CURSO ACREDITADO POR LA UNIVERSIDAD CATÓLICA DE ÁVILA

- **On-line**

1. INTRODUCCIÓN

El CURSO ESPECIALISTA en Ethical Hacking y Ciberseguridad Legal, se plantea como una formación integral para el alumno en los distintos campos y aspectos relacionados con la **Ciberseguridad y el Hacking Ético**: Desde las más actuales técnicas y herramientas de análisis de vulnerabilidades, hasta los aspectos más necesarios a tener en cuenta para proteger los datos y sistemas de una empresa de los ataques de los Ciberdelincuentes.

En el panorama actual y futuro de la empresa, la constante evolución de los Delitos Tecnológicos hace que se requieran profesionales altamente cualificados en la protección de los datos, sistemas y procesos de negocio de la empresa.

La actividad de los Ciberdelincuentes supone una amenaza a la continuidad de negocio de la empresa, por lo que es necesario que los profesionales dedicados a las áreas de Tecnologías de la Información (TI) tengan los conocimientos y habilidades para la adecuada planificación y gestión de los riesgos tecnológicos a los que la empresa debe hacer frente, de una manera práctica y con una visión integral de sus áreas de responsabilidad.

Identificar los riesgos tecnológicos de una empresa, así como conocer los principales riesgos y amenazas tecnológicas de cara a la adecuada protección contra los ciberdelincuentes, es una prioridad en el perfil profesional orientado a TI, para lo cual resulta imprescindible una formación actualizada, completa y práctica como la que se ofrece en este curso.

IMQ Ibérica Business School y **Hack by Security** ofrecen mediante este curso una perspectiva integral de cómo el Hacking Ético puede convertirse en un aliado de la empresa y los profesionales de las áreas de TI, al permitir reconocer la cantidad de datos que de manera inadvertida están publicados en internet, y que pueden comprometer la seguridad y fiabilidad de su actividad profesional. Además, se mostrarán técnicas de Hacking Ético que pueden permitir mejorar y facilitar los procesos de detección de las vulnerabilidades que los sistemas y la presencia online de la empresa ofrecen, y que pueden suponer un vector de riesgo tecnológico para la empresa, sus procesos y sus datos, o los de sus clientes.

2. IMQ - UCAV

IMQ son las siglas del **Istituto Italiano del Marchio di Qualità,** Entidad de Certificación líder en Italia. Se fundó en 1951 en Milán (Italia) y tiene como objeto social la Certificación de Productos y de Sistemas de Gestión (más de 20.000 certificados emitidos en Sistemas de Gestión y 140.000 en Producto).

Actualmente IMQ es un grupo de empresas que abarca múltiples certificaciones de producto y de sistemas.

Las empresas del grupo IMQ representan la más importante realidad italiana en el campo de la evaluación de la conformidad (certificaciones, pruebas, verificaciones, inspecciones). Con la fortaleza de la sinergia entre las sociedades que lo componen, la relevancia adquirida en más de 60 años de experiencia y la integridad de los servicios ofrecidos, el grupo IMQ se erige como un punto de referencia y socio ideal de empresas que tienen como objetivo la seguridad, la calidad y la sostenibilidad ambiental.

Los sectores de referencia son múltiples, y van desde la electrotecnia a la electrónica, desde las telecomunicaciones a la automoción, desde el sector del gas al diseño de instalaciones, desde los productos de construcción hasta los productos agroalimentarios y las energías renovables.

Para cada sector, las empresas del grupo IMQ pueden ofrecer, según corresponda, servicios horizontales o específicos:

Certificación de productos, certificaciones ambientales, certificación según las directivas de la UE, certificación de sistemas de gestión y figuras profesionales, controles de plantas y edificios, pruebas de laboratorio, pruebas para obtener marcados internacionales y apoyo a la exportación, supervisión de la producción en el extranjero, apoyo técnico reglamentario y formación. La integridad de los servicios prestados está garantizada gracias a la experiencia adquirida en todas estas áreas durante décadas por parte de las empresas del grupo IMQ que está compuesto por: IMQ S.p.A., CSI S.p.A., **IMQ Ibérica S.L. (España), IMQ Tecnocrea (España)**, IMQ Polska (Polonia), IMQ Turkey (Turquía), IMQ Gulf FZCo (Dubái), IMQ Certification Shanghai Co. Ltd (China); IMQ United Kingdom.

NUESTROS OBJETIVOS

Cuantificar la gestión ética y responsable como generadora de valor reputacional y de mejora de la competitividad de la empresa. Aportar herramientas de gestión y control de cumplimiento normativo con el fin de evitar o minorar el riesgo de llevar a cabo actuaciones ilícitas por parte de los directivos y empleados de una organización que puedan derivar en sanciones administrativas, económicas o en responsabilidad penal de la persona jurídica.

NUESTRA VISIÓN

Integridad moral, honestidad profesional, lealtad e imparcialidad para/con los grupos de interés y transparencia de mercado. Interpretamos los sistemas de gestión como una herramienta que genera valor añadido a las empresas, y les permite controlar y gestionar sus riesgos y oportunidades, aumentando su competitividad.

