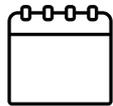


# Máster en **Diseño y Desarrollo Seguro de Software**

- 1ª ED. CLASES ONLINE EN DIRECTO -



Inicio  
07/11/2023



9 meses



Clases  
online en  
directo



Bolsa de  
empleo

# Máster en **Diseño y Desarrollo Seguro de Software**

**online**   
EN DIRECTO

**- 1ª ED. CLASES ONLINE EN DIRECTO -**

## **Descubre el Máster en Diseño y Desarrollo Seguro de Software**

---

La **ciberseguridad** ha adquirido una relevancia sin precedentes. Ataques constantes a los sistemas básicos de nuestra sociedad y el crecimiento exponencial de amenazas cibernéticas, hace que **proteger la información y la privacidad** se haya vuelto fundamental.

**No basta** con tener un **software funcional y eficiente**, sino que también es **imprescindible** contar con una **base sólida de seguridad**. Un software atractivo pero vulnerable puede ser el blanco perfecto para ataques maliciosos, poniendo en riesgo datos sensibles y la integridad de sistemas enteros. La **conjunción de un software de calidad con una base de seguridad robusta** se convierte en una pieza clave para salvaguardar tanto los intereses de los usuarios como los de las empresas.

El **Máster en Diseño y Desarrollo Seguro de Software** te dotará de las competencias necesarias para aplicar **los modelos y técnicas más actuales en desarrollo seguro**.

Empezarás aprendiendo a **programar desde cero** y, posteriormente, te enfocarás en el **desarrollo seguro aplicado** en áreas, como **aplicaciones, web, IoT, seguridad en redes y entornos cloud**.

Con un enfoque **100% práctico**, el programa será **impartido por profesionales expertos** y referentes en el sector de la ciberseguridad y el desarrollo seguro de software desde la práctica.

Al finalizar el máster, **estarás preparado para enfrentar desafíos reales en el ámbito de la seguridad informática**.

# Objetivos

1. Aprenderás tanto fundamentos como nivel avanzado de programación, seguridad e integración de esta última en todas las fases de SDLC.
2. Sabrás cómo crear un software atractivo habiendo pensado en la seguridad en todas sus fases de diseño e implementación. Y aprenderás a detectar amenazas y vulnerabilidades tanto en tu código como en código ajeno auditado
3. Estudiarás criptografía con un enfoque práctico y analizarás cómo integrarla en las comunicaciones y almacenamiento de datos de tu software. Además, conocerás los diferentes algoritmos de cifrado relevantes, cómo implementarlos y tener pleno control sobre los flujos de información en, desde y hacia tu software
4. Averiguarás cómo detectar y corregir errores tanto de seguridad como en la construcción de software
5. Controlarás la seguridad en todas las fases del desarrollo de software, averiguando cómo integrar tu software en los procesos de gestión de incidentes, realizar auditorías incluyendo pentesting de software y adaptar tu trabajo a los diferentes marcos legislativos actuales alrededor del mundo
6. Descubrirás cómo crear software seguro en todo el ciclo de producto, desde el cloud a dispositivos IoT, a nivel hardware y sensores, partiendo de una arquitectura robusta y creando en ambos niveles infraestructuras seguras.

# Requisitos técnicos

Para este programa, es importante contar con un ordenador que sea lo suficientemente potente para manejar diversas tareas, como ejecutar entornos de desarrollo, ejecutar máquinas virtuales para pruebas de seguridad, análisis de datos y codificación en general.

Por eso te recomendamos tener una configuración de hardware que sería adecuada para llevar a cabo este máster:

- Procesador (CPU): Un procesador de al menos cuatro núcleos, tal como Intel Core i5 o superior, o AMD Ryzen 5 o superior.
- Para tareas más intensivas, un Core i7, Ryzen 7 o equivalentes podrían ser útiles.
- Memoria (RAM): Un mínimo de 16 GB de RAM. Para ejecutar múltiples máquinas virtuales al mismo tiempo.
- Sistema Operativo: Una copia genuina de Windows 10 o más reciente o una distribución de Linux como Ubuntu, Kali Linux o Debian.
- Conectividad: Asegúrate de que tu computadora tiene capacidades de conectividad robustas, incluyendo Wi-Fi y Ethernet. La capacidad de conexión con cable puede ser importante en algunas pruebas de seguridad.
- Si tienes un Mac, es importante que verifiques que puedes abrir máquinas virtuales.

Ten en cuenta que para poder seguir el curso y realizar los ejercicios prácticos es necesario disponer de un ordenador en el que cuentes con todos los permisos de administración que le permitan instalar los programas que se utilizarán durante las clases.

## Perfil del alumno

---

El **Máster en Diseño y Desarrollo de Software** está diseñado para personas que cuenten con **un perfil técnico**. Ya sea tu área la programación, la ciberseguridad u otra área técnica, te recomendamos algunos **conocimientos previos** que te resultarán útiles para:

- **Disposición para aprender a programar:** No es necesario tener experiencia previa en programación, pero tendrás que estar dispuesto a aprender y desarrollar habilidades de programación durante el curso del programa. La programación es una habilidad esencial en la seguridad informática y en el desarrollo de software seguro. El programa te proporcionará la formación necesaria para aprender a programar.
- **Conocimientos básicos de Linux y/o Windows:** Estar familiarizado con uno o ambos de estos sistemas operativos será de ayuda. Muchas de las actividades y proyectos del programa implicarán trabajar dentro de estos entornos.
- **Entender las infraestructuras TIC:** Deberías tener una comprensión básica de lo que es un servidor, cómo funcionan las aplicaciones y cómo estas y otras tecnologías se integran para formar una infraestructura de tecnología de la información.

No obstante, el programa está diseñado para ser accesible y comprensible si aún no tienes estos conocimientos. Los profesores te ofrecerán instrucción y apoyo para ayudarte a lo largo del camino.

# Salidas profesionales

---

Al finalizar el máster, estarás preparado para trabajar como:

- **Ingeniero de Software de Seguridad:** Desarrolla aplicaciones y sistemas seguros, implementando prácticas de codificación segura y pruebas de penetración para identificar vulnerabilidades.
- **Arquitecto de Seguridad de Software:** Diseña estructuras de software seguras, y guía a los equipos de desarrollo para implementar la seguridad en todas las fases del desarrollo de software.
- **Analista de Seguridad de Aplicaciones:** Encuentra y corrige vulnerabilidades en las aplicaciones ya existentes.
- **Consultor de Seguridad de Software:** Asesora a las empresas en términos de buenas prácticas de seguridad de software, análisis de riesgos, cumplimiento de regulaciones, y mejora continua.
- **Gerente de Proyecto de Seguridad de Software:** Lidera equipos de desarrollo para garantizar que todos los aspectos de la seguridad se aborden durante el ciclo de vida del desarrollo del software.
- **Especialista en Pruebas de Penetración (Pen Tester):** Realiza pruebas activas en sistemas y redes para encontrar vulnerabilidades que podrían ser explotadas por los atacantes.
- **Auditor de Seguridad de TI:** Examina los sistemas y las prácticas de una organización para asegurar que cumplan con las políticas y normas internas y externas.

## Modalidad Online

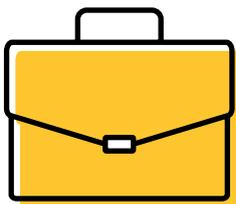
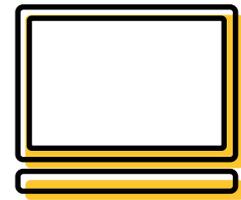
### Lo mejor de nuestro presencial, ahora desde casa

El formato Online te permitirá vivir la experiencia presencial, desde tu casa: un profesor/a se conectará en directo para impartir su clase y responder preguntas y proponer ejercicios prácticos. Será como estar en KSchool pero desde la silla de tu escritorio.



**CLASES EN DIRECTO** en horario entre semana.  
+  
**CLASES GRABADAS**, ¡para que no te pierdas nada!

ACCESO AL **CAMPUS VIRTUAL** para ver las clases y consultar material adicional, grabaciones y ejercicios.



ACCESO VITALICIO A LA **BOLSA DE EMPLEO** de KSchool.  
+  
INVITACIÓN A **EVENTOS EXCLUSIVOS** solo para alumnos.

Te esperamos en clase para que puedas aprender de la mano de los mejores profesores.

¿Estás preparado para convertirte en el mejor hacker ético? Elige tu futuro, ¡qué nosotros te ayudamos a llegar a él!

# Temario

## 01. FUNDAMENTOS DE DESARROLLO DE SOFTWARE

- Fundamentos de desarrollo de software
- Introducción a la programación
- Introducción a la programación orientada a objetos (OOP)
- Desarrollo de aplicaciones web
- Desarrollo de aplicaciones móviles
- Pruebas y calidad de software
- DevOps y desarrollo continuo
- Arquitectura de software y diseño de sistemas

## 02. FUNDAMENTOS DE LA SEGURIDAD INFORMÁTICA

- Introducción a la seguridad informática
- Seguridad física
- Conceptos básicos de red y seguridad de red
- Seguridad de Internet
- Seguridad en redes inalámbricas
- Criptografía
- Defensa en profundidad
- Gestión de incidentes y recuperación ante desastres
- Evaluación de seguridad y pruebas de penetración

## 03. CRIPTOGRAFÍA

- Introducción a la criptografía
- Conceptos básicos de la criptografía
- Tipos de criptografía
- Criptografía de clave pública (PKI)
- Hashes criptográficos y funciones de hash
- Firmas digitales y Autenticación
- Protocolos criptográficos
- Criptografía en aplicaciones prácticas
- Temas avanzados en criptografía

## **04. SEGURIDAD EN LA ARQUITECTURA Y DESARROLLO DE SOFTWARE**

- Introducción a la seguridad de la programación
- Conceptos básicos de seguridad en la programación
- Buenas prácticas en la programación
- Principales amenazas y vulnerabilidades en la programación
- Protección contra las amenazas y vulnerabilidades comunes
- Análisis de seguridad del código
- Avanzado en la programación segura
- Pruebas de seguridad del software
- Integración de la seguridad en el ciclo de vida del desarrollo de software (SDLC)

## **05. SEGURIDAD DE REDES Y COMUNICACIONES**

- Fundamentos de redes
- Introducción a la seguridad de redes
- Herramientas y técnicas básicas de seguridad de redes
- Seguridad en redes inalámbricas
- Seguridad en protocolos de red
- Monitoreo y detección de intrusiones
- Segmentación de Redes
- Criptografía en las comunicaciones de red
- Casos prácticos y conclusiones

## **06. DESARROLLO SEGURO DE APLICACIONES WEB**

- Introducción a la Seguridad Web
- Principios Básicos de la Seguridad en Aplicaciones Web
- Cross-Site Scripting en web (XSS)
- Cross-Site Request Forgery en web (CSRF)
- Inyección SQL
- Otras amenazas y contramedidas
- Mejores Prácticas para el Desarrollo Seguro
- Seguridad en el lado del servidor
- Seguridad en el lado del cliente
- Herramientas de Pruebas de Seguridad Web
- DevSecOS
- Seguridad en APIs
- Seguridad en Aplicaciones Web de Una Sola Página (SPA)
- Controles de Seguridad Avanzados

## **07. DESARROLLO SEGURO DE APLICACIONES MÓVILES**

- Introducción al Desarrollo de Aplicaciones Móviles
- Fundamentos de Seguridad en Aplicaciones Móviles
- Diseño Seguro Autenticación y Autorización Segura
- Almacenamiento Seguro de Datos
- Seguridad en la Comunicación
- Testing y Auditoría de Seguridad
- Protección contra Vulnerabilidades Específicas
- Respuesta a Incidentes de Seguridad

## **08. DESARROLLO SEGURO PARA IOT (INTERNET DE LAS COSAS)**

- Introducción al internet de las cosas (IoT)
- Arquitectura de sistemas IoT/Embebidos
- Diseño seguro de IoT
- Comunicaciones seguras en IoT
- Almacenamiento y procesamiento seguro de datos
- Gestión segura de dispositivos IoT
- Análisis y pruebas de seguridad en IoT
- Uso de dispositivos IoT para Red Team y pentesting
- Normativas y estándares de seguridad en IoT

## **09. SEGURIDAD EN EL DESARROLLO DE SISTEMAS EN LA NUBE**

- Introducción a la computación en la nube
- Fundamentos de seguridad en la nube
- Diseño seguro en la nube
- Gestión de identidad y acceso (IAM)
- Seguridad de datos en la nube
- Monitoreo y detección de amenazas en la nube
- Cumplimiento y auditoría en la nube
- Recuperación de desastres y continuidad de negocio

## **10. EVALUACIÓN DE SEGURIDAD Y PENTESTING**

- Introducción a la evaluación de la seguridad y al pentesting
- Principios básicos de la evaluación de la seguridad y del pentesting
- Herramientas y técnicas básicas para el pentesting
- Evaluación de la seguridad en sistemas y aplicaciones
- Automatización de pruebas y gestión de vulnerabilidades
- Evaluación de la seguridad en entornos específicos
- Técnicas avanzadas de pentesting
- Análisis forense y respuesta a incidentes
- Temas avanzados en evaluación de seguridad

## 11. GESTIÓN DE INCIDENTES DE SEGURIDAD

- Introducción a la gestión de incidentes de seguridad
- Principios básicos de la gestión de incidentes de seguridad
- Preparación para la gestión de incidentes de seguridad
- Respuesta a incidentes de seguridad
- Herramientas y técnicas para la gestión de incidentes de seguridad
- Comunicación durante la gestión de incidentes
- Análisis post-incidente
- Mejora de la gestión de incidentes de seguridad
- Temas avanzados en la gestión de incidentes de seguridad

## 12. GESTIÓN DE LA SEGURIDAD Y CUMPLIMIENTO

- Introducción a la seguridad en el desarrollo de sistemas de Cloud y móviles
- Principios básicos de seguridad en la nube
- Principios básicos de seguridad en el desarrollo de aplicaciones móviles
- Seguridad en el desarrollo de sistemas de cloud Seguridad en el desarrollo de aplicaciones móviles Cumplimiento y auditoría en sistemas de cloud y móviles
- Temas avanzados en seguridad en la nube
- Temas avanzados en seguridad en el desarrollo de aplicaciones móviles
- Gestión de incidentes y respuesta a amenazas en sistemas de cloud y móviles

## Trabajo Fin de Máster

El TFM se basará en un firmware custom compilado basado en OpenWrt que establecerá comunicación con una API alojada en AWS, permitiendo a los usuarios registrados encender y apagar el LED mediante un frontend web o una aplicación móvil.

Será evaluado por cada profesor y la nota final será la ponderación de las notas otorgadas por cada docente.

El TFM no exige presentación en público ni tribunal y la corrección al alumno se entregará en un único feedback que unificará el criterio de los profesores, las notas obtenidas y la media de las mismas.

# Metodología de evaluación

---

En cada clase, se impartirá contenido teórico seguido de ejercicios prácticos, para afianzar el conocimiento mientras “aprendes haciendo”.

Al concluir cada módulo, realizarás una práctica final que será evaluada y te para reforzar lo aprendido en clase.

Recibirás feedback en todos los trabajos para identificar áreas de mejora y perfeccionar tus habilidades de cara al trabajo final.

# Herramientas

Durante el curso se utilizarán herramientas cloud, IDEs, herramientas de auditoría y monitorización:



SonarQube



Fortify



OWASP ZAP



Burp Suite



Snyk



OWASP's SAMM



OpenVAS



Docker



AWS



Splunk



OpenWrt



BuildRoot



DeviceTree



VirtualBox



VMWare



Ubuntu



Linux

# Profesores

**Directora del Máster en Diseño y Desarrollo Seguro de Software**



**Gabriela García**

Secure Software Dev | Speaker | Coding & CyberSec Instructor



**Antonio Juanilla aka Specter**

DevSecOps(SecDevOps) professional  
AppSec Bro | HackMadrid -  
flagHunters - HackBarcelona -  
HackerDreams A



**David Meléndez Cano**

I+D Engineer | R&D Embedded  
Software | DEFCON USA Speaker,  
BlackHat | Maker | Book author:  
"Hacking con Drones"

\* El claustro de profesores puede sufrir modificaciones.

# Inscripción y precio

## 1º. RESERVA DE PLAZA

500 €

## 2º. OPCIONES DE PAGO

Pago único  
**-5% de descuento**

Ponemos a tu disposición las mejores alternativas para **financiar** el importe total de la formación. ¡Tú eliges!

Desde KSchool te ofrecemos dos opciones de financiación



Hasta 12 cuotas  
**sin intereses\***

¿Necesitas más tiempo?  
Estudiaremos tu situación de forma **personalizada** para encontrar la solución más adecuada.

\*Hasta 12 cuotas sin intereses: financiación a medida según el perfil crediticio del alumno. El 100% de las cuotas deberán de estar abonadas 30 días antes de la finalización del máster. El número de cuota se adapta a 30 días antes de la finalización, al perfil crediticio y según la fecha de contratación.

## Bonificable con FUNDAE

Todos nuestros cursos son bonificables a través de la **Fundación Estatal para la Formación en el Empleo** (FUNDAE, antigua FUNDACIÓN TRIPARTITA).

Si estás interesado coméntanoslo al hacer tu inscripción. Desde KSchool nos encargamos de la gestión para cursos o másteres de más de 60 horas.

Si nuestros planes de financiación o becas no se ajustan a tu situación, ¡escríbenos!

En KSchool **tratamos cada caso de forma personalizada**. Queremos que te formes con nosotros.

## Bolsa de Empleo

En KSchool contamos con una Bolsa de Empleo propia donde las mejores empresas buscan talento.

Nos enorgullece decir que el 96% de nuestros alumnos están trabajando y que muchos de ellos consiguieron su primer empleo en el sector digital o lograron cambiar su puesto gracias a la Bolsa de Empleo.

Pero, ¿**cómo funciona** esta Bolsa de Empleo?

1. Tienes que ser alumno de KSchool
2. Entra a la plataforma y consulta las nuevas ofertas (becas o empleos, siempre remunerados). Solo recibirás las que vayan dirigidas a tu área de formación. ¡Todo bien filtrado para que solo te lleguen las ofertas de empleo que de verdad te interesan!
3. Aplicas a la oferta y si todo va bien...
4. La empresa te contactará para que hagas una entrevista y puedas formar parte de su proceso de selección.
5. Este es el punto que más nos gusta: cuando os eligen para cubrir su vacante y nos escribís para contarnoslo :) ¡Es genial cada vez que un/a KSchoolero/a nos dice que tiene un nuevo trabajo gracias a la Bolsa de Empleo!

## Eventos y networking

Además de poder aprender mucho en clase, desde KSchool os invitamos a eventos, masterclass, talleres y conferencias que os servirán para ampliar vuestros conocimientos y para contactar con grandes profesionales.

Síguenos a través de las redes sociales para estar al tanto de estas acciones y revisa tu mail. ¡Algunos de nuestros eventos son exclusivos para alumnos!

# Preguntas frecuentes

Para resolver cualquier duda podéis escribirnos a [admisiones@kschool.com](mailto:admisiones@kschool.com) o llamarnos al **91 910 09 54**, pero a continuación recogemos algunas de las preguntas que más nos hacéis. ¡Esperamos que os sean de ayuda!

## ¿Qué diferencias hay entre la modalidad presencial y Online?

La principal, el formato presencial requiere que acudas a clase, por lo que solo podrás cursarla si estás en Madrid o Barcelona, y siempre que tengas disponibilidad los viernes por la tarde y sábados por la mañana.

El formato Online es para todos aquellos que tengan una buena conexión a internet, ya sea desde Granada, Teruel o Cuenca. Las clases se imparten entre semana a partir de las 18:30 horas.

## ¿Qué pasa si no puedo acudir a una clase?

En la modalidad Online las clases quedan grabadas, ¡así que podrás verla en cualquier otro momento!

## ¿Para qué sirve el Campus Virtual?

Desde Campus Virtual podrás acceder a las clases en directo y volver a ver las grabaciones. Encontrarás ejercicios y materiales complementarios para que puedas mejorar tus habilidades y conocimientos. Además, también tendrás acceso a las presentaciones que los profesores utilizarán en sus clases y podrás comunicarte con tus compañeros y profesores para resolver dudas a través de los foros que se incluyen en él.

## ¿Hay exámenes?

¡No! Durante las clases realizaréis ejercicios prácticos y en la plataforma virtual podréis seguir practicando para adquirir los conocimientos necesarios para superar el máster.

