



**Seguridad informática (Máster)**

Edición: 9.a  
Fecha de inicio: 19/10/2011  
Duración: 2 años  
Nro. de créditos: 60 ECTS  
Idioma: Multilingüe

---

La Universitat Oberta de Catalunya (UOC), a través del Instituto Internacional de Posgrado, da un paso más en el liderazgo de la formación continua en línea de calidad, poniendo al alcance de las personas y de las organizaciones y empresas una oferta de programas de reconocido rigor académico, orientada a las necesidades del mundo profesional y con una visión y orientación claramente internacional.

El uso intensivo de las tecnologías de la información y de la comunicación (TIC) en los programas que ofrece el Instituto Internacional de Posgrado de la UOC garantiza a los participantes el conocimiento de las herramientas necesarias para la comunicación y la creación de redes de relación social, que la sociedad de hoy y las personas y las organizaciones que la conforman piden.

El Instituto Internacional de Posgrado tiene una amplia oferta de programas, en formato modular y progresivo, de Formación de Posgrado (Máster, diplomas de Posgrado y especializaciones) acreditados por agencias de calidad y con titulaciones oficiales y propias de la universidad según el caso. Además, cada una de las áreas de conocimiento del Instituto Internacional de Posgrado pone a vuestra disposición una diversa oferta de programas abiertos, accesibles a todo el mundo y de calidad reconocida, además de una oferta de formación a medida específica para las empresas.

La innovación es el eje vertebrador de una oferta educativa que pretende el estímulo de la emprendeduría, y que pone un especial énfasis en la formación de las personas en las competencias que demanda la sociedad actual.

La satisfacción de miles de estudiantes y graduados nos avala. Si quieres, puedes añadirte a la comunidad de nuestra universidad. Te esperamos y contamos con tus aportaciones para continuar construyendo entre todos esta oferta de formación válida y eficaz para todas las personas e instituciones relacionadas

**Josep M.<sup>a</sup> Duart**

Vicerrector de Posgrado y Formación Continua

## Universidad abierta al mundo

---

El uso de internet y el modelo asíncrono facilitan la participación de estudiantes de todo el mundo en los programas de Formación de Posgrado. La dimensión internacional de la universidad se materializa en forma de convenios interuniversitarios, que facilitan la movilidad y la presencia de estudiantes de diversas procedencias geográficas en las aulas, con una serie de características comunes que permiten compartir intereses y enriquecer el aprendizaje.

El perfil de los participantes de Formación de Posgrado se caracteriza por los siguientes rasgos:

- Conocedores y usuarios avanzados de las nuevas tecnologías
- El 12% es de procedencia internacional
- El 81% tiene entre 25 y 45 años
- El 83% trabaja

Más de 20.000 profesionales han realizado diferentes actividades en la programación docente periódica de Formación de Posgrado.

## Máster de Seguridad informática

Actualmente, las organizaciones modernas que operan o centran gran parte de su actividad en el negocio a través de Internet necesitan dotar sus sistemas e infraestructuras informáticas de las políticas y medidas de protección más adecuadas que garanticen el continuo desarrollo y sostenibilidad de sus actividades; en este sentido, cobra especial importancia el hecho de que puedan contar con profesionales especializados en las nuevas tecnologías de seguridad que implementen y gestionen de manera eficaz sus sistemas.

La sociedad de la información y las nuevas tecnologías de comunicación plantean la necesidad de mantener la usabilidad y confidencialidad de la información que soportan los sistemas de sus organizaciones; para ello, es especialmente importante elegir e implantar los sistemas y métodos de seguridad más idóneos, que protejan sus redes y sistemas ante eventuales amenazas, ya sean presentes o futuras.

Dentro de la oferta de formación del área de seguridad informática, el profesional podrá encontrar programas especializados que le aportarán o complementarán sus conocimientos en materia de seguridad informática. Gracias a la diversidad temática de nuestro itinerario de aprendizaje en seguridad informática, el estudiante podrá optar por especializarse en las diferentes tecnologías y conocimientos que le proporcionarán cada uno de nuestros cursos. Los programas de posgrado de Tecnologías de seguridad informática persiguen, como uno de nuestros máximos objetivos, poder convertir al participante en un auténtico experto en seguridad, con lo que pueda hacer frente a una de las profesiones más demandadas y competitivas del mercado laboral actual.

### Una titulación pensada para tu progreso

---

#### Itinerario académico

El máster de Seguridad informática se ha diseñado y estructurado como un itinerario, de manera que permite a los participantes el acceso a una formación lo más ajustada posible a sus necesidades y a matricularse de acuerdo con sus intereses específicos y sus posibilidades de tiempo y dedicación.

Los programas que forman parte del itinerario son los siguientes

#### Máster

- Máster en Seguridad informática

#### Posgrados

- Posgrado en Seguridad técnica: redes, sistemas y aplicaciones
- Posgrado en Sistemas de gestión de la seguridad y análisis forense

La mayor parte de los programas que forman un itinerario académico se inician en noviembre. Para la matrícula hay dos períodos al año, cada uno con una oferta distinta de programas. Llamando al teléfono 902 372 373 pueden conocerse todos los programas previstos y sus períodos de matriculación.

### A quién se dirige

---

Este máster se dirige a titulados universitarios con conocimientos previos sobre sistemas operativos, hardware, software y programación, que necesiten obtener unos conocimientos avanzados sobre seguridad informática.

## Objetivos académicos

---

- Conocer los diferentes tipos de vulnerabilidad que presentan las redes TCP/IP.
- Conocer los principales ataques que puede recibir un sistema informático, así como los posibles métodos de protección, detección y políticas de seguridad que permitan evitar el daño al sistema o minimizar su repercusión.
- Saber configurar la prevención contra los ataques más frecuentes.
- Conocer la configuración experta de los servidores de GNU/Linux.
- Conocer la configuración experta de Windows 2003 Server.
- Saber las técnicas principales de seguridad en los sistemas operativos.
- Conocer el marco normativo de la protección de datos a través de textos normativos.
- Conocer las obligaciones legales respecto a las medidas de seguridad.
- Conocer la legitimación de ficheros y datos, y la jurisdicción que comporta la protección de éstos.
- Conocer la visión completa y actual de la posibilidad de la puesta en marcha del plan de gestión de la seguridad en la empresa para mejorar el entorno de los sistemas informáticos. Abordar modelos de estudio de costes y factibilidad de sistemas informáticos de seguridad.
- Saber identificar y dimensionar amenazas de sistemas informáticos: elaborar planes de contingencia, evaluación/análisis de riesgos, implantación de políticas de seguridad.
- Conocer las ISO de seguridad (27001, 27002Andhellip;).
- Saber hacer una auditoría de seguridad en un sistema informático.
- Saber elaborar un análisis forense de cualquier sistema informático; PC, móviles, routers, etc.
- Saber identificar las vulnerabilidades de las aplicaciones web, proyecto OWASP (Open Web Application Security Project).

## Aplicación profesional

---

Este máster permite obtener conocimientos que se pueden desarrollar en los ámbitos profesionales de:

- Responsable de red informática o responsable de seguridad informática.
- Profesionales, administradores y responsables de áreas de informática y comunicaciones en ámbitos empresariales, comerciales, industriales, académicos y el sector público.
- Profesores, consultores y asesores en las áreas de informática, comunicaciones, sistemas y demás áreas relacionadas con la seguridad de los sistemas y la información.

## Metodología

---

El modelo pedagógico de la UOC se basa en el participante, que trabaja con autonomía, gestionando su tiempo y construyendo su propio itinerario de aprendizaje por medio de la interacción y el trabajo cooperativo.

Mediante el Campus Virtual, se consigue un aprendizaje profundo y flexible, sin barreras de espacio ni de tiempo, desde cualquier lugar y en cualquier momento.

Este modelo permite una atención personalizada por parte de profesionales, docentes y expertos de reconocido prestigio, que acompañan a cada participante de forma individual y al grupo en su conjunto hacia la construcción del nuevo conocimiento.

Los materiales y recursos didácticos incluyen e integran contenidos, aplicaciones prácticas y herramientas directamente relacionadas con el entorno y las actividades laborales concretas. En este programa se utiliza una variada combinación de metodologías, considerando que los participantes son profesionales en activo y que el intercambio de sus propias experiencias profesionales

será un aspecto muy relevante para conseguir los objetivos académicos.

Los participantes que acceden por primera vez al entorno del campus virtual realizarán una formación paralela al inicio del programa docente, basada en un breve curso introductorio para aprender a navegar por el entorno, conocer sus funcionalidades y utilización de los espacios destinados a la comunicación y la docencia.

Si deseas realizar un recorrido virtual por el campus de la UOC, visita <http://www.uoc.edu/presentaciones/campus/>.

## **Materiales**

---

Los cursos de posgrado de la UOC pueden tener material en papel y/o en formato digital. Los materiales se entregan a los estudiantes a medida que avanza el curso

Los cursos de posgrado de la UOC pueden tener material en papel y/o en formato digital. Los materiales se entregan a los estudiantes a medida que avanza el curso.

El material didáctico del posgrado se compone de diferentes módulos didácticos en formato papel.

También se proporcionará al estudiante software de apoyo o complementario en soporte CD para la realización de las prácticas y demás ejercicios de evaluación.

## **Estructura i contenidos del programa**

---

### **Seguridad en redes**

Ataques contra las redes TCP/IP

- Seguridad en redes TCP/IP
- Actividades previas a la realización de un ataque
- Escuchadores de red
- Ataques de denegación deservicio
- Deficiencias de programación

Mecanismos de prevención

- Sistemas cortafuegos
- Construcción de sistemas cortafuegos
- Zonas desmilitarizadas
- Características adicionales de los sistemas cortafuegos

Mecanismos de protección

- Sistemas de autoidentificación
- Protección del nivel de red: IPsec
- Protección del nivel de transporte: SSL/TLS
- Redes privadas virtuales

### Aplicaciones seguras

- El protocolo SSH
- Correo electrónico seguro

### Sistemas para la detección de intrusiones

- Necesidad de mecanismos adicionales
- Sistemas de detección de intrusos
- Escáneres de vulnerabilidad
- Sistemas de detección
- Prevención de intrusiones
- Detección de ataques distribuidos

## **Seguridad en sistemas operativos**

### Introducción a la seguridad

- La seguridad en la empresa
- Modelos y políticas de seguridad

### Administración de servidores

- Análisis de requisitos
- Configuraciones hardware recomendadas
- Listas de compatibilidad de hardware
- Consideraciones software
- Planificación de la instalación
- Sistemas de archivos
- Administración de discos
- Instalación del servidor
- Activación de servicios y protocolos de red
- Protocolos y sistemas de autenticación de usuarios
- Administración y mantenimiento del servidor
- Altas/bajas/modificaciones de usuarios
- Cuotas de disco
- Herramientas básicas

### La seguridad pasiva

- Política de backups
- Planes de contingencia
- Sistemas de recuperación

### La seguridad activa

- Certificados y sistemas de claves públicas y privadas
- IPSEC
- Redes privadas virtuales
- Monitorización de la red
- Herramientas de comprobación

### Configuración de servicios

- Servidores de ficheros e impresoras
- Configuración
- Análisis de riesgos
- Prevención
- Servidor de correo
- Configuración
- Análisis de riesgos
- Prevención
- Servidores web y Ftp
- Configuración
- Análisis de riesgos
- Prevención

### Mantenimiento

- Actualizaciones
- Monitorización de eventos
- Automatización de tareas

### **Aspectos legales**

#### LOPD

- Generalidades
- Principios fundamentales
- Las bases de la protección de datos
- Ficheros de titularidad pública y privada
- Derechos de los interesados
- Infracciones y sanciones
- APD Agencia de Protección de Datos
- Reglamento de medidas de seguridad (¿Qué hay que hacer?)

#### LSSI

- Principios y definiciones
- Obligaciones impuestas
- Resolución de conflictos
- Infracciones y sanciones

### **Sistemas de gestión de la seguridad de la información**

#### Gestión de la seguridad informática

- Seguridad de la información
- Principios de seguridad
- Normativas de seguridad
- Grado de implantación de estas normativas

#### Análisis de riesgos

- Ciclo de vida de la seguridad
- Análisis de riesgos
- Metodologías: MAGERIT, NIST, CRAMM, OCTAVE

#### Sistemas de gestión de la seguridad de la informática

- Normativas de seguridad de la información
- Sistemas de gestión de la seguridad de la información
- Medidas de seguridad: ISO
- Implantación de un SGSI

### **Planes de continuidad de negocio**

- La gestión de la continuidad de negocio
- El BIA, el análisis de riesgos y las estrategias
- Desarrollo de un plan de continuidad
- La gestión operativa del plan de continuidad

### **Auditoría técnica y de certificación**

#### Introducción

#### Tipos de auditorías

#### Auditorías de certificación (SGSI)

- Introducción
- Objetivos
- Fases: documental/presencial/documentación
- Certificación

## Auditoría técnica de sistemas de información

- Objetivos de las auditorías técnicas de seguridad
- Metodologías de auditoría
- Ejecución de auditorías de seguridad
- Herramientas

## **Análisis forense y evidencia digital**

### Introducción

### Recuperación de información

### Análisis forense

### Metodología

- Adquisición de datos
- Análisis e investigación de datos
- Documentación del proceso

### Situación legal

### Ejemplos de aplicación

### Herramientas

## **Programación segura**

### Programación segura de aplicaciones web

- Seguridad en el navegador
- Cómo programar aplicaciones inmunes a SQL injection
- Cómo programar aplicaciones inmunes a Cross Site Scripting
- Prevención de vulnerabilidades LFI y RFI
- Almacenamiento seguro de recursos en servidor
- Autenticación y autorización en aplicaciones multiusuario

### Programación segura de aplicaciones locales

- Prevención de desbordamientos de Stack y Heap
- Prevención de vulnerabilidades de tipo format strings
- Prevención de vulnerabilidades off-by-one
- Prevención de condiciones de carrera
- Programación con mínimos privilegios

### Programación segura de aplicaciones en red

- Criptografía en las comunicaciones

- Almacenamiento de logsremoto
- Programación inmune adenegaciones de servicio

Otros aspectos de la programación

- Manejo seguro decodificación de caracteres internacionales
- Problemas de programaciónespecíficos de algunos lenguajes
- Criptografía general

## **Seguridad en BB. DD.**

Introducción

- Importancia de las basesde datos
- Evolución del mercado
- Evolución de los ataques
- Perspectivas

Principales arquitecturas

- Introducción
- Oracle
- Microsoft SQL
- MySQL
- DB2
- Otros sistemas de basesde datos

Vulnerabilidades

- Introducción
- Inyección SQL
- Inyección SQL ciega
- Inyección de código
- Denegación de servicio
- Desbordamiento debuffer/ejecución de código
- Backdoors y rootkits
- Otros ataques
- Historial de lasprincipales vulnerabilidades

Fortificación

- Introducción
- Servicios
- Permisos, usuarios ycontraseñas

- Tablas Principales
- Procedimientos almacenados
- Criptografía
- Prevención de desastres
- Otros aspectos
- Análisis forense
- Uso de herramientas para la securización

#### Intrusión

- Introducción
- Detección e identificación de objetivos
- Inyección SQL
- Denegación de servicio y desbordamiento de buffer
- Ataques de fuerza sucia
- Ataques internos

#### Desarrollo seguro

- Introducción
- Arquitecturas seguras
- Técnicas básicas de desarrollo seguro
- Busca de problemas al código fuente
- Otras consideraciones

### **Seguridad en aplicaciones web**

#### Arquitectura de aplicaciones web

- Arquitectura en capas
- La capa de presentación
- La capa de negocios
- La capa de datos
- Estándares

#### Ataques a aplicaciones web

- Ataques de inyección de scripts
- Cross-Site Scripting
- Hijacking
- Cross-Site Request Forgery
- Clickjacking
- Ataques de inyección de código

- SQL Injection
- Manipulación de recordset
- Serialized SQL Injection
- Basado en errores ODBC
- Blind SQL Injection
- Time-based BlindSQL Injection
- Arithmetic BlindSQL Injection
- RFD (Remote FileDownloading)
- LDAP Injection
- AND LDAP Injection
- OR LDAP Injection
- Blind LDAP Injection
- Xpath Injection
- Xpath, Xquery
- Blind Xpath Injection
- Ataques de PathTransversal
- Descarga de ficheros
- Ataques de inyección deficheros
- Local File Inclusion
- Remote File Inclusion
- WebShells AndWebtrojans
- Otros ataques aplicaciones web
- Decompiladores Flash,Java y .NET
- Ruptura de sesión
- Fuzzing deaplicaciones web

#### Auditoría y desarrollo seguro

- OWASP (Open Web Application SecurityProject)
- Code Analysis Tools
- Scanners devulnerabilidad de caja negra
- Acunetix
- W3af
- WAF (Web ApplicatonFirewalls)
- ModSecurity

#### **Introducción a la explotación de vulnerabilidades**

#### Gestión de memoria

- Segmentos
- Utilización de la pila

#### Ejecución de procesos

- Espacio de usuario/sistema
- Llamadas a funciones

#### Conceptos básicos de lenguaje máquina

#### Herramientas

- Debuggers
- Syser (Reemplazo SoftICE- Windows)
- OllyDbg (Windows)
- RR0D (Debugger multiplataforma)
- Fenris (Linux)
- Compiladoras/Lenguajes
- C
- Ensamblador

#### Exploits

- Locales/Remotos
- Alteraciones básicas
- Integer overflow
- Static data overflow
- Heap overflow
- Buffer overflow
- Shellcodes
- Escalada de privilegios
- Detección y/o protección de ataques
- Dependencias con sistemas operativos

### **Administración de Programa**

---

**null**  
null

## Requisitos de admisión

---

Para acceder al programa, es necesario disponer de **una titulación universitaria legalizada**. En el caso de no tenerla, un comité de admisión valorará los conocimientos y la experiencia de solicitudes a partir de su curriculum.

## Conocimientos Previos

---

Para la parte de redes:

- Se requieren conocimientos básicos de redes: estructura paquete IP, nociones de comunicaciones entre ordenadores, etc.
- También se debe conocer, a nivel de usuario, el sistema operativo Linux.

Para la parte de sistemas operativos:

- Se requieren conocimientos básicos de administración de Windows, de Linux a nivel de usuario avanzado y de redes y protocolos de redes (SMTP, Samba, DHCP, SSH, HTTP).

## Titulación

---

Una vez superado el proceso global de evaluación, la UOC otorgará un **Diploma de Máster de Seguridad Informática** a los participantes que acrediten una titulación universitaria legalizada en España.

En el caso de no disponer de esta titulación, se expedirá un **Certificado en Seguridad Informática**.

## Sistema de evaluación

---

La evaluación del proceso de aprendizaje es continua y se centra mayoritariamente en trabajos que facilitan la integración del conocimiento y la adquisición de competencias para la praxis profesional de cada estudiante.

Si deseas más información sobre el sistema de evaluación no dudes en ponerte en contacto con nuestros asesores formativos en el 902 372 373 o enviando un correo a [infofp@uoc.edu](mailto:infofp@uoc.edu).

## Matrícula

---

El importe de la matrícula es de: 4.200 euros

El precio de este programa se deberá confirmar en el momento de formalizar la inscripción.

## Otras ventajas

---

El Club de Graduados y Antiguos Estudiantes de la UOC representa la continuidad del concepto de comunidad universitaria con adscripción voluntaria durante los periodos en que no se está matriculado.

El Club UOC se centra en ofrecer servicios, recursos y actividades en el ámbito de la progresión personal y profesional. Los principales ejes de actuación son la proyección profesional, el aprendizaje no formal o postformación, la cultura, el ocio, las relaciones y los intercambios de experiencias y conocimientos.

Además de:

Biblioteca Virtual, conexión con las principales bibliotecas del mundo y disposición de extensos servicios de consulta. Cooperativa Virtual, ser socio de la cooperativa permite disfrutar de sus servicios de librería y material informático. Espacios virtuales de comunicación, en dónde se facilita la relación con otros participantes y profesionales mediante los foros y chats del Campus.

## Información y matrícula

---

Si deseas conocer más detalles sobre los programas de posgrado puedes contactar con nuestros asesores formativos en:

- El teléfono 902 372 373
- Enviando un correo a [infofp@uoc.edu](mailto:infofp@uoc.edu)
- Dirigiéndote personalmente a cualquiera de las Sedes de la UOC.
  - Madrid  
Plaza de las Cortes, 4  
28014 Madrid
  - Sevilla  
C/ Virgen de Luján, 12  
41011 Sevilla
  - Valencia  
C/ Paz, 3  
46003 Valencia
  - Barcelona  
Rambla de Catalunya, 6, plantas 1 y 2  
08907 Barcelona
  - México, D.F.  
Paseo de la Reforma, 265, Piso 1  
Col. Cuauhtémoc  
06500 México, D.F.  
Horarios: de lunes a viernes de 9 a 19h  
Teléfono: + (52 55) 55 11 42 25

Además la UOC facilita a empresas, instituciones y colectivos una interlocución directa y ágil, y unas condiciones preferentes en la matrícula de sus profesionales.

Para más información:  
[matriculacorporativa@uoc.edu](mailto:matriculacorporativa@uoc.edu)

Los programas de formación que figuran en este documento están disponibles en modalidad in company.

Para más información:

[incompany@uoc.edu](mailto:incompany@uoc.edu)

Nota: La información que contiene este PDF es a título informativo. Su vigencia se deberá contrastar en el momento de formalizar la inscripción.