

ACG275/11: Aprobación de la modificación sustancial del Máster Universitario en Ciberseguridad y Ciberinteligencia Internacional (Master In International Cybersecurity and Cyberintelligence) por la Universidad de Granada; Universidade Do Minho (Portugal); Università Degli Studi di Padova (Italia) y Vilnius University (Lituania).

- Aprobado en la sesión ordinaria de Consejo de Gobierno de 29 de abril de 2025



**SOLICITUD DE MODIFICACIÓN DEL MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD Y
CIBERINTELIGENCIA INTERNACIONAL / MASTER IN INTERNATIONAL CYBERSECURITY AND
CYBERINTELLIGENCE POR LA UNIVERSIDAD DE GRANADA; UNIVERSIDADE DO MINHO (PORTUGAL);
UNIVERSITÀ DEGLI STUDI DI PADOVA(ITALIA) Y VILNAUS UNIVERSITETAS-VILNIUS
UNIVERSITY(LITUANIA)**

DESCRIPCIÓN DE LA MODIFICACIÓN Y JUSTIFICACIÓN DE LA PROPUESTA

El plan de estudios del Máster corresponde a un título conjunto impartido en el seno de la Alianza Arqus, y en el que participan 4 universidades diferentes: Universidad de Granada (como coordinadora), Universidad de Vilna (Lituania), Universidad de Padua (Italia) y Universidad de Minho (Portugal). El plan de estudios fue aprobado en febrero de 2024 por parte de la Agencia de Calidad Lituaniana, siguiendo el European Approach. El inicio de impartición de dicho programa ha sido en septiembre de 2024.

En el marco de la evaluación de la calidad del programa se establece que se realizará la recogida de información por parte de los estudiantes sobre la calidad del mismo, con el fin de detectar posibles deficiencias en su ejecución o diseño. De este modo, durante el primer cuatrimestre (impartido en Padua), se ha realizado este proceso, habiéndose detectado una carencia relevante del programa que se explica a continuación y que motiva esta solicitud de modificación.

El diseño del programa está realizado de modo que en los tres primeros cuatrimestres existen 4 asignaturas obligatorias (de 6 créditos) y 6 créditos de optativas. En el caso del segundo y tercer cuatrimestre, la oferta de optativas es relativamente reducida. Así, en el segundo cuatrimestre el número de optativas a elegir es de una (de 6 créditos) de un total de 2 optativas. En el tercer cuatrimestre, el número de optativas a elegir es de dos (de 3 créditos) de un total de 3. El programa fue diseñado para que la oferta de optatividad fuera más elevada durante el primer cuatrimestre, aprovechando la existencia de otro máster en ciberseguridad impartido en Padua en inglés. De este modo, durante el primer cuatrimestre se ofertan un total de 7 asignaturas. Sin embargo, debido a que dichas asignaturas son de 6 créditos, en realidad los estudiantes solamente pueden elegir una de ellas. Esto hace que los estudiantes reclamen la posibilidad de poder elegir al menos dos asignaturas.

De este modo, en esta solicitud se solicita modificar el plan de estudios haciendo que **una de las asignaturas actualmente obligatoria se convierta en optativa**, haciendo que la obligatoriedad durante el primer cuatrimestre pase de 24 a 18 créditos, y la optatividad durante el mismo pase de 6 a 12 créditos. En concreto, la asignatura que se solicita pasar a optativa es la de: "Secure Software Development" (6 ECTS).

1. Descripción, objetivos formativos y justificación del título

[1.4-1.9] Universidades, centros, modalidades, créditos, idiomas y plazas

- Los **créditos del máster** se modifican de la siguiente forma:

Créditos Obligatorios	72 66
Créditos Optativos	18 24
Prácticas Externas	0



Créditos Complementos de Formación	0
Trabajo Fin de Máster	30
TOTAL CRÉDITOS ECTS	120

4. Planificación de las Enseñanzas

El plan de estudios se modifica del siguiente modo :

Descripción general del plan de estudios

El plan de estudios está estructurado en cuatro semestres, con un total de ~~42~~ **11** clases obligatorias y **4** ~~5~~ optativas a elegir entre 12. El plan de estudios consta de las siguientes clases obligatorias:

1. Fundamentals of cryptography (I semester, Padova) (6 ECTS)
2. Digital Forensics (I semester, Padova) (6 ECTS)
- ~~3. Secure software development (I semester, Padova) (6 ECTS))~~
4. Fundamentals on international cybersecurity (I semester, Minho) (6 ECTS)
5. Operating systems security (II semester, Vilnius) (6 ECTS)
6. Security of applications (II semester, Vilnius) (6 ECTS)
7. International management of cybersecurity (II semester, Vilnius) (6 ECTS)
8. Research projects (II semester, Vilnius) (6 ECTS)
9. Ethical hacking (III semester, Granada) (6 ECTS)
10. Cyberprotection systems (III semester, Granada) (6 ECTS)
11. Network security (III semester, Granada) (6 ECTS)
12. International cyberintelligence (III semester, Granada) (6 ECTS)

Los estudiantes elegirán entre las siguientes asignaturas optativas en el primer semestre (Universidad de Padua):

1. Mobile security (6 ECTS)
2. Cyberphysical and IoT security (6 ECTS)
3. Machine Learning techniques for event correlation (6 ECTS)
4. Formal methods for cyberphysical systems (6 ECTS)
5. Quantum cryptography and security (6 ECTS)
6. Privacy preserving information access (6 ECTS)
7. Law and data (6 ECTS)

8. Secure software development (Padova) (6 ECTS))

Para el segundo semestre (Universidad de Vilna), se elegirá entre una de las siguientes optativas:

1. Malware (6 ECTS)
2. Rapid reaction and first response (6 ECTS)

En el tercer trimestre (Universidad de Granada), los estudiantes eligen dos optativas entre estas ofertadas:

1. International cooperation in cyberspace (3 ECTS)
2. Cyberwarfare (3 ECTS)
3. Post-quantum cryptography (3 ECTS)

El IV semestre se dedicará principalmente al trabajo de fin de master y a su redacción. Los estudiantes realizarán opcionalmente prácticas en una empresa o en una institución de investigación para la realización de su trabajo fin de master.

La conclusión del programa tendrá lugar en la Universidad de Minho con la defensa del trabajo fin de master por parte de todos los alumnos, así como también por un ejercicio práctico de laboratorio de ataque-defensa en equipo.

La carga de trabajo asignada a la realización del trabajo fin de master se complementa con una serie de seminarios que serán cursados a lo largo de todo el programa, impartidos por experto en la industria de la ciberseguridad.

El esquema del programa completo es el siguiente:

