valiente, Escuela Politécnica Superior
28049 MADRID
Secretaría Administrativa: 91 497 6135
Correo electrónico: araceli.bailon@inv.uam.es
Página web: www.icfs.es

8.2 Previsión de adquisición de los recursos materiales y servicios necesarios con cargo al presupuesto del título [máx. 1000 caracteres o 15 líneas].

Aula para 30 alumnos. No es necesario laboratorio, puesto que se va a requerir a los alumnos que traigan su portátil.

9. RESULTADOS PREVISTOS

Valores cuantitativos estimados para los indicadores y su justificación.

TASA DE GRADUACIÓN	**94 %**
TASA DE ABANDONO	**4 %**
TASA DE EFICIENCIA	**96 %**

Justificación de las estimaciones realizadas.

Se han realizado en base a otros programas parecidos que gestiona el ICFS.

10. SISTEMA DE GARANTÍA DE CALIDAD DEL TÍTULO

Este título está sometido al Sistema de Garantía Interna de la Calidad (SGIC) de los títulos propios de la UAM

11. CALENDARIO DE IMPLANTACIÓN

11.1 Cronograma de implantación de la titulación (por semanas)

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

SEMANA Núm. 1

	Nº asignatura	Tema/s	Horario	Profesor/es
L				
M				
X				
J				
V	1	Fundamentos red team y blue team	15.30 a 20.00 (30min. de descanso)	Álvaro Ortigosa
S	1	Fundamentos red team y blue team	9.30 a 14.00 (30min. de descanso)	Álvaro Ortigosa

SEMANA Núm. 2

	Nº asignatura	Tema/s	Horario	Profesor/es
L				
M				
X				
J				
V	1	Fundamentos red team y blue team	15.30 a 20.00 (30min. de descanso)	F. Damián Ruiz Soriano
S	1	Fundamentos red team y blue team	9.30 a 14.00 (30min. de descanso)	F. Damián Ruiz Soriano

SEMANA Núm. 3

	Nº asignatura	Tema/s	Horario	Profesor/es
L				

M				
X				
J				
V	2	Reconocimiento de vectores de entrada y acceso	15.30 a 20.00 (30min. de descanso)	Álvaro Ortigosa
S	2	Reconocimiento de vectores de entrada y acceso	9.30 a 14.00 (30min. de descanso)	Eduardo Arriols

SEMANA Núm. 4

	Nº asig-natura	**Tema/s**	**Horario**	**Profesor/es**
L				
M				
X				
J				
V	3	Extracción de artefactos forenses y caracterización de malware en sistemas operativos windows	15.30 a 20.00 (30min. de descanso)	Mario Guerra Soto
S	3	Extracción de artefactos forenses y caracterización de malware en sistemas operativos windows	9.30 a 14.00 (30min. de descanso)	Mario Guerra Soto

SEMANA Núm. 5

	Nº asig-natura	**Tema/s**	**Horario**	**Profesor/es**
L				
M				
X				
J				

V	3	Extracción de artefactos forenses y caracterización de malware en sistemas operativos windows	15.30 a 20.00 (30min. de descanso)	Mario Guerra Soto
S	3	Extracción de artefactos forenses y caracterización de malware en sistemas operativos windows	9.30 a 14.00 (30min. de descanso)	Mario Guerra Soto
SEMANA Núm. 6				
	Nº asig-natura	**Tema/s**	**Horario**	**Profesor/es**
L				
M				
X				
J				
V	4	Ciberinteligencia de la amenaza	15.30 a 20.00 (30min. de descanso)	Mario Guerra Soto
S	4	Ciberinteligencia de la amenaza	9.30 a 14.00 (30min. de descanso)	Mario Guerra Soto
SEMANA Núm. 7				
	Nº asig-natura	**Tema/s**	**Horario**	**Profesor/es**
L				
M				
X				
J				
V	5	Arquitectura de detección SIEM	15.30 a 20.00 (30min. de descanso)	Maite Moreno

S	5	Arquitectura de detección SIEM	9.30 a 14.00 (30min. de descanso)	Maite Moreno
SEMANA Núm. 8				
	Nº asig-natura	**Tema/s**	**Horario**	**Profesor/es**
L				
M				
X				
J				
V	6	Modelado de casos de uso, reglas de correlación y alertas en SIEM	15.30 a 20.00 (30min. de descanso)	Marta López Pardal
S	6	Modelado de casos de uso, reglas de correlación y alertas en SIEM	9.30 a 14.00 (30min. de descanso)	Marta López Pardal
SEMANA Núm. 9				
	Nº asig-natura	**Tema/s**	**Horario**	**Profesor/es**
L				
M				
X				
J				
V	7	Pentesting de sistemas	15.30 a 20.00 (30min. de descanso)	Miguel Ángel Mora
S	7	Pentesting de sistemas	9.30 a 14.00 (30min. de descanso)	Roberto Latorre

