Instituto de
Ciencias Forenses y de la Seguridad

Universidad Autónoma de Madrid

MÁSTER EN CIBERSEGURIDAD. RED TEAM – BLUE TEAM

ICFS Instituto de Ciencias Forenses y de la Seguridad ICFS

PRESENTACIÓN

En estos momentos en que 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 conocer la forma en que los atacantes pueden sacar partido de las vulnerabilidades, siendo de una importancia crítica la prevención de estos ataques.

Una gestión básica de la Ciberseguridad pivota sobre los ámbitos de Protección, Detección y Respuesta, enmarcados en un aseguramiento continuo que garantice el adecuado funcionamiento de las actividades que incluyen. Por ello, 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.

OBJETIVOS

En este máster se engloban los enfoques Red Team y BlueTeam 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, proporcionando todos los elementos conceptuales y prácticos para conseguir una mejora continua en Protección, Detección y Respuesta.

El alumno aprenderá tanto la vertiente defensiva como la ofensiva siendo capaz de entender los distintos métodos de ataque y defensa de las redes inalámbricas que cada vez tienen más presencia en nuestros vehículos, hogares, etc: 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.

DIRIGIDO A

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.

Si bien no es un requisito obligatorio tener formación técnica para matricularse, el contenido del máster no lo hace recomendable para personas que no tengan conocimientos previos relacionados con informática y, más específicamente, con seguridad informática. En este sentido queremos dejar claro que no es un máster de introducción a la ciberseguridad. Se verán los temas específicos de red teaming y blue teaming, asumiendo que los estudiantes tienen conocimientos o son capaces de autoformarse sobre temas tales como redes de información, programación/scripting, arquitectura de sistemas distribuidos, administración y uso del sistema operativo Linux, entre otros.

CRITERIOS GENERALES DE SELECCIÓN 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%)

CARACTERÍSTICAS DEL TÍTULO

GENERALES

- **Número de Créditos**: 70 ECTS
  - Asignaturas presenciales: 40 ECTS
  - Asignaturas no presenciales: 17 ECTS
  - Trabajo Final: 13 ECTS
- **Número de Plazas**: 30
- **Modalidad**: Semipresencial
- **Lugar de Impartición**: Escuela Politécnica Superior de la Universidad Autónoma de Madrid
- **Horario**: viernes 15.30 a 20.00 y sábados de 9.30 a 14.00
- **Duración**:
  - **Fecha de inicio**: octubre de 2020.
  - **Finalización**: diciembre de 2021.

PROGRAMA ACADÉMICO

Asignatura	ECTS	Tipo
Arquitecturas de detección de SIEM (Security Information and Event Management)	3	Obligatoria
Bitácoras e informes técnicos y ejecutivos. Cuadros de mandos de detección	3	Obligatoria
Ciberinteligencia de la amenazas	3	Obligatoria
Esquemas de respuesta y Playbooks	3	Obligatoria
Extracción de artefactos forenses y caracterización de malware en sistemas operativos Windows	6	Obligatoria
Fundamentos Red Team y Blue Team	3	Obligatoria
Fuzzing. Exploiting	6	Obligatoria
Gestión de alertas y threat hunting	3	Obligatoria
Modelado de casos de uso, reglas de correlación y alertas en SIEM	3	Obligatoria
Pentesting de sistemas	9	Obligatoria
Pentesting web	3	Obligatoria
Pentesting wifi y redes inalámbricas	3	Obligatoria
Pentesting de sistemas industriales	3	Obligatoria
Preparación Offensive Security Certified Professional (OSCP)	3	Obligatoria
Reconocimiento. vectores de entrada y acceso	3	Obligatoria
Trabajo Final de Máster	13	Obligatoria

TRABAJO FIN DE TÍTULO:

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, tanto desde el punto de vista ofensivo como defensivo.

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.

EQUIPO DOCENTE

- Álvaro Ortigosa. Director del Instituto de Ciencias Forenses y de la Seguridad.
- Jorge López de Vergara. Profesor EPS-UAM.
- Roberto Latorre. Profesor EPS-UAM
- Francisco Damián Ruiz Soriano. Singular Bank. Chief information Security Officer (CISO)
- Óscar Maqueda Hortells. Disruptive Consulting. S. L.
- Mario Guerra Soto. Ministerio de Defensa
- Ramon Fuentes Requena. Guardia Civil.
- Sandra Bardón. Ministerio de Defensa
- Maite Moreno. S2 Group.
- Marta López Pardal. Eleven Paths. Telefónica S. A.
- Martina Matari. Telefónica S. A.
- Eduardo Arriols. Co-foundador de RootPointer y profesor Universitario en U-tad.
- Santiago González. CNPIC.
- Miguel Ángel Mora. Profesor EPS-UAM.
- Luis Herrero Pérez. Ministerio de Defensa.

ORGANIZACIÓN

Dirección del título

- **Álvaro Ortigosa.** Director del Instituto de Ciencias Forenses y de la Seguridad. Profesor contratado doctor de la EPS-UAM.

Subdirección del título:

- **Jorge López de Vergara**. Profesor EPS-UAM.

Codirección del título:

- **Óscar Maqueda Hortells.** Empresa Disruptive Consulting.
- **Mario Guerra Soto.** Ministerio de Defensa
- **Ramón Fuentes Requena.** Ministerio del Interior.

Coordinación: Araceli Bailón ICFS (araceli.bailon@inv.uam.es)

SALIDAS PROFESIONALES

En un informe de la Unión Europea se cifraba en más de 1 millón de puestos de trabajo relacionados con la ciberseguridad que se habrían creado para el año 2020.

El World Economic Forum identifica la ciberseguridad como uno de los principales riesgos para la economía mundial y las áreas de seguridad de las grandes empresas alertan de que la oferta de trabajo es enorme y no hay suficientes profesionales capacitados. Ya el pasado año medios como El País se hacían eco de la falta de 350.000 posiciones en seguridad, para el año 2022 la demanda no habrá dejado de crecer.

Los perfiles técnicos requeridos son, entre otros:

- Analistas de ciberseguridad
- Pentester o hackers éticos
- Especialistas de respuesta a incidentes
- Consultor de Seguridad Informática.
- Gestor de protección de datos
- Administrador de seguridad de sistemas y redes

INSCRIPCIÓN Y MATRICULACIÓN

TASAS

El precio del curso es de 9.000€. En el precio está incluida la tasa de matriculación, la tasa por expedición del título y un seguro de accidentes.

Existe la posibilidad de realizar un pago fraccionado en tres plazos de 3.000€ cada uno (primer plazo en el momento de la matrícula; segundo plazo: diciembre 2020; tercer plazo: marzo 2020) [consultar].

INSCRIPCIÓN

Fechas de inscripción y matrícula Inscripciones abiertas a partir del 1 de abril de 2020.

Para inscribirse en el Máster, deberá seguir las instrucciones que facilitaremos en la web y aportar la documentación correspondiente.

Para poder proceder a la tramitación de los documentos de solicitud se requerirán los siguientes documentos:

- **Título (ambas caras) o Certificado del trámite para su obtención**. También podrán acceder aquellos estudiantes que se encuentren cursando el último año de estas titulaciones superiores (en este caso, será preceptivo un escrito por parte del alumno/a comprometiéndose a finalizar los estudios antes de la finalización del máster. Dicho escrito deberá contar con el visto bueno de la dirección del máster).

  ***Estudiantes extranjeros: Si sus documentos son extracomunitarios (de fuera de la Unión Europea) no olvide que deben estar debidamente legalizados y autentificados. Pinche aquí para descargar una guía para la legalización y autentificación de documentos.*

- **Fotocopia del Documento Nacional de Identidad por ambas caras** (Candidatos extranjeros: pasaporte o cualquier otro documento acreditativo de la identidad personal, oficial en el país de origen. En el caso de presentar una estancia en España superior a 3 meses, deberá adjuntar copia de su NIE).
- **Curriculum Vitae.**
- **Carta de motivación**

Es importante señalar que el programa posee un número de plazas limitado por lo que su asignación se efectuará por el orden de llegada de las solicitudes y el cumplimiento de los requisitos mínimos establecidos.

- El periodo de inscripción está previsto desde el 01/04/2020 hasta el 02/09/2020.
- El periodo de matriculación se inicia a partir de mayo de 2020 hasta el 02/09/2020. Para poder matricularse se debe abonar el primer plazo del Máster.
- El inicio de curso está previsto para el 04/09/2020.

BECAS

Los criterios de selección de becarios son:

1. Ser ganador de la NCL de organización conjunta del ICFS y Guardia Civil (100%)
2. Alumno y ex alumnos del ICFS (50%)
3. Ser personal de Policía Nacional, Guardia Civil, Policía Autonómica, Policía Municipal, o personal del Ministerio de Defensa (50%)
4. Estar desempleado (30%)
5. Situación socio-económica (25%)
6. 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.

INFORMACIÓN Y CONTACTO

Ante cualquier consulta, puede ponerse en contacto con nosotros:

- Email: araceli.bailon@inv.uam.es
- Teléfono: (+34) 91 497 42 68/ 61 35.
- Dirección: C/ Francisco Tomás y Valiente 11. 28049 Madrid (Edificio C- Escuela Politécnica Superior, despacho 308). Universidad Autónoma de Madrid. Carretera de Colmenar km 15.