



CURSO



Curso Práctico en
**Gestión y Herramientas
de Ciberseguridad**



INEAF
BUSINESS SCHOOL

INEAF Business School



Índice

Curso Práctico en **Gestión y Herramientas de Ciberseguridad**

1. Historia
2. Titulación Curso Práctico en Gestión y Herramientas de Ciberseguridad
[Resumen](#) / [A quién va dirigido](#) / [Objetivos](#) / [Para que te prepara](#) / [Salidas Laborales](#) / [INEAF Plus](#)
3. Metodología de Enseñanza
4. Alianzas
5. Campus Virtual
6. Becas
7. Claustro Docente
8. Temario Completo



Historia

Ineaf Business School



En el año 1987 nace la primera promoción del Máster en Asesoría Fiscal impartido de forma presencial, a sólo unos metros de la histórica Facultad de Derecho de Granada. Podemos presumir de haber formado a profesionales de éxito durante las 27 promociones del Máster presencial, entre los que encontramos abogados, empresarios, asesores fiscales, funcionarios, directivos, altos cargos públicos, profesores universitarios...

El Instituto Europeo de Asesoría Fiscal INEAF ha realizado una apuesta decidida por la innovación y nuevas tecnologías, convirtiéndose en una Escuela de Negocios líder en formación fiscal y jurídica a nivel nacional.

Ello ha sido posible gracias a los cinco pilares que nos diferencian:

- **Claustro** formado por profesionales en ejercicio.
- **Metodología y contenidos** orientados a la práctica profesional.
- **Ejemplos y casos prácticos** adaptados a la realidad laboral.
- **Innovación** en formación online.
- **Acuerdos** con Universidades.



Curso Práctico en Gestión y Herramientas de Ciberseguridad

DURACIÓN	50 H
PRECIO	199 €
MODALIDAD	Online

Entidad impartidora:

INEAF - Instituto Europeo de Asesoría Fiscal



Programa de Becas / Financiación 100% Sin Intereses

Titulación Curso Práctico

- Titulación expedida por el Instituto Europeo de Asesoría Fiscal (INEAF), avalada por el Instituto Europeo de Estudios Empresariales (INESEM) "Enseñanza no oficial y no conducente a la obtención de un título con carácter oficial o certificado de profesionalidad."



Resumen

La aparición de modelos de negocio online ha ido aumentando hasta la actualidad, donde son cada vez más las empresas que se han subido a la ola de la digitalización. El intercambio de información o datos en estas webs ha generado la necesidad de contratar perfiles expertos en auditar, evaluar y detectar aquellas fugas de información que son trascendentales para la viabilidad de las empresas. Con el Curso en Gestión y Herramientas de Ciberseguridad te convertirás en el profesional cualificado que todas las empresas digitales demandan.

A quién va dirigido

Los profesionales de la informática son los más interesados en el Curso en Gestión y Herramientas de Ciberseguridad siendo esta formación una especialización dentro de su carrera profesional. También es demandado por aquellos estudiantes o titulados universitarios que desean profundizar en el área de la ciberseguridad, y acceder a los puestos más demandados en el mercado laboral.

Objetivos

Con el Curso Práctico en **Gestión y Herramientas de Ciberseguridad** usted alcanzará los siguientes objetivos:

- Concienciar de la importancia de la seguridad de la formación a través del análisis de los factores de riesgo.
- Estudiar la normativa nacional e internacional sobre el sistema de gestión de la seguridad de la formación y los estándares comunitarios.
- Diseñar un plan de sistema de gestión de la seguridad de la formación a través del análisis exhaustivo y la gestión de los riesgos.
- Elaborar una auditoría con el uso de herramientas como Traceroute, Nmap, Nessus, WireShark, Acunetix o John the Ripper entre otras.
- Establecer protocolos de seguridad por niveles.
- Conocer la influencia de la Ley de Protección de Datos en la gestión de la ciberseguridad.





¿Y, después?

INEAF *Plus*. Descubre las ventajas

SISTEMA DE CONVALIDACIONES INEAF

La organización modular de nuestra oferta formativa permite formarse paso a paso; si ya has estado matriculado con nosotros y quieres cursar nuevos estudios solicita tu plan de convalidación. No tendrás que pagar ni cursar los módulos que ya tengas superados.

ACCESO DE POR VIDA A LOS CONTENIDOS ONLINE

Aunque haya finalizado su formación podrá consultar, volver a estudiar y mantenerse al día, con acceso de por vida a nuestro Campus y sus contenidos sin restricción alguna.

CONTENIDOS ACTUALIZADOS

Toda nuestra oferta formativa e información se actualiza permanentemente. El acceso ilimitado a los contenidos objeto de estudio es la mejor herramienta de actualización para nuestros alumno/as en su trabajo diario.

DESCUENTOS EXCLUSIVOS

Los antiguos alumno/as acceden de manera automática al programa de condiciones y descuentos exclusivos de INEAF Plus, que supondrá un importante ahorro económico para aquellos que decidan seguir estudiando y así mejorar su currículum o carta de servicios como profesional.



OFERTAS DE EMPLEO Y PRÁCTICAS

Desde INEAF impulsamos nuestra propia red profesional entre nuestros alumno/as y profesionales colaboradores. La mejor manera de encontrar sinergias, experiencias de otros compañeros y colaboraciones profesionales.

NETWORKING

La bolsa de empleo y prácticas de INEAF abre la puerta a nuevas oportunidades laborales. Contamos con una amplia red de despachos, asesorías y empresas colaboradoras en todo el territorio nacional, con una importante demanda de profesionales con formación cualificada en las áreas legal, fiscal y administración de empresas.

SALIDAS LABORALES

- Director en ciberseguridad.- Director de Seguridad de la información.- Director de Seguridad Corporativa.- Auditor en ciberseguridad.- Consultor especializado en seguridad de la información.

¿PARA QUÉ TE PREPARA?

El Curso en Gestión y Herramientas de Ciberseguridad te prepara para que afrontes la ciberseguridad de una empresa desde una triple perspectiva: la detección de los ciberataques a través de la elaboración de una auditoría, la gestión de la seguridad y la evaluación de los sistemas de gestión de la seguridad. Una formación con la que alcanzar puestos de trabajo en áreas tan demandadas como la arquitectura de sistemas, dirección de proyectos de ciberseguridad o consultor de seguridad.

En INEAF ofrecemos oportunidades de formación sin importar horarios, movilidad, distancia geográfica o conciliación.

Nuestro método de estudio online se basa en la integración de factores formativos y el uso de las nuevas tecnologías. Nuestro equipo de trabajo se ha fijado el objetivo de integrar ambas áreas de forma que nuestro alumnado interactúe con un CAMPUS VIRTUAL ágil y sencillo de utilizar. Una plataforma diseñada para facilitar el estudio, donde el alumnado obtenga todo el apoyo necesario, ponemos a disposición del alumnado un sinfín de posibilidades de comunicación.

Nuestra metodología de aprendizaje online, está totalmente orientada a la práctica, diseñada para que el alumnado avance a través de las unidades didácticas siempre prácticas e ilustradas con ejemplos de los distintos módulos y realice las Tareas prácticas (Actividades prácticas, Cuestionarios, Expedientes prácticos y Supuestos de reflexión) que se le irán proponiendo a lo largo del itinerario formativo.

Al finalizar el máster, el alumnado será capaz de transformar el conocimiento académico en conocimiento profesional.

metodología INEAF



Profesorado y servicio de tutorías

Todos los profesionales del Claustro de INEAF compatibilizan su labor docente con una actividad profesional (Inspectores de Hacienda, Asesores, Abogados ...) que les permite conocer las necesidades reales de asesoramiento que exigen empresas y particulares. Además, se encargan de actualizar continuamente los contenidos para adaptarlos a todos los cambios legislativos, jurisprudenciales y doctrinales.

Durante el desarrollo del programa el alumnado contará con el apoyo permanente del departamento de tutorización. Formado por especialistas de las distintas materias que ofrecen al alumnado una asistencia personalizada a través del servicio de tutorías on-line, teléfono, chat, clases online, seminarios, foros ... todo ello desde nuestro CAMPUS Online.

Materiales didácticos

Al inicio del programa el alumnado recibirá todo el material asociado al máster en papel. Estos contenidos han sido elaborados por nuestro claustro de expertos bajo exigentes criterios de calidad y sometido a permanente actualización. Nuestro sistema de Campus online permite el acceso ilimitado a los contenidos online y suministro gratuito de novedades y actualizaciones que hacen de nuestros recursos una valiosa herramienta para el trabajo diario.



Alianzas

En INEAF, las **relaciones institucionales** desempeñan un papel fundamental para mantener el máximo grado de excelencia en nuestra oferta formativa y situar a nuestros alumno/as en el mejor escenario de oportunidades laborales y relaciones profesionales.



ASOCIACIONES Y COLEGIOS PROFESIONALES

Las alianzas con asociaciones, colegios profesionales, etc. posibilitan el acceso a servicios y beneficios adicionales a nuestra comunidad de alumno/as.



EMPRESAS Y DESPACHOS

Los acuerdos estratégicos con empresas y despachos de referencia nos permiten nutrir con un especial impacto todas las colaboraciones, publicaciones y eventos de INEAF. Constituyendo INEAF un cauce de puesta en común de experiencia.

CALIDAD

PRÁCTICO

ACTUALIZADO

Si desea conocer mejor nuestro Campus Virtual puede acceder como invitado al curso de demostración a través del siguiente enlace:

alumnos.ineaf.es

campus virtual

En nuestro afán por adaptar el aprendizaje a la filosofía 3.0 y fomentar el empleo de los nuevos recursos tecnológicos en la empresa, **hemos desarrollado un Campus virtual (Plataforma Online para la Formación 3.0) exclusivo de última generación con un diseño funcional e innovador.**

Entre las herramientas disponibles encontrarás: servicio de tutorización, chat, mensajería y herramientas de estudio virtuales (ejemplos, actividades prácticas – de cálculo, reflexión, desarrollo, etc.-, vídeo-ejemplos y videotutoriales, además de “supercasos”, que abarcarán módulos completos y ofrecerán al alumnado una visión de conjunto sobre determinadas materias).

El Campus Virtual permite establecer contacto directo con el equipo de tutorización a través del sistema de comunicación, permitiendo el intercambio de archivos y generando sinergias muy interesantes para el aprendizaje.

El alumnado dispondrá de **acceso ilimitado a los contenidos** contando además con manuales impresos de los contenidos teóricos de cada módulo, que le servirán como apoyo para completar su formación.

En INEAF apostamos por tu formación y ofrecemos un **Programa de becas y ayudas al estudio**. Somos conscientes de la importancia de las ayudas al estudio como herramienta para garantizar la inclusión y permanencia en programas formativos que permitan la especialización y orientación laboral.

BE
CAS

BECA DESEMPLEADOS Y ESTUDIANTES	BECA ANTIGUOS ALUMNOS	BECA AUTÓNOMOS	BECA FORMATIVA DE COLABORACIÓN
Para aquellos que se encuentre en situación de desempleo o estén cursando estudios y decidan invertir su tiempo en actualizar sus conocimientos o reorientar su carrera profesional.	Queremos que sigas formándote con nosotros, por ello INEAF te ofrece un 20% dto. en todo nuestro catálogo y te garantiza la beca en los programas Máster.	Valoramos a aquellos que inician su propia aventura empresarial y ven en la formación un valor añadido a sus servicios. INEAF ofrece a los autónomos una beca del 15% dto.	Colaboradores y personal asociado. Tanto por ciento de beca acordado en función del convenio de colaboración.
Documentación a aportar: <ul style="list-style-type: none">• Justificante de encontrarse en situación de desempleo• Documentación que acredite la situación de estudiante	Documentación a aportar: <ul style="list-style-type: none">• No tienes que aportar nada. ¡Eres parte de INEAF!	Documentación a aportar: <ul style="list-style-type: none">• Copia del último recibo de autónomo	Documentación a aportar: <ul style="list-style-type: none">• Consulta información sobre el convenio de colaboración
20%	20%	15%	%