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

SEMANA Núm. 10

	Nº asig-natura	Tema/s	Horario	Profesor/es
L				
M				
X				
J				
V	7	Pentesting de sistemas	15.30 a 20.00 (30min. de descanso)	Jorge López de Vergara
S	7	Pentesting de sistemas	9.30 a 14.00 (30min. de descanso)	Jorge López de Vergara

SEMANA Núm. 11

	Nº asig-natura	Tema/s	Horario	Profesor/es
L				
M				
X				
J				
V	7	Pentesting de sistemas	15.30 a 20.00 (30min. de descanso)	Luis Herrero
S	7	Pentesting de sistemas	9.30 a 14.00 (30min. de descanso)	Luis Herrero

SEMANA Núm. 12

	Nº asig-natura	Tema/s	Horario	Profesor/es
L				
M				

X				
J				
V	8	Pentesting Web	15.30 a 20.00 (30min. de descanso)	Ramón Fuentes
S	8	Pentesting Web	9.30 a 14.00 (30min. de descanso)	Ramón Fuentes

SEMANA Núm. 13

	Nº asig-natura	**Tema/s**	**Horario**	**Profesor/es**
L				
M				
X				
J				
V	9	Pentesting wifi y redes inalámbricas	15.30 a 20.00 (30min. de descanso)	Jorge López de Vergara
S	9	Pentesting wifi y redes inalámbricas	9.30 a 14.00 (30min. de descanso)	Jorge López de Vergara

SEMANA Núm. 14

	Nº asig-natura	**Tema/s**	**Horario**	**Profesor/es**
L				
M				
X				
J				
V	10	Pentesting de sistemas industriales	15.30 a 20.00	Martina Matari

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

			(30min. de descanso)	
S	10	Pentesting de sistemas industriales	9.30 a 14.00 (30min. de descanso)	Santiago González

SEMANA Núm. 15

	Nº asig-natura	**Tema/s**	**Horario**	**Profesor/es**
L				
M				
X				
J				
V	11	Fuzzing. Exploiting	15.30 a 20.00 (30min. de descanso)	Sandra Bardón
S	11	Fuzzing. Exploiting	9.30 a 14.00 (30min. de descanso)	Sandra Bardón

SEMANA Núm. 16

	Nº asig-natura	**Tema/s**	**Horario**	**Profesor/es**
L				
M				
X				
J				
V	11	Fuzzing. Exploiting	15.30 a 20.00 (30min. de descanso)	Sandra Bardón
S	11	Fuzzing. Exploiting	9.30 a 14.00 (30min. de descanso)	Sandra Bardón

CENTRO DE FORMACIÓN CONTINUA

PROPUESTA ACADÉMICA DE NUEVA CREACIÓN DE TÍTULO PROPIO

SEMANA Núm. 17

	Nº asignatura	Tema/s	Horario	Profesor/es
L				
M				
X				
J				
V	12	Análisis de alertas y threat hunting	15.30 a 20.00 (30min. de descanso)	Mario Guerra Soto
S	12	Análisis de alertas y threat hunting	9.30 a 14.00 (30min. de descanso)	Álvaro Ortigosa

SEMANA Núm. 18

	Nº asignatura	Tema/s	Horario	Profesor/es
L				
M				
X				
J				
V	13	Esquema de respuestas y playbook	15.30 a 20.00 (30min. de descanso)	Marta López Pardal
S	13	Esquema de respuestas y playbook	9.30 a 14.00 (30min. de descanso)	Marta López Pardal

SEMANA Núm. 19

	Nº asignatura	Tema/s	Horario	Profesor/es
L				

M				
X				
J				
V	14	Preparación OSCP	15.30 a 20.00 (30min. de descanso)	Óscar Maqueda Hortells
S	14	Preparación OSCP	9.30 a 14.00 (30min. de descanso)	Óscar Maqueda Hortells

SEMANA Núm. 20

	Nº asig-natura	**Tema/s**	**Horario**	**Profesor/es**
L				
M				
X				
J				
V	15	Bitácoras e informes técnicos y ejecutivos. Cuadros de mandos de detección	15.30 a 20.00 (30min. de descanso)	Ramón Fuentes
S	15	Bitácoras e informes técnicos y ejecutivos. Cuadros de mandos de detección	9.30 a 14.00 (30min. de descanso)	Ramón Fuentes
		«Doble clic aquí para añadir semana»		

12. OBSERVACIONES

Como es semipresencial, se ha puesto en el calendario de implantación de cada asignatura sólo las semana que hay docencia presencial.

