# MÁSTER INTERUNIVERSITARIO EN CIBERSEGURIDAD

MUniCS

Universidade Vigo

UNIVERSIDADE DA CORUÑA

## 1. DESCRIPCIÓN DEL TITUTLO

| | |
|---|---|
| **Nombre de la Universidad** | Universidade de Vigo |
| **CIF** | Q8.650.002B |
| **Centro responsable del título** | Escola de Enxeñaría de Telecomunicación |
| **Denominación del título** | Máster en Ciberseguridad |
| **Centro/s donde se imparte el título** | Escola de Enxeñaría de Telecomunicación (UVigo); Facultade de Informática (UdC) |
| **Título conjunto** | Sí |
| **Universidades participantes** | Universidade de Vigo (coordinadora); Universidade da Coruña |
| **Rama de conocimiento** | Ingeniería y Arquitectura |
| **Código ISCED** | 480 (Informática)<br>520 (Ingeniería y profesiones afines) |
| **Habilita para profesión regulada** | No |
| **Modalidad de enseñanza** | Presencial |
| **Número de plazas ofertadas en el primer curso de implantación** | 40 (20 en cada una de las universidades participantes) |
| **Número de plazas en el segundo curso de implantación** | 40 (20 en cada una de las universidades participantes) |
| **Lenguas empleadas** | Español, gallego, inglés |
| **Número de ECTS del título** | 90 |

| **Universidad de Vigo** | **Tiempo completo** | | **Tiempo parcial** | |
|---|---|---|---|---|
| | **ECTS matrícula mínima** | **ECTS matrícula máxima** | **ECTS matrícula mínima** | **ECTS matrícula máxima** |
| **1er curso** | 48 | 60 | 18 | 47 |
| **Resto cursos** | 48 | 78 | 18 | 47 |

| **Universidad de La Coruña** | **Tiempo completo** | | **Tiempo parcial** | |
|---|---|---|---|---|
| | **ECTS matrícula mínima** | **ECTS matrícula máxima** | **ECTS matrícula mínima** | **ECTS matrícula máxima** |
| **1er curso** | 60 | 60 | 24 | 48 |
| **Resto cursos** | 48 | 78 | 24 | 48 |

## 2. CONTACTO

- Coordinador: Ana Fernández Vilas
- Email: camc@uvigo.es
- Web: http://munics.es

## 3. REQUISITOS DE ACCESO

Tal y como se recoge en el Real Decreto 1393/2007, que establece la ordenación de las enseñanzas universitarias oficiales, para acceder a las enseñanzas oficiales de Máster Universitario las y los aspirantes deberán de cumplir alguno de los siguientes requisitos:

a) Estar en posesión de un título universitario oficial español (graduada o graduado universitario, licenciada o licenciado, arquitecta o arquitecto, ingeniera o ingeniero, arquitecta técnica o arquitecto técnico, ingeniera técnica o ingeniero técnico, diplomada o diplomado) u otro expedido por una institución de educación superior perteneciente a otro Estado integrante del Espacio Europeo de Educación Superior que faculte en el mismo para el acceso a enseñanzas de Máster.

b) Las y los aspirantes con titulación extranjera expedida en una institución de educación superior no perteneciente a un Estado del Espacio Europeo de Educación Superior podrán acceder a los estudios de Máster si cumple alguno de los siguientes requisitos:

   a. Estar en posesión de un título expedido por un sistema universitario extranjero que esté homologado a un título español que habilite para el acceso a los estudios de posgrado.

   b. Poseer un título expedido por un sistema universitario extranjero, ajeno al EEES, y sin homologación, con la comprobación previa de que el título expedido por el sistema universitario extranjero acredita un nivel de formación equivalente al correspondiente título español de grado y que faculta para el acceso a los estudios de posgrado en el país en el que se expide el título.

      El acceso por esta vía no implicará, en ningún caso, la homologación del título previo de que esté en posesión el interesado, ni su reconocimiento a otros efectos que el de cursar las enseñanzas de Máster.

## 4. ADMISIÓN

Los criterios específicos de admisión al Máster serán, por orden de prevalencia, la titulación de acceso de los solicitantes, el expediente académico y la experiencia profesional. Tendrán preferencia en la admisión quienes posean un título de grado relacionado directamente con las tecnologías de la información y las comunicaciones por cualquier universidad del EEES, seguidos por quienes posean un título de grado en disciplinas científicas básicas (Matemáticas, Física o estudios afines), y estos tendrán preferencia sobre cualquier otro título académico. La experiencia profesional previa en el ámbito de la seguridad informática podrá ser utilizada por la comisión Académica del Máster como criterio adicional para decidir las admisiones, así como también, si lo considera necesario, la entrevista personal con las personas solicitantes para calibrar debidamente su aptitud y motivación. No se establecen complementos formativos de ninguna clase para las personas que no se adecuen significativamente a los criterios de admisión anteriores. El baremo de puntuación para la admisión es el siguiente:

- Estudios de acceso y expediente académico: 7 puntos
- Otros: 3 puntos

- Experiencia profesional: 0 a 2 puntos
- Motivación, interés, entrevista personal: 1 a 2 puntos

Las titulaciones de acceso se ordenarán según la siguiente prelación:

1. Máster Universitario en Informática y Máster Universitario en Ingeniería de Telecomunicación o sus equivalentes LRU (Ingeniería de Telecomunicación y Licenciatura o Ingeniería en Informática).
2. Grado en Ingeniería Informática y Grado con atribuciones profesionales en Ingeniería Técnica de Telecomunicación, en la rama Telemática, o sus equivalentes LRU.
3. Grado con atribuciones profesionales en Ingeniería Técnica de Telecomunicación, en otras ramas y grados "blancos" en Telecomunicación o sus equivalentes LRU.
4. Otras titulaciones de Ingeniería, Matemáticas o Física.
5. Otras titulaciones en función de la decisión de la Comisión Académica del Máster en Ciberseguridad (CAMC)

## 5. ÁREAS DE CONOCIMIENTO

En cuanto a las áreas de conocimiento responsables de la docencia de las materias del plan de estudios en la Universidad de La Coruña, la tabla siguiente recoge la adscripción del personal docente.

| | |
|---|---|
| Conceptos y Leyes en Ciberseguridad | Derecho Penal |
| Gestión da Seguridad da Información | Ciencia de la Computación e Inteligencia Artificial |
| Fundamentos de Ciberseguridad | Ciencia de la Computación e Inteligencia Artificial |
| Seguridad en Comunicación | Ingeniería Telemática |
| Seguridad en Aplicaciones | Ingeniería Telemática |
| Redes Seguras | Ingeniería Telemática |
| Fortificación de Sistemas Operativos | Ciencia de la Computación e Inteligencia Artificial |
| Test de Intrusión | Ciencia de la Computación e Inteligencia Artificial |
| Análisis de Malware | Ciencia de la Computación e Inteligencia Artificial |
| Seguridad como Negocio | Ingeniería Telemática |
| Seguridad en Dispositivos Móviles | Tecnología Electrónica |
| Análisis Forense de Equipos | Ciencia de la Computación e Inteligencia Artificial |
| Seguridad Ubicua | Ciencia de la Computación e Inteligencia Artificial |
| Ciberseguridad en Entornos Industriales | Tecnología Electrónica |
| Gestión de Incidentes | Ciencia de la Computación e Inteligencia Artificial |
| Prácticas en Empresa | Ingeniería Telemática |
| Trabajo Fin de Máster | Ingeniería Telemática |