## ¿Necesito un título universitario para cursar un máster en KSchool?

No, no necesitas ningún título previo. Existen formaciones donde si es necesario contar con unos conocimientos básicos, pero no te preocupes por esto ya que antes de realizar la reserva te preguntaremos por tu preparación previa y si fuese necesario te solicitaríamos el CV. ¡Queremos que aproveches al máximo tu paso por KSchool!

# Los números de KSchool

Nacimos en 2011 con una idea en la cabeza: formar a los nuevos perfiles profesionales que la red demanda de forma constante y hacerlo de la mejor forma posible. Por ello, nos definimos como “La escuela de los profesionales de Internet”.

La experiencia y los grandes profesionales con los que contamos como profesores nos avalan. Como siempre decimos, en ciertos sectores a día de hoy, el valor no lo aporta un título si no lo que el profesional sabe hacer.

**DESDE 2011**

FORMANDO  
PERFILES

**+6.000**

**ALUMNOS**  
HAN PASADO  
POR NUESTRAS  
AULAS

**3**

**MODALIDADES**  
DE FORMACIÓN:  
PRESENCIAL,  
ONLINE E  
HÍBRIDA

**+20**

**PROGRAMAS**  
¡PARA QUE  
ELIJAS TU  
FUTURO!

**+60**

**EDICIONES**  
EN ALGUNOS  
DE NUESTROS  
PROGRAMAS

**+ 1.600**

**EMPRESAS**  
HAN BUSCADO  
TALENTO EN  
NUESTRA BOLSA DE  
EMPLEO

Tenemos **experiencia**, los mejores y más actualizados **programas de formación**, y a los **profesionales** más reconocidos del sector impartiendo clases en nuestras aulas.

# Manifiesto

- Si el sistema no está preparado para darnos el conocimiento que necesitamos lo vamos a conseguir por nuestra cuenta.
- Hoy, en ciertos sectores el valor no lo aporta un título. Lo aporta lo que cada profesional sabe hacer.
- Si dependemos de nosotros mismos, vamos a pensar por nosotros mismos.
- No queremos, ni podemos sentarnos a esperar a que alguien se fije en nosotros.
- No hay ningún mapa. Debemos hacer nuestro camino, y es un camino que muchas veces no ha sido explorado, pavimentado, ni señalizado.
- Nuestro conocimiento es la clave de nuestro desarrollo personal y profesional.
- Todo el mundo tiene algo que enseñar. Queremos aprender todos de todos.
- En el mundo del conocimiento, cuanto más se comparte más se tiene.
- Lo que aprendemos es lo que practicamos.
- Especializarse es ponerle un apellido a nuestra profesión. Es echarle especias a nuestro ingrediente principal.
- Queremos construirnos un futuro fuera del rebaño. Para eso vamos a pensar y hacer las cosas de forma diferente.
- No vamos a seguir instrucciones a ciegas, no vamos a ser pelotas, no vamos a mantener la cabeza agachada. Esas formas no van con nosotros.
- Vamos a estar siempre en movimiento. No vamos a parar de movernos. Somos inquietos, y nos gusta ser así.
- Como queremos resultados diferentes, vamos a hacer las cosas de forma diferente.
- Las pirámides son monumentos funerarios. Nos divierte verlas en los libros de historia, no sufrirlas en nuestro trabajo.
- Nuestro mercado no es el de los empleos. Es el de las oportunidades.
- Queremos colaborar con nuestras empresas a generar ingresos, no queremos tener un simple empleo.
- Queremos avanzar elaborando mejores recetas, no cocinando más.
- Queremos poner vida a los años, no solo años a la vida.
- Somos mucho más que un perfil y unas competencias. Somos algo más que las hojas de nuestro CV.
- Queremos levantarnos con ilusión los próximos 40 años. Queremos hacer las cosas con pasión, cariño y humanidad.

# Contacto

---

No te quedes con ninguna duda, estamos aquí para ayudarte. Llámanos o escríbenos y tendremos una conversación personalizada contigo, ¡nos encanta conoceros!

## INFORMACIÓN KSCHOOL

✉ [admisiones@kschool.com](mailto:admisiones@kschool.com)

☎ 91 910 09 54