Las herramientas que se van a usar en la parte on line, son Moodle (se implantarán foros de participación y tutorías on line, además de subir material para el estudio de los alumnos), Adobe Connet de la UAM, a través del cual grabaremos clases de los profesores, las cuales se colgarán en moodle y algunas se retransmitirán en streaming.
Ya estamos en contacto con la UTED para su valoración.

Justificación de la necesidad de uso de plataforma comercial: Una de las premisas fundamentales de los estudios que se están proponiendo es ofrecer a los estudiantes conocimientos teóricos y prácticos sobre los temas avanzados en ciberseguridad. De esta forma, al finalizar estarán en condiciones de poner en práctica de forma inmediata los conocimientos adquiridos en un entorno profesional.

Uno de los principales inconvenientes para alcanzar este objetivo es la dificultad de ofrecer experiencias realistas para ejercitar, y posteriormente evaluar, las habilidades prácticas. En el fondo, estamos hablando de que los estudiantes deberían atacar un sistema real en busca de vulnerabilidades, o experimentar con un sistema real para ver si son capaces de evitar/detener los ataques de cibercriminales reales.

Debido a que esto no es posible por motivos legales, técnicos y éticos, se deben buscar alternativas que permitan la práctica y evaluación de estas habilidades técnicas prácticas en situaciones lo más parecidas posibles al entorno de trabajo real. El mejor enfoque conocido para superar esta dificultad es el uso de plataformas digitales de simulación, las cuales son capaces de reproducir y simular las condiciones, propiedades y características de una red de ordenadores y los dispositivos conectados a ella. Dentro de este entorno, los estudiantes pueden conectarse a dispositivos (ordenadores, servidores, routers e incluso teléfonos móviles) simulados y poner en práctica el conocimiento adquirido, ya sea para securizar los sistemas, buscar vulnerabilidades o realizar actividades de respuesta a incidentes y análisis forense.

De esta forma, los estudiantes podrán interactuar con el entorno virtual con muy pocas diferencias respecto a cómo lo harían en situaciones del mundo real. De hecho, desde un punto de vista técnico, estas plataformas digitales son prácticamente indistinguibles de una infraestructura real de ordenadores interconectados.

Existen diversas alternativas en el mercado para utilizar algunas de estas plataformas para la enseñanza de habilidades de seguridad informática. Durante el último año el cuerpo docente de esta propuesta de título propio estuvo investigando las alternativas disponibles y en este momento la elección se reduce a 2 opciones: la plataforma provista por la empresa iHacklab (https://www.ihacklabs.com/) y la plataforma utilizada por el Mando Conjunto de Ciberdefensa, con quien se espera poder hablar una vez pasada la situación de emergencia.

Respecto de las alternativas gratuitas, la plataforma que podría ser más apropiada, aunque con limitaciones, es TryHackMe (https://tryhackme.com/). El principal problema de esta plataforma es que ofrece menos soporte en general, y no contempla toda la

gama de actividades que incluyen las plataformas comerciales. Aunque no se descarta en el futuro desarrollar una infraestructura propia de la máster basada en esta plataforma gratuita, hemos considerado que sería demasiado arriesgado para este primer año, un año que necesariamente será de ajustes y solucionar situaciones imprevistas.

Por todo ello es que el presupuesto del máster contempla la necesidad de adquirir una de estas plataformas comerciales. Respecto de las cantidades estimadas, se ha optado por incluir la oferta comercial de iHacklab, por ser la única disponible en el momento de elaborar el presupuesto, pero se estima que en el caso de optar por la segunda plataforma no habrá grandes cambios.

PRESUPUESTO ECONÓMICO PARA TÍTULOS PROPIOS

Denominación del título	MÁSTER EN CIBERSEGURIDAD. RED TEAM - BLUE TEAM				
Periodo de impartición	Inicio:	02/10/2020	Final:	30/12/2021	Número de Edición: 1

INGRESOS PREVISTOS / INGRESOS REALIZADOS

1. Tasas.

P.V.P. MATRÍCULA	PLAZAS DE PAGO	Nº BECAS (min 10%)	PLAZAS TOTALES	PRESUPUESTADO	PLAZAS CUBIERTAS	Nº BECAS concedidas	EJECUTADO
9.000 €	19	4	23	171.000 €	0	0	0 €
					0	0	0 €