Para más información puedes contactar con nosotros en el teléfono 958 050 207 y también en el siguiente correo electrónico: formacion@ineaf.es

El Claustro Docente de INEAF será el encargado de analizar y estudiar cada una de las solicitudes, y en atención a los **méritos académicos y profesionales** de cada solicitante decidirá sobre la concesión de **beca**.

A photograph of three people (two men and one woman) sitting around a wooden conference table in a room with bookshelves. They are dressed in business attire. The man on the left is wearing glasses and a suit. The woman in the middle has curly hair and is wearing a pink top. The man on the right is wearing glasses and a suit. There are papers, a calculator, and a pen holder on the table.

"Preparamos profesionales con casos prácticos,
llevando la realidad del mercado laboral a
nuestros Cursos y Másteres"

Claustro docente

Nuestro equipo docente está formado por Inspectores de Hacienda, Abogados, Economistas, Graduados Sociales, Consultores, ... Todos ellos profesionales y docentes en ejercicio, con contrastada experiencia, provenientes de diversos ámbitos de la vida empresarial que aportan aplicación práctica y directa de los contenidos objeto de estudio, contando además con amplia experiencia en impartir formación a través de las TICs.

Se ocupará además de resolver dudas al alumnado, aclarar cuestiones complejas y todas aquellas otras que puedan surgir durante la formación.

Si quieres saber más sobre nuestros docentes accede a la sección Claustro docente de nuestra web desde

[aquí](#)



UNIDAD DIDÁCTICA 1.

GESTIÓN Y HERRAMIENTAS DE CIBERSEGURIDAD: INTRODUCCIÓN Y CONCEPTOS BÁSICOS

1. La sociedad de la información
2. - ¿Qué es la seguridad de la información?
3. - Importancia de la seguridad de la información
4. Seguridad de la información: Diseño, desarrollo e implantación
5. - Descripción de los riesgos de la seguridad
6. - Selección de controles
7. Factores de éxito en la seguridad de la información
8. Vídeo tutorial: relación entre la ciberseguridad y el Big Data

UNIDAD DIDÁCTICA 2.

NORMATIVA SOBRE EL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

1. Estándares y Normas Internacionales sobre los SGSI
2. - Familia de Normas ISO 27000
3. - La Norma UNE-EN ISO/IEC 27001:2017
4. - Buenas prácticas en seguridad de la información, Norma ISO/IEC 27002
5. Normativa aplicable a los SGSI
6. - Normativa comunitaria sobre seguridad de la información
7. - Legislación Española sobre seguridad de la información
8. - El Instituto Nacional de Ciberseguridad (INCIBE)

UNIDAD DIDÁCTICA 3.

POLÍTICA DE SEGURIDAD: ANÁLISIS Y GESTIÓN DE RIESGOS

1. Plan de implantación del SGSI
2. Análisis de riesgos
3. - Análisis de riesgos: Aproximación
4. - Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura
5. - Particularidades de los distintos tipos de código malicioso
6. - Principales elementos del análisis de riesgos y sus modelos de relaciones
7. - Metodologías cualitativas y cuantitativas de análisis de riesgos
8. - Identificación de los activos involucrados en el análisis de riesgos y su valoración
9. - Identificación de las amenazas que pueden afectar a los activos identificados previamente
10. - Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo el análisis local
11. - Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría
12. - Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas
13. - Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse
14. - Determinación de la probabilidad e impacto de materialización de los escenarios
15. - Establecimiento del nivel de riesgo para los distintos

20. - Exposición de la metodología Magerit
21. Gestión de riesgos
22. - Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes
23. - Metodologías comúnmente aceptadas de identificación y análisis de riesgos
24. - Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo

UNIDAD DIDÁCTICA 4. AUDITORÍA DE CIBERSEGURIDAD

1. Criterios Generales en la Auditoría de Seguridad de la Informática
2. - Código deontológico de la función de auditoría
3. - Relación de los distintos tipos de auditoría en el marco de los sistemas de información
4. - Criterios a seguir para la composición del equipo auditor
5. - Tipos de pruebas a realizar en el marco de la auditoría, pruebas sustantivas y pruebas de cumplimiento
6. - Tipos de muestreo a aplicar durante el proceso de auditoría
7. - Utilización de herramientas tipo CAAT (Computer Assisted Audit Tools)
8. - Explicación de los requerimientos que deben cumplir los hallazgos de auditoría
9. - Aplicación de criterios comunes para categorizar los hallazgos como observaciones o no conformidades
10. - Relación de las normativas y metodologías relacionadas con la auditoría de sistemas de información comúnmente aceptadas
11. Aplicación de la normativa de protección de datos de carácter personal
12. - Normativa de referencia: Reglamento General de Protección de Datos y Ley Orgánica de Protección de Datos

20. - Herramientas de análisis de red, puertos y servicios tipo Nmap, Netcat, NBTScan, etc.
21. - Herramientas de análisis de vulnerabilidades tipo Nessus
22. - Analizadores de protocolos tipo WireShark, DSniff, Cain & Abel, etc.
23. - Analizadores de páginas web tipo Acunetix, Dirb, Parosproxy, etc
24. - Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc.
25. Descripción de los aspectos sobre cortafuego en auditorías de sistemas de información
26. - Principios generales de cortafuegos
27. - Componentes de un cortafuegos de red
28. - Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
29. - Arquitecturas de cortafuegos de red
30. Guías para la ejecución de las distintas fases de la auditoría de sistemas de información
31. - Normas para la implantación de la auditoría de la documentación
32. - Instrucciones para la elaboración del plan de auditoría
33. - Pruebas de auditoría
34. - Instrucciones para la elaboración del informe de auditoría

pares de activo y amenaza

16. - Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no
17. - Relación de las distintas alternativas de gestión de riesgos
18. - Guía para la elaboración del plan de gestión de riesgos
19. - Exposición de la metodología NIST SP 800-30

UNIDAD DIDÁCTICA 5. COMUNICACIONES SEGURAS: SEGURIDAD POR NIVELES

1. Seguridad a nivel físico
2. - Tipos de ataques
3. - Servicios de Seguridad
4. - Medidas de seguridad a adoptar
5. Seguridad a nivel de enlace
6. - Tipos de ataques
7. - Medidas de seguridad a adoptar
8. Seguridad a nivel de red
9. - Datagrama IP
10. - Protocolo IP
11. - Protocolo ICMP
12. - Protocolo IGMP
13. - Tipos de Ataques
14. - Medidas de seguridad a adoptar
15. Seguridad a nivel de transporte
16. - Protocolo TCP
17. - Protocolo UDP
18. - Tipos de Ataques
19. - Medidas de seguridad a adoptar

20. Seguridad a nivel de aplicación
21. - Protocolo DNS
22. - Protocolo Telnet
23. - Protocolo FTP
24. - Protocolo SSH
25. - Protocolo SMTP
26. - Protocolo POP
27. - Protocolo IMAP
28. - Protocolo SNMP
29. - Protocolo HTTP
30. - Tipos de Ataques
31. - Medidas de seguridad a adoptar

13. - Principios generales de la protección de datos de carácter personal

14. - Legitimación para el tratamiento de datos personales

15. - Medidas de responsabilidad proactiva

16. - Los derechos de los interesados

17. - Delegado de Protección de Datos

18. Herramientas para la auditoría de sistemas

19. - Herramientas del sistema operativo tipo Ping, Traceroute, etc.

www.ineaf.es



INEAF BUSINESS SCHOOL

958 050 207 · formacion@ineaf.es