## 6. PLANIFICACIÓN DE MATERIAS

Para una gestión más eficiente las asignaturas se han agrupan por módulos, y la distribución por módulos es la siguiente:

- Módulo de Gestión y Legislación en Ciberseguridad, de carácter obligatorio. Este módulo consta de 9 ECTS, repartidos en dos asignaturas de 6 y 3 ECTS, respectivamente.
- Módulo de Fundamentos de Ciberseguridad, de carácter obligatorio, compuesto por cuatro materias de 6 ECTS cada una.
- Módulo de Técnicas de Ciberseguridad. El módulo consta de cuatro materias, tres de ellas de 5 ECTS y una de 3 ECTS. El propósito de estas materias es completar la formación de los alumnos aplicando los conocimientos del módulo de Fundamentos a la protección de sistemas.
- Módulo de Formación Complementaria, de carácter obligatorio, pero formado por asignaturas optativas de 3 ECTS cada una.
- Módulo de Prácticas en Empresa y trabajo de fin de Máster, obligatorio, de 30 ECTS. Dentro de este módulo se contempla el reconocimiento de experiencia profesional. Corresponden 15 ECTS a la asignatura Prácticas en Empresa y otros 15 ECTS al Trabajo de Fin de Máster.

<table>
<tr><th>Cuatrimestre 1</th><th>Cuatrimestre 2</th></tr>
<tr><td>Gestión y legislación en ciberseguridad<br>(6 ECTS)</td><td rowspan="2">Técnicas de ciberseguridad<br>(18 ECTS)</td></tr>
<tr><td rowspan="2">Fundamentos de ciberseguridad<br>(24 ECTS)</td></tr>
<tr><td>Gestión y legislación en ciberseguridad<br>(3 ECTS)</td></tr>
<tr><td></td><td>Formación complementaria<br>(9 ECTS)</td></tr>
<tr><td colspan="2">Cuatrimestre 3</td></tr>
<tr><td colspan="2">Módulo de prácticas en empresa (15 ECTS)</td></tr>
<tr><td colspan="2">Módulo de trabajo de fi de máster (15 ECTS)</td></tr>
</table>

Con esta estructura y estas asignaturas se obtendría el título de Máster en Ciberseguridad con 90 ECTS. Para completar la titulación, un/a alumno/a habrá de cursar todos los módulos obligatorios y 3 materias (9 ECTS) a elegir libremente de entre las del módulo de Formación Complementaria. El plan de estudios no contempla especialidades, pero, como se ve, reserva 9 ECTS para que los/las estudiantes particularicen su formación en aquellas áreas específicas que resulten de su mayor interés.

| Tipo de materia | Créditos a cursar | Créditos ofertados |
|---|---|---|
| Obligatorias | 51 | 51 |
| Optativas | 9 | 15 |
| Prácticas externas (si son OB) | 15 | 15 |
| Trabajo fin de Máster | 15 | 15 |
| **Total** | 90 | 96 |

## 7. MATERIAS POR MÓDULO

| Módulo | Asignaturas | ECTS | Carácter | Cuatrimestre | Curso |
|---|---|---|---|---|---|
| Gestión y legislación en ciberseguridad | Conceptos y leyes en ciberseguridad | 3 | Obligatorio | 2 | 1 |
| | Gestión de la seguridad de la información | 6 | Obligatorio | 1 | 1 |
| Fundamentos de Ciberseguridad | Seguridad de la información | 6 | Obligatorio | 1 | 1 |
| | Seguridad en comunicaciones | 6 | Obligatorio | 1 | 1 |
| | Seguridad de aplicaciones | 6 | Obligatorio | 1 | 1 |
| | Redes seguras | 6 | Obligatorio | 1 | 1 |
| Técnicas de ciberseguridad Formación complementaria | Fortificación de sistemas operativos | 5 | Obligatorio | 2 | 1 |
| | *Tests* de intrusión | 5 | Obligatorio | 2 | 1 |
| | Análisis de *malware* | 5 | Obligatorio | 2 | 1 |
| | Seguridad como negocio | 3 | Obligatorio | 2 | 1 |
| Formación Complementaria | Seguridad en dispositivos móviles | 3 | Optativo | 2 | 1 |
| | Análisis forense de equipos | 3 | Optativo | 2 | 1 |
| | Seguridad ubicua | 3 | Optativo | 2 | 1 |
| | Gestión de incidentes | 3 | Optativo | 2 | 1 |
| | Ciberseguridad en entornos industriales | 3 | Optativo | 2 | 1 |
| Prácticas en empresa y trabajo de fin de máster | Prácticas en empresa | 15 | Prácticas externas | 1 | 2 |
| | Trabajo de fin de máster | 15 | Trabajo de fin de máster | 1 | 2 |

## 8. MÓDULO DE GESTIÓN Y LEGISLACIÓN EN CIBERSEGURIDAD

| **Gestión y legislación en ciberseguridad** | **Gestión de seguridad de la información** |
|---|---|
| Curso | Primero |
| ECTS | 6 |
| Carácter | Obligatoria |
| Semestre | Primero |
| Competencias básicas y generales | (CB2) (CB3) (CG1) (CG2) |
| Competencias específicas | (CE5) (CE7) (CE13) |
| Competencias transversales | (CT4) (CT5) |
| Resultados de aprendizaje | • Conocer los conceptos fundamentales relacionados con la Gestión de la Seguridad de la Información: vulnerabilidad, amenaza, riesgo, contramedida, política de seguridad, plan de seguridad, auditoría<br>• Conocer las diferentes metodologías de Gestión de Seguridad de la Información, comúnmente aceptadas<br>• Conocer las herramientas propias para llevar a cabo tareas relacionadas con el análisis de riesgos y la auditoría de seguridad, así como saber cuáles son las más adecuadas a cada entorno |
| Contenidos | • Fundamentos<br>• Análisis de impacto en el negocio<br>• Análisis y gestión de riesgos<br>• Plan de seguridad<br>• Auditoría de seguridad.<br>• Herramientas |
| Observaciones | |
| Metodologías docentes (incluir listado) | Sesión magistral; Prácticas TIC; Trabajos y/o proyectos (individuales o en grupo); Trabajo autónomo del alumno; Atención personalizada |

| Actividades formativas | | |
|---|---|---|
| Denominación de la actividad formativa | Horas | Presencialidad (%) |
| Sesión magistral y Resolución de problemas/ejercicios | 63 | 33,3 |
| Prácticas de laboratorio | 87 | 24,1 |

| Sistemas de evaluación | | |
|---|---|---|
| Denominación del sistema de evaluación | Ponderación mínima (%) | Ponderación máxima (%) |
| Pruebas de desarrollo, objetivas y resolución de problemas y/o ejercicios (con posibilidad de examen final) | 15 | 100 |
| Pruebas prácticas (con posibilidad de un examen final) | 0 | 85 |
| Evaluación de trabajos y actividades | 0 | 85 |