2. Subvenciones, donaciones y otros ingresos.

NOMBRE ENTIDAD		PRESUPUESTADO		EJECUTADO
	.....	0 €		0 €
	.....	0 €		0 €
	.....	0 €		0 €
TOTAL Euros.....	.....	0 €		0 €

3. Remanente ediciones anteriores

DESCRIPCIÓN		PRESUPUESTADO		EJECUTADO
	.....			
	.....	0 €		0 €
	.....	0 €		0 €
TOTAL Euros.....		0 €		0 €

4. TOTAL INGRESOS	PRESUPUESTADO		EJECUTADO
TOTAL Euros (=total 1+...+total 3)	171.000 €		0 €

GASTOS PREVISTOS / GASTOS EJECUTADOS

1. CANON INSTITUCIONAL UAM (15% de los Ingresos totales)	25.650 €		0 €

2. DIRECCIÓN Y COORDINACIÓN ACADÉMICAS (incluidas retenciones art. 83 LOU e IRPF)

APELLIDOS	NOMBRE	CARGO	PRESU-PUESTADO		EJECUTADO
			1.500 €		0 €
			1.500 €		0 €
			1.000 €		
			1.000 €		0 €
			1.000 €		
TOTAL Euros.....			6.000 €		0 €

3. PROFESORADO UAM (incluidas retenciónes art. 83 LOU e IRPF) *

*** La docencia presencial se retribuirá por horas. Si el título tiene carácter semipresencial, la docencia *on line* se retribuirá por créditos. El resto de actividades docentes se retribuirá, con carácter general, por unidades (ej. nº trabajos dirigidos).**

3.1. Docencia Presencial (profs. UAM)

APELLIDOS	NOMBRE	HORAS	€/ HORA	PRESUPUESTADO	HORAS REALIZADAS	€/ HORA APLICADO	EJECUTADO
		16	75 €	1.200 €	0	0 €	0 €
		8	75 €	600 €	0	0 €	0 €
		4	75 €	300 €			
		8	75 €	600 €			
		4	75 €	300 €	0	0 €	0 €
TOTALES.....		40		3.000 €	0		0 €

3.2. Dirección Trabajos Fin de Título (profs. UAM)

APELLIDOS	NOMBRE	TRABAJOS	€ / TRABAJO	PRESUPUESTADO	TRABAJOS DIRIGIDOS	€/TRABAJO APLICADO	EJECUTADO
		4	100 €	400 €	0	0 €	0 €
		4	100 €	400 €	0	0 €	0 €
		4	100 €	400 €	0	0 €	0 €
TOTAL Euros.....		12		1.200 €	0		0 €

3.3. Tutorías Practicum (profs. UAM)

APELLIDOS	NOMBRE	ALUMNOS	€/ALUMNO	PRESUPUESTADO	ALUMNOS ATENDIDOS	€/ALUMNO APLICADO	EJECUTADO
		0	0 €	0 €	0 €	0 €	0 €
		0	0 €	0 €	0 €	0 €	0 €
		0	0 €	0 €	0 €	0 €	0 €
TOTAL Euros.....		0		0 €	0 €		0 €

3.4. Docencia *on line* (profs. UAM) *

*** Sólo se preverán pagos por docencia *on line* en caso de títulos de carácter "semipresencial"**

APELLIDOS	NOMBRE	CRÉDITOS	€/CRÉDITO	PRESU-PUESTADO	CRÉDITOS	€/CRÉDITO	EJECUTADO

APELLIDOS	NOMBRE	CRÉDITOS	€/CRÉDITO	PRESU-PUESTADO	CRÉDITOS IMPARTIDOS	€/CRÉDITO APLICADO	EJECUTADO
		2,5	600 €	1.500 €	0 €	0 €	0 €
		1	600 €	600 €	0 €	0 €	0 €
		1	600 €	600 €			
		2	600 €	1.200 €			
		1	600 €	600 €			
L.O.U.				270 €			
					0 €	0 €	0 €
TOTAL Euros.....		**7,5**		**4.770 €**	**0 €**		**0 €**

3.5. Otras actividades o colaboraciones docentes (profs. UAM) *

*** Indíquese el concepto**

APELLIDOS	NOMBRE	CONCEPTO	PRESU-PUESTADO		EJECUTADO
		Tribunal defensa TFM	500 €		0 €
			0 €		0 €
			0 €		0 €
TOTAL Euros.....			**500 €**		**0 €**

4. PROFESORADO EXTERNO (incluida retención IRPF)

4.1. Docencia Presencial (profs. EXTERNOS)

APELLIDOS	NOMBRE	HORAS	€/ HORA	PRESUPUESTADO	HORAS REALIZADAS	€/ HORA APLICADO	EJECUTADO
		8	75	600 €	0 €	0 €	0 €
		8	75	600 €	0 €	0 €	0 €
		28	75	2.100 €	0 €	0 €	0 €
		16	75	1.200 €	0 €	0 €	0 €
		16	75	1.200 €	0 €	0 €	0 €
		8	75	600 €	0 €	0 €	0 €
		16	75	1.200 €	0 €	0 €	0 €
		4	75	300 €	0 €	0 €	0 €
		4	75	300 €	0 €	0 €	0 €
		4	75	300 €	0 €	0 €	0 €
		8	75	600 €	0 €	0 €	0 €
TOTAL Euros.....		**120**	**75**	**600 €**	**0 €**		**0 €**

4.2. Dirección Trabajos Fin de Título (profs. EXTERNO)

APELLIDOS	NOMBRE	TRABAJOS	€ / TRABAJO	PRESUPUESTADO	TRABAJOS DIRIGIDOS	€/TRABAJO APLICADO	EJECUTADO
		1	150 €	150 €	0	0 €	0 €
		5	150 €	750 €	0	0 €	0 €
		4	150 €	600 €			
		4	150 €	600 €			
		1	150 €	150 €			
		2	150 €	300 €	0	0 €	0 €
TOTAL Euros.....		**17**		**2.550 €**	**0**		**0 €**

4.3. Tutorías Practicum (profs. EXTERNOS)

APELLIDOS	NOMBRE	ALUMNOS	€/ALUMNO	PRESUPUESTADO	ALUMNOS ATENDIDOS	€/ALUMNO APLICADO	EJECUTADO
		0	0	0 €	0 €	0 €	0 €
		0	0	0 €	0 €	0 €	0 €
		0	0	0 €	0 €	0 €	0 €
TOTAL Euros.....		**0**	**0**	**0 €**	**0 €**		**0 €**

4.4. Docencia *on line* (profs. EXTERNOS) *

*** Sólo se preverán pagos por docencia *on line* en caso de títulos de carácter "semipresencial"**

APELLIDOS	NOMBRE	CRÉDITOS	€/CRÉDITO	PRESU-PUESTADO	CRÉDITOS IMPARTIDOS	€/CRÉDITO APLICADO	EJECUTADO
		0,5	600 €	300 €	0 €	0 €	0 €
		2	600 €	1.200 €	0 €	0 €	0 €
		7	600 €	4.200 €			
		4	600 €	2.400 €			
		4	600 €	2.400 €			
		2	600 €	1.200 €			
		4	600 €	2.400 €			
		1	600 €	600 €			
		1	600 €	600 €			
		1	600 €	600 €			
		3	600 €	1.800 €	0 €	0 €	0 €
TOTAL Euros.....		**29,5**		**17.700 €**	**0 €**		**0 €**

4.5. Otras actividades o colaboraciones docentes (profs. EXTERNOS) *

*** Indíquese el concepto**

APELLIDOS	NOMBRE	CONCEPTO	PRESUPUESTADO		EJECUTADO
		Tribunal defensa TFM	500 €		0 €
		Tribunal defensa TFM	500 €		0 €
		Tribunal defensa TFM	500 €		0 €
TOTAL Euros.....			**1.500 €**		**0 €**

5. PERSONAL ADMINISTRATIVO UAM (incluida retención IRPF)

APELLIDOS	NOMBRE	CONCEPTO	PRESUPUESTADO		EJECUTADO
			0 €		0 €
			0 €		0 €
			0 €		0 €
TOTAL Euros.....			**0 €**		**0 €**

6. PERSONAL ADMINISTRATIVO EXTERNO (incluida retención IRPF)

APELLIDOS	NOMBRE	CONCEPTO	PRESUPUESTADO		EJECUTADO
PERSONAL ICFS			40.000 €		0 €
			0 €		0 €
			0 €		0 €
TOTAL Euros.....			**40.000 €**		**0 €**

7. MATERIAL INVENTARIABLE

DESCRIPCIÓN		PRESUPUESTADO		EJECUTADO
		0 €		0 €
		0 €		0 €
		0 €		0 €
TOTAL Euros.....		**0 €**		**0 €**

8. GESTIÓN ECONÓMICA FUAM (6%)

	8.721 €			**0 €**

9. GASTOS VARIOS

DESCRIPCIÓN		PRESUPUESTADO		EJECUTADO
9.1 Tasa por Expedición de Título		4.025 €		0 €
9.2 Seguro de Accidente		276 €		0 €
9.3 Viajes y Dietas		0 €		0 €
9.4 Publicidad y Difusión		2.000 €		0 €
9.5 PLATAFORMA HICK LABS		32.200 €		
9.6 Pasgo gestión servicios técnicos laboratorios EPS		3.000 €		
9.6 GESTIÓN ICFS		17.100 €		0 €
TOTAL Euros.....		**58.601 €**		**0 €**

10. TOTAL GASTOS	PRESUPUESTADO		EJECUTADO
TOTAL Euros (=total 1 +…+ total 9)	**170.792 €**		**0 €**

38,21

BALANCE FINAL

	PREVISTO				EJECUTADO		
	INGRESOS (A)		**GASTOS (B)**		**INGRESOS (A)**		**GASTOS (B)**
	171.000 €		**170.792 €**		**0 €**		**0 €**
BALANCE (A-B)		**208 €**				**0 €**	

OBSERVACIONES

9.5 Se pretende utilizar esta plataforma por las razones expuestas en la memoria. El precio que nos han ofrecido es de 1400€ por alumno, de ahí la cantidad resultante.

PRESUPUESTO ECONÓMICO PARA TÍTULOS PROPIOS

Denominación del título	MÁSTER EN CIBERSEGURIDAD. RED TEAM - BLUE TEAM				
Periodo de impartición	Inicio:	#########	Final:	#########	Número de Edición: 1

INGRESOS PREVISTOS					INGRESOS REALIZADOS		
1. Tasas.							
P.V.P. MATRÍCULA	PLAZAS DE PAGO	Nº BECAS (min 10%)	PLAZAS TOTALES	PRESUPUESTADO	PLAZAS CUBIERTAS	Nº BECAS concedidas	EJECUTADO
9.000 €	19	4	23	171.000 €	0	0	0 €
					0	0	0 €

2. Subvenciones, donaciones y otros ingresos.

NOMBRE ENTIDAD		PRESUPUESTADO		EJECUTADO
	.....	0 €		0 €
	.....	0 €		0 €
	.....	0 €		0 €
TOTAL Euros.....	.....	0 €		0 €

3. Remanente ediciones anteriores

DESCRIPCIÓN		PRESUPUESTADO		EJECUTADO
	.....			
	.....	0 €		0 €
	.....	0 €		0 €
TOTAL Euros.....		0 €		0 €

4. TOTAL INGRESOS	PRESUPUESTADO		EJECUTADO
TOTAL Euros (=total 1+...+total 3)	171.000 €		0 €

GASTOS PREVISTOS		GASTOS EJECUTADOS	
1. CANON INSTITUCIONAL UAM (15% de los Ingresos totales)	25.650 €		0 €

2. DIRECCIÓN Y COORDINACIÓN ACADÉMICAS (incluidas retenciones art. 83 LOU e IRPF)

APELLIDOS	NOMBRE	CARGO	PRESU-PUESTADO		EJECUTADO
ORTIGOSA	ÁLVARO	DIRECTOR	1.500 €		0 €
MAQUEDA	ÓSCAR	CODIRECTOR	1.500 €		0 €
FUENTES	RAMÓN	CODIRECTOR	1.000 €		
GUERRA SOTO	MARIO	CODIRECTOR	1.000 €		0 €
LÓPEZ DE VERGARA	JORGE	SUBDIRECTOR	1.000 €		
TOTAL Euros.....			6.000 €		0 €

3. PROFESORADO UAM (incluidas retenciónes art. 83 LOU e IRPF) *

*** La docencia presencial se retribuirá por horas. Si el título tiene carácter semipresencial, la docencia *on line* se retribuirá por créditos. El resto de actividades docentes se retribuirá, con carácter general, por unidades (ej. nº trabajos dirigidos).**

3.1. Docencia Presencial (profs. UAM)

APELLIDOS	NOMBRE	HORAS	€/ HORA	PRESUPUESTADO	HORAS REALIZADAS	€/ HORA APLICADO	EJECUTADO
Ortigosa Juárez	Álvaro	16	75 €	1.200 €	0	0 €	0 €
Lopez de Vergara	Jorge	8	75 €	600 €	0	0 €	0 €
Mora Rincón	Miguel Ángel	4	75 €	300 €			
Andrés Sáez	Juan Antonio	8	75 €	600 €			
Latorre Camino	Roberto	4	75 €	300 €	0	0 €	0 €
TOTALES.....		40		3.000 €	0		0 €

3.2. Dirección Trabajos Fin de Título (profs. UAM)

APELLIDOS	NOMBRE	TRABAJOS	€ / TRABAJO	PRESUPUESTADO	TRABAJOS DIRIGIDOS	€/TRABAJO APLICADO	EJECUTADO
Ortigosa Juárez	Alvaro	4	100 €	400 €	0	0 €	0 €
López Vergara	Jorge	4	100 €	400 €	0	0 €	0 €
Latorre Camino	Roberto	4	100 €	400 €	0	0 €	0 €
TOTAL Euros.....		12		1.200 €	0		0 €

3.3. Tutorías Practicum (profs. UAM)

APELLIDOS	NOMBRE	ALUMNOS	€/ALUMNO	PRESUPUESTADO	ALUMNOS ATENDIDOS	€/ALUMNO APLICADO	EJECUTADO
		0	0 €	0 €	0 €	0 €	0 €
		0	0 €	0 €	0 €	0 €	0 €
		0	0 €	0 €	0 €	0 €	0 €

TOTAL Euros.....		**0**		**0 €**	**0 €**		**0 €**

3.4. Docencia *on line* (profs. UAM) *

*** Sólo se preverán pagos por docencia *on line* en caso de títulos de carácter "semipresencial"**

APELLIDOS	NOMBRE	CRÉDITOS	€/CRÉDITO	PRESU-PUESTADO	CRÉDITOS IMPARTIDOS	€/CRÉDITO APLICADO	EJECUTADO
Ortigosa	Álvaro	2,5	600 €	1.500 €	0 €	0 €	0 €
López de Vergara	Jorge	1	600 €	600 €	0 €	0 €	0 €
Latorre Camino	Roberto	1	600 €	600 €			
Andrés Sáez	Juan Antonio	2	600 €	1.200 €			
Mora Rincón	Miguel Ángel	1	600 €	600 €			
L.O.U.				270 €			
					0 €	0 €	0 €
TOTAL Euros.....		**7,5**		**4.770 €**	**0 €**		**0 €**

3.5. Otras actividades o colaboraciones docentes (profs. UAM) *

*** Indíquese el concepto**

APELLIDOS	NOMBRE	CONCEPTO	PRESU-PUESTADO		EJECUTADO
Ortigosa	Álvaro	Tribunal defensa TFM	500 €		0 €
			0 €		0 €
			0 €		0 €
TOTAL Euros.....			**500 €**		**0 €**

4. PROFESORADO EXTERNO (incluida retención IRPF)

4.1. Docencia Presencial (profs. EXTERNOS)

APELLIDOS	NOMBRE	HORAS	€/ HORA	PRESUPUESTADO	HORAS REALIZADAS	€/ HORA APLICADO	EJECUTADO
Ruiz Soriano	Francisco Damia	8	75	600 €	0 €	0 €	0 €
Maqueda Hortells	Óscar	8	75	600 €	0 €	0 €	0 €
Guerra Soto	Mario	28	75	2.100 €	0 €	0 €	0 €
Fuentes Requena	Ramón	16	75	1.200 €	0 €	0 €	0 €
Bardón Moral	Sandra	16	75	1.200 €	0 €	0 €	0 €
Moreno García	Maite	8	75	600 €	0 €	0 €	0 €
López Pardal	Marta	16	75	1.200 €	0 €	0 €	0 €
Matarí González	Martina	4	75	300 €	0 €	0 €	0 €
Arriols Nuñez	Eduardo	4	75	300 €	0 €	0 €	0 €
González González	Santiago	4	75	300 €	0 €	0 €	0 €
Herrero Pérez	Luis	8	75	600 €	0 €	0 €	0 €
TOTAL Euros.....		**120**	**75**	**600 €**	**0 €**		**0 €**

4.2. Dirección Trabajos Fin de Título (profs. EXTERNO)

APELLIDOS	NOMBRE	TRABAJOS	€ / TRABAJO	PRESUPUESTADO	TRABAJOS DIRIGIDOS	€/TRABAJO APLICADO	EJECUTADO
Ruiz Soriano	Francisco Damia	1	150 €	150 €	0	0 €	0 €
Maqueda Hortells	Óscar	5	150 €	750 €	0	0 €	0 €
Guerra Soto	Mario	4	150 €	600 €			
Fuentes Requena	Ramón	4	150 €	600 €			
Bardón Moral	Sandra	1	150 €	150 €			
Herrero Pérez	Luis	2	150 €	300 €	0	0 €	0 €
TOTAL Euros.....		**17**		**2.550 €**	**0**		**0 €**