| Gestión y legislación en ciberseguridad | Conceptos y leyes en ciberseguridad |
|---|---|
| Curso | Primero |
| ECTS | 3 |
| Carácter | Obligatoria |
| Semestre | Segundo |
| Competencias básicas y generales | (CB3) |
| Competencias específicas | (CE3) (CE18) |
| Competencias transversales | (CT1) (CT5) |
| Resultados de aprendizaje | • Dominio de los conceptos jurídicos relacionados con la cibercriminalidad<br>• Dominio de los criterios de aplicación de los diferentes tipos penales relacionados con la criminalidad<br>• Adquisición de la capacidad crítica sobre legislación, doctrina y jurisprudencia relativa a la criminalidad informática.<br>• Capacidad de afrontar la resolución de casos prácticos con rigor científico |
| Contenidos | • Parte General: *Computer crime* y *cybercrime*: evolución del Derecho penal informático. Internet y libertad de expresión; Problemáticas especiales de los delitos informáticos en el contexto de la parte general del Derecho penal; La criminalidad informática desde el punto de vista criminológico<br>• Parte específica: Delitos contra la intimidad y la privacidad; Delitos contra la libertad: *Stalking* y *Cyberstalking;* Delitos contra la propiedad: estafa y fraudes informáticos; daños de datos y sistemas informáticos; Delitos contra la fe pública; falsificación electrónica; Delitos contra la propiedad intelectual La cibercriminalidad relacionada con menores: pornografía infantil, *child grooming*; Ciberterrorismo |
| Observaciones | |
| Metodologías docentes (incluir listado) | Sesión magistral<br>Prácticas TIC<br>Trabajos y/o proyectos (individuales o en grupo)<br>Trabajo autónomo del alumno<br>Atención personalizada |

| Actividades formativas | | |
|---|---|---|
| Denominación de la actividad formativa | Horas | Presencialidad (%) |
| Sesión magistral y resolución de problemas/ejercicios | 48 | 33,3 |
| Prácticas de laboratorio y proyectos individuales o en grupo | 27 | 18,5 |

| Sistemas de evaluación | | |
|---|---|---|
| Denominación del sistema de evaluación | Ponderación mínima (%) | Ponderación máxima (%) |
| Pruebas de desarrollo, objetivas y resolución de problemas y/o ejercicios (con posibilidad de un examen final) | 30 | 100 |
| Evaluación de trabajos y actividades | 0 | 70 |

# 9. MÓDULO FUNDAMENTOS DE CIBERSEGURIDAD

| **Fundamentos de ciberseguridad** | **Seguridad de la información** |
|---|---|
| Curso | Primero |
| ECTS | 6 |
| Carácter | Obligatoria |
| Semestre | Primero |
| Competencias básicas y generales | (CB2) (CB4) (CB5) |
| Competencias específicas | (CE1) (CE4) (CE10) |
| Competencias transversales | (CT4) (CT5) |
| Resultados de aprendizaje | • Comprender los mecanismos básicos que se esconden tras los algoritmos de cifrado simétrico en bloque, y contrastarlos con los utilizados en los cifradores de flujo.<br>• Explicar qué son las funciones hash, qué papel juegan en el ámbito de la seguridad de la información, y, en particular, cómo se utilizan para confirmar la inviolabilidad (integridad) de los datos.<br>• Explicar los fundamentos que hay detrás de los algoritmos de cifrado asimétrico, sus ventajas/desventajas con respecto al cifrado simétrico, y las aplicaciones de sus diferentes implementaciones (RSA, Diffie-Hellman, DSS, ECC).<br>• Describir en qué consisten los sistemas PKI (infraestructura de clave pública), y cualquier concepto relacionado con los certificados digitales y su estructura/uso/gestión.<br>• Describir en qué consisten los mecanismos/sistemas de firma y sobre digital.<br>• Comprender la importancia de los generadores de números aleatorios en el ámbito de la criptografía.<br>• Manejar herramientas criptográficas para el cifrado, autenticación y firma digital de la información, y para la creación de certificados y autoridades de certificación.<br>• Evaluar cuál es la solución más adecuada (tipo, algoritmo, longitud de clave, etc.) para implantar en el sistema que tengan que administrar. |
| Contenidos | • Confidencialidad, integridad y autenticación.<br>• Clasificación de los algoritmos de cifrado.<br>• Confidencialidad de la información mediante cifrado simétrico.<br>• Autenticación de mensajes y funciones Hash.<br>• Cifrado de clave pública.<br>• Firmas digitales.<br>• Gestión de claves.<br>• Generación de números aleatorios. |
| Observaciones | |
| Metodologías docentes (incluir listado) | Sesión magistral; Prácticas TIC; Trabajos y/o proyectos (individuales o en grupo); Trabajo autónomo del alumno; Atención personalizada |

| Actividades formativas | | |
|---|---|---|
| Denominación de la actividad formativa | Horas | Presencialidad (%) |
| Sesión magistral y Resolución de problemas/ejercicios | 63 | 33,3 |
| Prácticas de laboratorio y Proyectos individuales o en grupo | 87 | 24,1 |

| Sistemas de evaluación | | |
|---|---|---|
| Denominación del sistema de evaluación | Ponderación mínima (%) | Ponderación máxima (%) |
| Pruebas de desarrollo objetivos y resolución de problemas y/o ejercicios (con posibilidad de un examen final) | 15 | 100 |
| Pruebas prácticas (con posibilidad de un examen final) | 0 | 85 |
| Evaluación de trabajos y actividades | 0 | 85 |

| **Fundamentos de ciberseguridad** | **Seguridad en comunicaciones** |
|---|---|
| Curso | Primero |
| ECTS | 6 |
| Carácter | Obligatoria |
| Semestre | Primero |
| Competencias básicas y generales | (CB2) (CB4) (CB5) (CG1) (CG3) (CG8) |
| Competencias específicas | (CE1) (CE2) (CE4) (CE8) |
| Competencias transversales | (CT4) (CT5) |
| Resultados de aprendizaje | • Conocerán en detalle los protocolos de red que aportan seguridad a la transmisión de la información, y las implicaciones derivadas del lugar que ocupan dentro de la arquitectura en que se organiza el software de comunicaciones.<br>• Comprenderán que otros protocolos, siendo auxiliares (no relativos al mundo de la seguridad), presentan vulnerabilidades explotables; y podrán describir los ataques más comunes que tratan de aprovecharlas (mitm, suplantación de DHCP/DNS, DoS, SSL-Stripping, ...), y sus posibles contramedidas.<br>• Sabrán identificar qué solución/protocolo es el adecuado para asegurar un entorno determinado: seguridad en LAN (802.1X), acceso inalámbrico (EAPoW, WPA/WPA2), seguridad extremo a extremo (IPSEC en modo transporte, TLS/SSL), conexiones punto a punto (PPP, IPSEC en modo túnel), etc.<br>• Conocerán las soluciones que se esconden tras ciertos servicios de red y/o aplicaciones universalmente utilizadas (DNSSEC, S/MIME, HTTPS, SSH...).<br>• Serán capaces de configurar las diferentes herramientas (paquetes software) que los distintos sistemas operativos/plataformas nos aportan para activar la seguridad en las comunicaciones. |
| Contenidos | • Seguridad en capa física y de enlace.<br>• Seguridad en capa de red.<br>• Seguridad en capa de transporte.<br>• Seguridad en capa de aplicación. |
| Observaciones | |
| Metodologías docentes (incluir listado) | Sesión magistral; Prácticas TIC; Trabajos y/o proyectos (individuales o en grupo); Trabajo autónomo del alumno; Atención personalizada |

| Actividades formativas | | |
|---|---|---|
| Denominación de la actividad formativa | Horas | Presencialidad (%) |
| Sesión magistral y Resolución de problemas/ejercicios | 63 | 33,3 |
| Prácticas de laboratorio y Proyectos individuales o en grupo | 87 | 24,1 |

| Sistemas de evaluación | | |
|---|---|---|
| Denominación del sistema de evaluación | Ponderación mínima (%) | Ponderación máxima (%) |
| Pruebas de desarrollo, objetivas y resolución de problemas y/o ejercicios (con posibilidad de un examen final) | 15 | 100 |
| Pruebas prácticas (con posibilidad de un examen final) | 0 | 85 |
| Evaluación de trabajos y actividades | 0 | 85 |

| **Fundamentos de ciberseguridad** | **Seguridad de aplicaciones** |
|---|---|
| Curso | Primero |
| ECTS | 6 |
| Carácter | Obligatoria |
| Semestre | Primero |
| Competencias básicas y generales | (CB2) (CG2) |
| Competencias específicas | (CE2) (CE7) (CE13) |
| Competencias transversales | (CT4) (CT5) |
| Resultados de aprendizaje | • Comprender los problemas potenciales de seguridad que presentan las aplicaciones compiladas<br>• Detectar los problemas de seguridad de aplicaciones compiladas.<br>• Comprender los mecanismos de protección diseñados para limitar o anular el impacto de los problemas de seguridad del software compilado<br>• Ser capaz de corregir el software compilado para solucionar problemas detectados<br>• Entender las vulnerabilidades comunes de las aplicaciones web<br>• Encontrar problemas seguridad en aplicaciones web.<br>• Ser capaz de corregir los problemas de seguridad detectados en aplicaciones web. |
| Contenidos | • CWE y OWASP<br>• Seguridad del software compilado<br>• Vulnerabilidades específicas al código nativo<br>• Seguridad en aplicaciones web y servicios web (APIs)<br>• Autenticación y autorización, y frameworks de aplicación para la protección de recursos<br>• Integración de la seguridad en metodologías de desarrollo software<br>• Herramientas de protección y testing |
| Observaciones | |
| Metodologías docentes (incluir listado) | Sesión magistral; Prácticas TIC; Trabajos y/o proyectos (individuales o en grupo); Trabajo autónomo del alumno; Atención personalizada |

| Actividades formativas | | |
|---|---|---|
| Denominación de la actividad formativa | Horas | Presencialidad (%) |
| Sesión magistral y resolución de problemas/ejercicios | 63 | 33,3 |
| Prácticas de laboratorio y proyectos individuales o en grupo | 87 | 24,1 |

| Sistemas de evaluación | | |
|---|---|---|
| Denominación del sistema de evaluación | Ponderación mínima (%) | Ponderación máxima (%) |
| Pruebas de desarrollo, objetivas y resolución de problemas y/o ejercicios (con posibilidad de un examen final) | 15 | 100 |
| Pruebas prácticas (con posibilidad de un examen final) | 0 | 85 |
| Evaluación de trabajos y actividades | 0 | 85 |

| **Fundamentos de ciberseguridad** | **Redes seguras** |
|---|---|
| Curso | Primero |
| ECTS | 6 |
| Carácter | Obligatoria |
| Semestre | Primero |
| Competencias básicas y generales | (CB2) (CB4) (CB5) (CG1) (CG3) (CG8) |
| Competencias específicas | (CE2) (CE4) (CE8) (CE12) |
| Competencias transversales | (CT4) (CT5) |
| Resultados de aprendizaje | • Comprenderán el papel de un cortafuegos en la estrategia de seguridad de un ordenador o de la red a la que protege.<br>• Serán capaces de describir qué son las políticas de acceso, y de diseñar/especificar el conjunto de las mismas que requiere un escenario o caso particular.<br>• Conocerán los diferentes modelos de filtrado de paquetes (con/sin estado) y los cortafuegos de nivel de aplicación, y sabrán configurarlos en diversas plataformas.<br>• Podrán diseñar y describir, para un escenario/topología concreto, configuraciones alternativas para emplazar el cortafuegos dentro de la red corporativa (sistema fortificado, DMZ, cortafuegos distribuido).<br>• Serán capaces de describir los principios básicos que sustentan la detección de intrusiones, los sensores habituales que utilizan para la recopilación de información, y las técnicas de análisis (detección de anomalías versus detección heurística) que deciden cuándo disparar una alarma. Y conocerán posibles soluciones técnicas (HIDS/NIDS, IPS, SIEM, honeypot), que sabrán instalar y configurar para algunas plataformas e implementaciones particulares.<br>• Estarán familiarizados con los conceptos de túnel y virtualización de redes, y serán capaces de elegir e implementar la tecnología de red privada virtual más apropiada para diferentes escenarios.<br>• Podrán explicar los principios sobre los que se construyen las redes anónimas. |
| Contenidos | • Seguridad perimetral.<br>• Cortafuegos.<br>• Sistemas de detección de intrusos.<br>• VPNs.<br>• Redes anónimas. |
| Observaciones | |
| Metodologías docentes (incluir listado) | Sesión magistral; Prácticas TIC; Trabajos y/o proyectos (individuales o en grupo); Trabajo autónomo del alumno; Atención personalizada |

| Actividades formativas | | |
|---|---|---|
| Denominación de la actividad formativa | Horas | Presencialidad (%) |
| Sesión magistral y Resolución de problemas/ejercicios | 63 | 33,3 |
| Prácticas de laboratorio y Proyectos individuales o en grupo | 87 | 24,1 |

| Sistemas de evaluación | | |
|---|---|---|
| Denominación del sistema de evaluación | Ponderación mínima (%) | Ponderación máxima (%) |
| Pruebas de desarrollo, objetivas y resolución de problemas y/o ejercicios (con posibilidad de un examen final) | 15 | 100 |
| Pruebas prácticas (con posibilidad de un examen final) | 0 | 85 |
| Evaluación de trabajos y actividades | 0 | 85 |

# 10. MÓDULO TÉCNICAS DE CIBERSEGURIDAD

| **Técnicas de ciberseguridad** | **Fortificación de sistemas operativos** |
|---|---|
| Curso | Primero |
| ECTS | 5 |
| Carácter | Obligatoria |
| Semestre | Segundo |
| Competencias básicas y generales | (CB2) (CB5) (CG1) (CG2) (CG5) |
| Competencias específicas | (CE4) (CE8) |
| Competencias transversales | (CT4) (CT5) |
| Resultados de aprendizaje | • Instalación y administración segura de sistemas (servidores, escritorio) tanto en entornos Microsoft como en entornos Linux<br>• Fortificación escalable de sistemas basada en mecanismos de gestión de identidad centralizada<br>• Reducción de las superficies de ataque en los sistemas operativos más habituales |
| Contenidos | • Seguridad en Sistemas Linux: Fortificación; Despliegue de Servicios<br>• Seguridad en Entornos Microsoft: Equipos de Escritorio; Servidores; Directorio Activo<br>• Entornos virtuales<br>• Otros sistemas |
| Observaciones | |
| Metodologías docentes (incluir listado) | Sesión magistral; Prácticas TIC; Trabajos y/o proyectos (individuales o en grupo); Trabajo autónomo del alumno; Atención personalizada |

| Actividades formativas | | |
|---|---|---|
| Denominación de la actividad formativa | Horas | Presencialidad (%) |
| Sesión magistral y Resolución de problemas/ejercicios | 27 | 33 |
| Prácticas de laboratorio y Proyectos individuales o en grupo | 98 | 26,5 |

| Sistemas de evaluación | | |
|---|---|---|
| Denominación del sistema de evaluación | Ponderación mínima (%) | Ponderación máxima (%) |
| Pruebas de desarrollo, objetivas y resolución de problemas y/o ejercicios (con posibilidad de un examen final) | 15 | 100 |
| Pruebas prácticas (con posibilidad de un examen final) | 0 | 85 |
| Evaluación de trabajos y actividades | 0 | 85 |

| Técnicas de ciberseguridad | Tests de intrusión |
|---|---|
| Curso | Primero |
| ECTS | 5 |
| Carácter | Obligatorio |
| Semestre | Segundo |
| Competencias básicas y generales | (CB2) (CB3) (CB4) (CB5) (CG1) (CG2) (CG4) |
| Competencias específicas | (CE2) (CE4) (CE7) |
| Competencias transversales | (CT4) (CT5) |
| Resultados de aprendizaje | • El alumno conocerá las herramientas habituales comúnmente utilizadas para el desarrollo de test de intrusión, y a usarlas con responsabilidad<br>• El alumno será capaz de planificar un test de intrusión en una organización, partiendo una información inicial limitada<br>• El alumno será capaz de llevar a cabo test de intrusión con el objetivo de detectar vulnerabilidades y documentarlas adecuadamente, sin provocar daño en las redes o sistemas<br>• El alumno interiorizará la ética relacionada con los test de intrusión y se comportará en base a dicha ética |
| Contenidos | • Fundamentos. Presentación de herramientas y "frameworks"<br>• Estrategias de reconocimiento<br>• Estrategias ofensivas<br>• Métodos de evasión<br>• Principios éticos de los test de intrusión |
| Observaciones | |
| Metodologías docentes (incluir listado) | Sesión magistral; Prácticas TIC; Trabajos y/o proyectos (individuales o en grupo); Trabajo autónomo del alumno; Atención personalizada |

| Actividades formativas | | |
|---|---|---|
| Denominación de la actividad formativa | Horas | Presencialidad (%) |
| Sesión magistral y Resolución de problemas/ejercicios | 27 | 33,3 |
| Prácticas de laboratorio y Proyectos individuales o en grupo | 98 | 26,5 |

| Sistemas de evaluación | | |
|---|---|---|
| Denominación del sistema de evaluación | Ponderación mínima (%) | Ponderación máxima (%) |
| Pruebas de desarrollo, objetivas y resolución de problemas y/o ejercicios (con posibilidad de examen final) | 15 | 100 |
| Pruebas prácticas (con posibilidad de un examen final) | 0 | 85 |
| Evaluación de trabajos y actividades | 0 | 85 |

| **Técnicas de ciberseguridad** | **Análisis de *malware*** |
|---|---|
| Curso | Primero |
| ECTS | 5 |
| Carácter | Obligatoria |
| Semestre | Segundo |
| Competencias básicas y generales | (CB1) (CG1) |
| Competencias específicas | (CE8) (CE11) (CE13) |
| Competencias transversales | (CT4) (CT5) |
| Resultados de aprendizaje | • Analizar, detectar y eliminar malware en sistemas y redes.<br>• Conocer, detectar y luchar contra las técnicas de ocultación y persistencia de malware en sistemas y redes.<br>• Estudiar sistemas y redes para detectar y eliminar las vulnerabilidades susceptibles de ser utilizadas por el malware.<br>• Conocer las tendencias actuales en malware y las experiencias aprendidas de casos reales. |
| Contenidos | • Introducción al análisis e ingeniería de *malware*<br>• Tipos de *malware*. Estructura, componentes, vectores de infección<br>• Ingeniería de *malware*. Técnicas de propagación, infección, persistencia, ocultación<br>• Ingeniería inversa de *malware*<br>• Herramientas de análisis de *malware* |
| Observaciones | |
| Metodologías docentes (incluir listado) | Sesión magistral; Prácticas TIC; Trabajos y/o proyectos (individuales o en grupo); Trabajo autónomo del alumno; Atención personalizada |

| Actividades formativas | | |
|---|---|---|
| Denominación de la actividad formativa | Horas | Presencialidad (%) |
| Sesión magistral y resolución de problemas/ejercicios | 51 | 33,3 |
| Prácticas de laboratorio y proyectos individuales o en grupo | 74 | 24,3 |

| Sistemas de evaluación | | |
|---|---|---|
| Denominación del sistema de evaluación | Ponderación mínima (%) | Ponderación máxima (%) |
| Pruebas de desarrollo, objetivas y resolución de problemas y/o ejercicios (con posibilidad de un examen final) | 15 | 100 |
| Pruebas prácticas (con posibilidad de un examen final) | 0 | 85 |
| Evaluación de trabajos y actividades | 0 | 85 |

| Técnicas de ciberseguridad | Seguridad como negocio |
|---|---|
| Curso | Primero |
| ECTS | 3 |
| Carácter | Obligatoria |
| Semestre | Segundo |
| Competencias básicas y generales | (CB1) (CB4)(CG3) (CG6) |
| Competencias específicas | (CE9) (CE11) (CE15) (CE16) (CE19) (CE20) |
| Competencias transversales | (CT4) (CT5) |
| Resultados de aprendizaje | • Conocer los conceptos fundamentales sobre el negocio de la seguridad digital siendo capaces de monetizar la información.<br>• Entender que es posible orientar una empresa en el ámbito de la seguridad e incluso a sectores más específicos dentro de este ámbito.<br>• Definir los perfiles necesarios, propios de la empresa o externos, asociados a la ciberseguridad.<br>• Conocer empresas del sector, su creación, desarrollo y orientación.<br>• Conocer los cauces correctos de comunicación en la institución, especialmente con la gerencia. |
| Contenidos | • La seguridad como elemento transversal de la institución. Monetización de los datos y de la seguridad de los mismos.<br>• Perfiles de ciberseguridad en las entidades.<br>• Oportunidades de negocio y orientación en los sectores productivos<br>• Casos de éxito. |
| Observaciones | |
| Metodologías docentes (incluir listado) | Sesión magistral; Resolución de problemas/ejercicios; Trabajos Tutelados individuales o en grupo |

| Actividades formativas | | |
|---|---|---|
| Denominación de la actividad formativa | Horas | Presencialidad (%) |
| Sesión magistral y resolución de problemas/ejercicios | 30 | 33,3 |
| Problemas/ejercicios en sesiones presenciales y seguimiento de trabajos tutelados | 45 | 24,4 |

| Sistemas de evaluación | | |
|---|---|---|
| Denominación del sistema de evaluación | Ponderación mínima (%) | Ponderación máxima (%) |
| Prueba objetiva y resolución de problemas y/o ejercicios (con posibilidad de examen final) | 30 | 70 |
| Evaluación de trabajos y actividades | 30 | 70 |

# 11. MÓDULO FORMACIÓN COMPLEMENTARIA

| Formación complementaria | Seguridad en dispositivos móviles |
|---|---|
| Curso | Primero |
| ECTS | 3 |
| Carácter | Optativa |
| Semestre | Segundo |
| Competencias básicas y generales | (CB2) (CB3) (CB4) (CG1) (CG2) (CG5) |
| Competencias específicas | (CE4) (CE6) (CE9) (CE15) |
| Competencias transversales | (CT4) (CT5) |
| Resultados de aprendizaje | • Conocer los conceptos fundamentales asociados con la seguridad en los sistemas operativos móviles y el desarrollo de apps seguras.<br>• Identificar una app con comportamiento malicioso y vulnerabilidades en sistemas operativos y apps<br>• Ser capaz de realizar un análisis forense de un dispositivo móvil<br>• Conocer los sistemas gestión de dispositivos móviles |
| Contenidos | • Estudio de arquitecturas de sistemas operativos móviles<br>• Desarrollo de apps seguras<br>• Apps maliciosas<br>• Vulnerabilidades de SO y apps<br>• Análisis forense de sistemas operativos móviles<br>• Sistemas Mobile Device Management (MDM) |
| Observaciones | |
| Metodologías docentes (incluir listado) | Sesión magistral; Prácticas TIC; Trabajos y/o proyectos (individuales o en grupo); Trabajo autónomo del alumno; Atención personalizada |

| Actividades formativas | | |
|---|---|---|
| Denominación de la actividad formativa | Horas | Presencialidad (%) |
| Sesión magistral y Resolución de problemas/ejercicios | 30 | 33,3 |
| Prácticas de laboratorio y Proyectos individuales o en grupo | 45 | 24,4 |

| Sistemas de evaluación | | |
|---|---|---|
| Denominación del sistema de evaluación | Ponderación mínima (%) | Ponderación máxima (%) |
| Pruebas de desarrollo, objetivas y resolución de problemas y/o ejercicios (con posibilidad de examen final) | 15 | 100 |
| Pruebas prácticas (con posibilidad de examen final) | 0 | 85 |
| Evaluación de trabajos y actividades | 0 | 85 |

| Formación complementaria | Análisis forense de equipos |
|---|---|
| Curso | Primero |
| ECTS | 3 |
| Carácter | Optativo |
| Semestre | Segundo |
| Competencias básicas y generales | (CB1) (CB2)(CB3) (CG2) |
| Competencias específicas | (CE6) |
| Competencias transversales | (CT4) (CT5) |
| Resultados de aprendizaje | • Conocimiento de las metodologías adecuadas para la realización de trabajos forenses con validez legal<br>• Capacidad para la realización de análisis forense de los diferentes elementos que forman un sistema de información, en múltiples plataformas y sistemas operativos<br>• Capacidad para generar informes como resultado del análisis forense claro, concisos e inteligibles tanto por expertos como por personas ajenas al ámbito de la seguridad informática |
| Contenidos | • Fundamentos<br>• Metodología de Análisis Forense<br>• Herramientas de Análisis Forense: Entornos Linux Y Windows<br>• Casos |
| Observaciones | |
| Metodologías docentes (incluir listado) | Sesión magistral; Resolución de problemas/ejercicios; Prácticas de laboratorio; Proyectos individuales o en grupo |

| Actividades formativas | | |
|---|---|---|
| Denominación de la actividad formativa | Horas | Presencialidad (%) |
| Sesión magistral y Resolución de problemas/ejercicios | 15 | 33,3 |
| Prácticas de laboratorio y Proyectos individuales o en grupo | 60 | 26,6 |

| Sistemas de evaluación | | |
|---|---|---|
| Denominación del sistema de evaluación | Ponderación mínima (%) | Ponderación máxima (%) |
| Preguntas tipo test y/o resolución de problemas/ejercicios | 10 | 80 |
| Prácticas de laboratorio | 10 | 80 |
| Proyectos individuales o en grupo | 10 | 80 |

| Formación complementaria | Seguridad ubicua |
|---|---|
| Curso | Primero |
| ECTS | 3 |
| Carácter | Optativa |
| Semestre | Segundo |
| Competencias básicas y generales | (CB2) (CB3) (CB4) (CG1) (CG2) (CG5) |
| Competencias específicas | (CE4) (CE9) |
| Competencias transversales | (CT4) (CT5) |
| Resultados de aprendizaje | • Conocer la seguridad en las diferentes capas relacionadas con los sistemas ubicuos y las tecnologías que utilizan<br>• Entender los problemas de seguridad asociados al mundo ubicuo<br>• Conocer casos reales de ataques a sistemas ubicuos |
| Contenidos | Seguridad:<br>-física<br>-en middleware<br>-en comunicaciones<br>-en percepción del entorno<br>Escenarios reales:<br>-redes PAN<br>-redes de sensores<br>-IoT<br>-drones<br>-coche conectado<br>-etc. |
| Observaciones | |
| Metodologías docentes (incluir listado) | Sesión magistral; Prácticas TIC; Trabajos y/o proyectos (individuales o en grupo); Trabajo autónomo del alumno; Atención personalizada |

| Actividades formativas | | |
|---|---|---|
| Denominación de la actividad formativa | Horas | Presencialidad (%) |
| Sesión magistral y Resolución de problemas/ejercicios | 30 | 33,3 |
| Prácticas de laboratorio y Proyectos individuales o en grupo | 45 | 24,4 |

| Sistemas de evaluación | | |
|---|---|---|
| Denominación del sistema de evaluación | Ponderación mínima (%) | Ponderación máxima (%) |
| Pruebas de desarrollo, objetivas y resolución de problemas y/o ejercicios (con posibilidad de examen final) | 15 | 100 |
| Pruebas prácticas (con posibilidad de examen final) | 0 | 85 |
| Evaluación de trabajos y actividades | 0 | 85 |

| Formación complementaria | Ciberseguridad en entornos industriales |
|---|---|
| Curso | Primero |
| ECTS | 3 |
| Carácter | Optativa |
| Semestre | Segundo |
| Competencias básicas y generales | (CB1) (CG2) (CG5) |
| Competencias específicas | (CE4) (CE7) (CE12) (CE15) |
| Competencias transversales | (CT4) (CT5) |
| Resultados de aprendizaje | • Comprender la ejecución de políticas de seguridad y sus implicaciones en entornos industriales<br>• Comprender las diferentes técnicas de protección y ataque en sistemas industriales y saber cómo se pueden implementar.<br>• Entender las problemáticas de seguridad y los ataques a redes de control en industria y conocer los mecanismos que permiten minimizarlos.<br>• Ser capaz de comprender las implicaciones a nivel de seguridad de la nueva industria 4.0 |
| Contenidos | • Introducción a la Seguridad en Sistemas industriales<br>• Análisis activo y pasivo en sistemas SCADA, DSS, PLC´s<br>• Protección y ataques de sistemas industriales y redes de control (LCN, Modbus, Fieldbus, RS422, ...)<br>• Seguridad de la industria 4.0 |
| Observaciones | |
| Metodologías docentes (incluir listado) | Sesión magistral; Prácticas TIC; Trabajos y/o proyectos (individuales o en grupo); Trabajo autónomo del alumno;Atención personalizada |

| Actividades formativas | | |
|---|---|---|
| Denominación de la actividad formativa | Horas | Presencialidad (%) |
| Sesión magistral y resolución de problemas/ejercicios | 30 | 33,3 |
| Prácticas de laboratorio y proyectos individuales o en grupo | 45 | 24,4 |

| Sistemas de evaluación | | |
|---|---|---|
| Denominación del sistema de evaluación | Ponderación mínima (%) | Ponderación máxima (%) |
| Pruebas de desarrollo, objetivas y resolución de problemas y/o ejercicios (con posibilidad de un examen final) | 15 | 100 |
| Pruebas prácticas (con posibilidad de un examen final) | 0 | 85 |
| Evaluación de trabajos y actividades | 0 | 85 |

| Formación complementaria | Gestión de incidentes |
|---|---|
| Curso | Primero |
| ECTS | 3 |
| Carácter | Optativo |
| Semestre | Segundo |
| Competencias básicas y generales | (CB2) (CB3) (CB5) (CG1) (CG5) |
| Competencias específicas | (CE3) (CE9) (CE14) (CE15) (CE17) |
| Competencias transversales | (CT4) (CT5) |
| Resultados de aprendizaje | • Manejar la proactividad para prevenir y atenuar posibles incidentes de seguridad.<br>• Obtener el conocimiento necesario sobre herramientas que pueden facilitar la gestión de los incidentes y las recuperaciones.<br>• Justificar económicamente los planes propuestos para recuperación y resiliencia.<br>• Identificar y clasificar los posibles incidentes y definir los cauces para su gestión y resolución. |
| Contenidos | • Fundamentos: resiliencia y el valor de la información.<br>• Detección de incidentes y gestión de respuesta.<br>• Estándares: planes de continuidad y de recuperación.<br>• Recuperación de desastres<br>• Legislación |
| Observaciones | |
| Metodologías docentes (incluir listado) | Sesión magistral<br>Resolución de problemas/ejercicios<br>Prácticas TIC<br>Trabajos y/o proyectos individuales o en grupo |

| Actividades formativas | | |
|---|---|---|
| Denominación de la actividad formativa | Horas | Presencialidad (%) |
| Sesión magistral y Resolución de problemas/ejercicios | 30 | 33,3 |
| Prácticas de laboratorio y Proyectos individuales o en grupo | 45 | 24,4 |

| Sistemas de evaluación | | |
|---|---|---|
| Denominación del sistema de evaluación | Ponderación mínima (%) | Ponderación máxima (%) |
| Prueba objetiva y/o resolución de problemas y/o ejercicios (con posibilidad de un examen final) | 30 | 60 |
| Prácticas TIC | 20 | 50 |
| Evaluación de trabajos y actividades | 20 | 50 |

| **Prácticas en empresa y trabajo de fin de máster** | **Prácticas en empresa** |
|---|---|
| Curso | Segundo |
| ECTS | 15 |
| Carácter | Obligatoria |
| Semestre | Primero |
| Competencias básicas y generales | (CB1) 0<br>(CB2) 0<br>(CB3) 0<br>(CB4) 0<br>(CB5) (CG1) (CG2) (CG3) (CG4) (CG5) (CG6) |
| Competencias específicas | Todas las del título |
| Competencias transversales | (CT1) (CT3) (CT4) (CT5) |
| Resultados de aprendizaje | Experiencia en el desempeño de la ciberseguridad, y de sus funciones más habituales en un entorno real de trabajo. |
| Contenidos | Estancia de 375 horas de duración en una empresa desarrollando funciones relacionadas con la ciberseguridad; tutorización por profesorado del Máster y personal de la empresa. |
| Observaciones | El alumnado puede integrar todas o parte de las competencias adquiridas durante su formación de las demás materias que conforman el título de Máster en Ciberseguridad, de forma que cada estudiante trabajará un conjunto diferente de competencias (ya adquiridas en otras materias), dependiendo de la naturaleza de la práctica que esté realizando en cada empresa determinada. |
| Metodologías docentes (incluir listado) | - Estancia en empresas. |

| Actividades formativas | | |
|---|---|---|
| Denominación de la actividad formativa | Horas | Presencialidad (%) |
| - Estancia en empresas. | 375 | 100 |

| Sistemas de evaluación | | |
|---|---|---|
| Denominación del sistema de evaluación | Ponderación mínima (%) | Ponderación máxima (%) |
| - Informe del profesorado tutor de la empresa | 30 | 70 |
| - Memoria de actividades | 30 | 70 |

| **Prácticas en empresa y trabajo de fin de máster** | **Trabajo de fin de máster** |
|---|---|
| Curso | Segundo |
| ECTS | 15 |
| Carácter | Obligatoria |
| Semestre | Primero |
| Competencias básicas y generales | (CB1) (CB2) (CB3) (CB4) (CB5) (CG1) (CG2) (CG3) (CG4) (CG5) (CG6) |
| Competencias específicas | Todas las del título |
| Competencias transversales | (CT1) (CT3) (CT4) (CT5) |
| Resultados de aprendizaje | • Búsqueda, ordenación y estructuración de información sobre Ciberseguridad.<br>• Elaboración de memoria de proyectos en la que se recojan los aspectos fundamentales del trabajo desarrollado.<br>• Diseño de prototipos, programas de simulación, etc., según especificaciones |
| Contenidos | Trabajo académico a presentar en público que será evaluado por un Tribunal. Puede ser continuación de las prácticas en empresa |
| Observaciones | El alumnado puede integrar todas o parte de las competencias adquiridas durante su formación de las demás materias que conforman el título de Máster en Ciberseguridad, de forma que cada estudiante trabajará un conjunto diferente de competencias (ya adquiridas en otras materias), dependiendo de la naturaleza del TFM que esté realizando. De forma opcional, el alumnado podrá realizar su TFM en el marco de una empresa, en cuyo caso existirá la actividad formativa de Estancia en empresas, cuya presencialidad se detraerá de las horas del trabajo autónomo del alumnado. |
| Metodologías docentes (incluir listado) | Trabajos y/o proyectos; Atención personalizada. |

| Actividades formativas | | |
|---|---|---|
| Denominación de la actividad formativa | Horas | Presencialidad (%) |
| - Trabajos y/o proyectos. | 350 | 0 |
| - Atención personalizada. | 25 | 100 |

| Sistemas de evaluación | | |
|---|---|---|
| Denominación del sistema de evaluación | Ponderación mínima (%) | Ponderación máxima (%) |
| - Rúbrica aprobada por la Comisión Académica del Máster. La evaluación se basará en la decisión del Tribunal nombrado a tal efecto, y tendrá en cuenta la opinión del profesorado tutor. | 100 | 100 |

## 12. EVALUACION

La evaluación de las competencias adquiridas se llevará a cabo en cada asignatura. Esta evaluación podrá realizarse tanto de forma continua, con pruebas que se llevan a cabo a lo largo del curso, como en el formato más tradicional de evaluación concentrada en un examen.

Las pruebas correspondientes a la evaluación continua tendrán una ponderación de, al menos, un 30% de la calificación final. Los contenidos y la organización docente de cada asignatura determinan la ponderación máxima de la evaluación continua, que en muchos casos puede llegar al 100% de la calificación final. La guía docente de cada asignatura, elaborada anualmente, aprobada por las Juntas de Centro, y publicada en la web del Máster previamente al periodo de matriculación, detallará la ponderación exacta de las pruebas de evaluación continua en la calificación final. El resto de la calificación final podrá ser alcanzada mediante el examen final.

Dado que, en cumplimiento de la normativa de la Universidad de Vigo, un alumno que no opte por evaluación continua debe poder optar a la calificación máxima mediante el examen final, en todas las fichas se especifica que el examen final podrá representar entre el 0% (para aquellas asignaturas en las que la evaluación continua pueda suponer el 100% de la nota final) y el 100% de la nota final.

## 13. IDIOMAS

Los idiomas oficiales en la comunidad autónoma de Galicia son el castellano y el gallego, por lo que serían las lenguas propias de la titulación. Además, debido al peso que el inglés tiene en el ámbito de la ciberseguridad a nivel internacional, se pretende que dicho idioma tenga un peso importante en las actividades formativas del Máster. Por ello, se garantiza que:

- Al menos en el 75% del material docente (presentaciones, ejercicios y problemas, manuales de prácticas, trabajos, etc.) y en el 30% de las actividades formativas de todas las asignaturas de la titulación se utilice el idioma inglés, garantizando que al menos dos de las materias obligatorias estén incluidas en dicho porcentaje.

- Y que los estudiantes que posean una certificación de nivel B2 puedan realizar el trabajo de fin de máster en inglés bajo la tutorización de un/a profesor/a acreditado, si así lo desean. Dicha certificación de idioma se les exigirá para la obtención del título y para la expedición del correspondiente certificado de estudios con constancia de haber realizado y defendido el TFM en inglés, e igualmente constará en el Suplemento Europeo al título de los/las titulados/as.

A medida que el número de profesores de las universidades participantes con docencia en la titulación y con la correspondiente certificación de idiomas vaya aumentando, el porcentaje de asignaturas y actividades docentes en inglés podrá aumentar también.

## 14. ITINERARIO A TIEMPO PARCIAL

Los estudiantes a tiempo parcial deberán completar un programa de estudios en tres años académicos, según establece el plan que se detalla a continuación.

- Primer año – primer cuatrimestre: se cursarán 18 ECTS de las materias *Gestión de la seguridad de la información* (6 ECTS), *Seguridad de la información* (6 ECTS) y *Seguridad en comunicaciones* (6 ECTS).

- Primer año – segundo cuatrimestre: se cursarán 13 ECTS compuestos por las materias *Fortificación de sistemas operativos* (5 ECTS), *Conceptos y leyes en la ciberseguridad* (3 ECTS) y *análisis de malware* (5 ECTS).
- Segundo año – primer cuatrimestre: se cursarán los 12 ETS de las materias *Seguridad de aplicaciones* (6 ECTS) y *Redes seguras* (6 ECTS).
- Segundo año – segundo cuatrimestre: se cursarán los 17 ECTS de las materias *Tests de intrusión* (5 ECTS), *Seguridad como negocio* (3 ECTS) y tres materias optativas (en total, 9 ECTS).
- Tercer año – primer cuatrimestre: *Prácticas en empresa* (15 ECTS)
- Tercer año – segundo cuatrimestre: *Trabajo de fin de máster* (15 ECTS)

## 15. COORDINACIÓN

Las labores de coordinación horizontal y vertical serán realizadas por el/la coordinador/a del Máster, por la Comisión Académica del Máster y por los coordinadores de módulo y especialidad (figuras que nombrará anualmente la Comisión Académica). La persona coordinadora del Máster y la Comisión Académica se encargan de que no haya solapamientos entre las asignaturas. Las personas que coordinan los módulos se encargan básicamente de la organización secuencial del contenido de las asignaturas de su módulo y de organizar las actividades docentes en conexión con todos los docentes que participan en ella (coordinación horizontal). Para ello, se reúnen con los profesores de cada asignatura para decidir cómo se va a impartir, para recabar el material necesario, para recopilar los trabajos a realizar durante la evaluación continua y las preguntas para el examen final. Una vez finalizada la asignatura, los coordinadores informan al coordinador/a del Máster y le comunican las posibles incidencias que hayan tenido lugar. Las labores de coordinación vertical (organización entre materias de distintos módulos) corresponden a la Comisión Académica, como órgano de supervisión común de todas las actividades del Máster, y a las personas coordinadoras de los módulos implicados. Puesto que la estructura define 5 módulos, la coordinación vertical resulta efectiva y ágil. Las funciones de coordinación de los distintos módulos estarán convenientemente repartidas entre todos los centros que tomen parte en la docencia del Máster, no siendo imprescindible para la coordinación que las reuniones sean siempre presenciales. Por último, las decisiones de organización práctica del Máster (horarios de aulas, laboratorios, calendarios de exámenes y otras pruebas, conferencias, etc.) se trasladarán a la persona responsable de esta área (jefaturas de estudios) en cada uno de los centros donde se desarrolle la docencia, para poder programarlas debidamente sin interferencia en la vida académica general de estos centros.

Al finalizar cada curso, la Comisión Académica del Máster se reunirá con los coordinadores de módulo para analizar el desarrollo del curso y determinar el grado de cumplimiento de los objetivos. Se analizarán los métodos empleados y los resultados alcanzados, se valorará la necesidad de realizar modificaciones en la organización académica, los sistemas de evaluación utilizados, el profesorado del máster, etc. En base a esta información se fijarán los objetivos para la siguiente edición del máster y las actividades a realizar que conformarán el plan de mejora.

## 16. RESULTADOS PREVISTOS

La estructura del plan de estudios del Máster en Ciberseguridad parte de la experiencia previa en el Máster de Ingeniería de Telecomunicación de la Universidade de Vigo y el Máster Universitario en Ingeniería Informática de la Universidade de A Coruña para intentar ajustar los contenidos al tiempo de trabajo real de los estudiantes, concentrando en el último cuatrimestre el trabajo fin de máster y las prácticas profesionales, sin otra carga lectiva. En cuanto a las normas de permanencia y matrícula, estas prevén la modalidad matrícula a tiempo parcial, con el fin de cubrir las necesidades de los diferentes tipos de

estudiantes, y se ha flexibilizado el número mínimo de créditos que garantizan la permanencia de los estudiantes. Por estos motivos, esperamos cumplir con una tasa de abandono inferior al 20% y una tasa de graduación superior al 70%.

Se ha preferido no incluir las tasas de rendimiento y éxito en las previsiones, pues los datos de la muestra referida contienen másteres con números de matrícula muy heterogéneos.

| Tasas propuestas para el Título | |
|---|---|
| **Denominación** | **Valor (%)** |
| Tasa de graduación | > 70% |
| Tasa de abandono | < 20% |
| Tasa de eficiencia | > 80% |
| Tasa de rendimiento | |
| Tasa de éxito | |

## 17. CALIDAD

La información completa sobre el Manual del Sistema de Garantía Interna de Garantía de Calidad de la Escuela de Ingeniería de Telecomunicación de la Universidad de Vigo, así como el conjunto de procedimientos asociados, se encuentran disponibles a través de este enlace.[1] Toda esta información es accesible para todos los colectivos implicados (estudiantes, personal académico y de administración y servicios, empleadores y sociedad en general) a través de la web de la Escuela (teleco.uvigo.es), siguiendo el menú Escuela -> Calidad.

Los órganos designados para la gestión del Sistema de Garantía Interna de Calidad de la Escuela de Ingeniería de Telecomunicación son: Comisión de Calidad, Coordinador de Calidad, Equipo Directivo y Junta de Titulación/Junta de Escuela

[1] http://teleco.uvigo.es/index.php/es/escuela/calidad