4.3. Tutorías Practicum (profs. EXTERNOS)

APELLIDOS	NOMBRE	ALUMNOS	€/ALUMNO	PRESUPUESTADO	ALUMNOS ATENDIDOS	€/ALUMNO APLICADO	EJECUTADO
		0	0	0 €	0 €	0 €	0 €
		0	0	0 €	0 €	0 €	0 €
		0	0	0 €	0 €	0 €	0 €
TOTAL Euros.....		**0**	**0**	**0 €**	**0 €**		**0 €**

4.4. Docencia *on line* (profs. EXTERNOS) *

*** Sólo se preverán pagos por docencia *on line* en caso de títulos de carácter "semipresencial"**

APELLIDOS	NOMBRE	CRÉDITOS	€/CRÉDITO	PRESU-PUESTADO	CRÉDITOS IMPARTIDOS	€/CRÉDITO APLICADO	EJECUTADO
Ruiz Soriano	Francisco Damia	0,5	600 €	300 €	0 €	0 €	0 €
Maqueda Hortells	Óscar	2	600 €	1.200 €	0 €	0 €	0 €
Guerra Soto	Mario	7	600 €	4.200 €			
Fuentes Requena	Ramón	4	600 €	2.400 €			
Bardón Moral	Sandra	4	600 €	2.400 €			
Moreno García	Maite	2	600 €	1.200 €			
López Pardal	Marta	4	600 €	2.400 €			
Matarí González	Martina	1	600 €	600 €			
Arriols Nuñez	Eduardo	1	600 €	600 €			
González González	Santiago	1	600 €	600 €			
Herrero Pérez	Luis	3	600 €	1.800 €	0 €	0 €	0 €

TOTAL Euros.....	**29,5**		**17.700 €**	**0 €**		**0 €**

4.5. Otras actividades o colaboraciones docentes (profs. EXTERNOS) *

*** Indíquese el concepto**

APELLIDOS	NOMBRE	CONCEPTO	PRESUPUESTADO		EJECUTADO
Maqueda Hortells	Óscar	Tribunal defensa TFM	500 €		0 €
Guerra Soto	Mario	Tribunal defensa TFM	500 €		0 €
Fuentes	Ramón	Tribunal defensa TFM	500 €		0 €
TOTAL Euros.....			**1.500 €**		**0 €**

5. PERSONAL ADMINISTRATIVO UAM (incluida retención IRPF)

APELLIDOS	NOMBRE	CONCEPTO	PRESUPUESTADO		EJECUTADO
			0 €		0 €
			0 €		0 €
			0 €		0 €
TOTAL Euros.....			**0 €**		**0 €**

6. PERSONAL ADMINISTRATIVO EXTERNO (incluida retención IRPF)

APELLIDOS	NOMBRE	CONCEPTO	PRESUPUESTADO		EJECUTADO
PERSONAL ICFS			40.000 €		0 €
			0 €		0 €
			0 €		0 €
TOTAL Euros.....			**40.000 €**		**0 €**

7. MATERIAL INVENTARIABLE

DESCRIPCIÓN		PRESUPUESTADO		EJECUTADO
		0 €		0 €
		0 €		0 €
		0 €		0 €
TOTAL Euros.....		**0 €**		**0 €**

8. GESTIÓN ECONÓMICA FUAM (6%)

		8.721 €		**0 €**

9. GASTOS VARIOS

DESCRIPCIÓN		PRESUPUESTADO		EJECUTADO
9.1 Tasa por Expedición de Título		4.025 €		0 €
9.2 Seguro de Accidente		276 €		0 €
9.3 Viajes y Dietas		0 €		0 €
9.4 Publicidad y Difusión		2.000 €		0 €
9.5 PLATAFORMA HICK LABS		32.200 €		
9.6 Pasgo gestión servicios técnicos laboratorios EPS		3.000 €		
9.6 GESTIÓN ICFS		17.100 €		0 €
TOTAL Euros.....		**58.601 €**		**0 €**

10. TOTAL GASTOS	PRESUPUESTADO		EJECUTADO
TOTAL Euros (=total 1 +…+ total 9)	**170.792 €**		**0 €**

38,21

BALANCE FINAL

	PREVISTO				EJECUTADO		
	INGRESOS (A)		**GASTOS (B)**		**INGRESOS (A)**		**GASTOS (B)**
	171.000 €		**170.792 €**		**0 €**		**0 €**
BALANCE (A-B)		**208 €**				**0 €**	

OBSERVACIONES

9.5 Se pretende utilizar esta plataforma por las razones expuestas en la memoria. El precio que nos han ofrecido es de 1400€ por alumno, de ahí la cantidad resultante.