QUE OFRECEMOS

IMQ es el socio ideal para todas aquellas empresas que quieren dar un valor añadido a su actividad, certificando su compromiso con la gestión ética y responsable, interesadas en exportar en Europa y el resto del mundo, que necesitan un apoyo competente para superar las barreras aduaneras y de obtención de las marcas extranjeras.

En particular, **IMQ** se presenta como una sociedad de servicios especializada en certificaciones de productos, sistema de producción, y pruebas de conformidad según las directivas europeas y normas internacionales. Estamos en el grado de ofrecer numerosos servicios como: Evaluación de las instalaciones de inmuebles, realización de pruebas de laboratorio, asistencia técnica/normativa y a la exportación.

COLABORACIÓN CON LA UCAV:

La Universidad Católica Santa Teresa de Jesús de Ávila (UCAV) surgió en 1996 bajo la tutela del Obispado de la Diócesis de Ávila. Su modelo educativo pretende una enseñanza moderna y ágil, adaptada a las demandas sociales y laborales del mundo actual, y a las inquietudes intelectuales de cada alumno. Su compromiso con la sociedad persigue el equilibrio entre la formación y las necesidades del mercado laboral y tiene como prioridad conseguir la más alta calidad tanto en la formación y los servicios que ofrece a sus alumnos, como en el trabajo de las personas que la integran, en orden a satisfacer las necesidades actuales y futuras de sus alumnos.

Como consecuencia de esto, el equipo rectoral de la Universidad apoya firmemente su estrategia de Calidad, que coloca a la UCAV en una situación de excelencia.

***"En la UCAV colaboramos con los mejores**: Múltiples y numerosos son los sectores con los que desde la Universidad Católica de Ávila trabajamos en la búsqueda de la excelencia en cada uno de los campos laborales, académicos y sociales. De ahí surge cada una de las colaboraciones en las que **cada uno de los planes de estudios ofrecidos por estas instituciones es revisado y sellado con la garantía educativa de nuestra universidad**, aportando así un valor añadido y un **certificado universitario**, así como una búsqueda de sinergias y en muchas ocasiones compartir equipos profesionales, educativos o de sistemas."*

¿Qué significa ser «Centro Acreditado por la Universidad Católica de Ávila»?

La principal ventaja que ofrece acreditar una titulación como título propio Universitario es que dichos estudios cuentan con el respaldo de la Universidad Católica de Ávila:

"Desde la UCAV, nos preocupamos mucho de que los títulos que acreditamos con otras instituciones reúnan los estándares que exige nuestra normativa interna de estudios propios. Asimismo, realizamos una **auditoría anual a través de la cual, podemos comprobar que los centros colaboradores mantienen los estudios según los requisitos que exigimos**.

Por otro lado, acreditar un título con nuestra Universidad, le da un valor añadido, ya que nuestro centro está consolidado y tiene un prestigio reconocido a nivel nacional e internacional. Algunos de los premios y rankings en los que destacamos son los siguientes:

- Está dentro del ranking Forbes de las 25 mejores universidades de España 2022
- Es la Universidad de Castilla y León mejor posicionada en la calidad del empleo de sus egresados.
- Premio Blackboard Catalyst 2021 por estar a la vanguardia de la innovación educativa"

3. HACK BY SECURITY

Las empresas cada vez son más complejas ya que cada día manejan un mayor volumen de información y éstas deben estar protegidas de manera activa. Todos los días y cada vez más, van apareciendo un número mayor de incidencias de seguridad, no solo en pequeñas, sino también en grandes organizaciones. Desde hace bastantes años, todos los días nos levantamos con algún nuevo incidente de seguridad que ha desembocado en el robo de datos de una compañía, en el robo de las identidades de los empleados o en un fraude que obliga a la empresa víctima a realizar una comunicación a sus clientes, que no suele salirle barata en términos de daño reputacional y por tanto en términos económicos.

En Hack by Security somos consciente de este continuo y creciente problema, y es por ello por lo que como solución al problema expuesto surge este proyecto.

Gracias a nuestra experiencia y conocimiento en el sector IT y ciberseguridad, ofrecemos principalmente dos ramas de servicios a nuestros clientes.

- Servicios de ciberseguridad basadas técnicas de hacking y seguridad informática.
- Formación presencial y online en materia de ciberseguridad, hacking ético y concienciación.

Ofrecemos servicios relacionados con el mundo de la ciberseguridad y hacking ético, realizando test de intrusión y análisis de vulnerabilidades sobre cualquier sistema que tenga su empresa, servidores, aplicaciones webs, redes inalámbricas, sistemas de videovigilancia, IoT (Internet of Things), peritaje informático forense, equipo de red & blue team, entre otros servicios.

Por otro lado, también ofrecemos una amplia gama formativa tanto presencial como online, relacionada con el Ethical Hacking y la Ciberseguridad; tanto para usuarios noveles que quieren adentrarse en el mundo de la ciberseguridad o usuarios avanzados y administradores de sistemas que quieren ampliar sus conocimientos en el mundo del Hacking Ético.

IMQ Ibérica y Hack by Security son empresas registradas en el INCIBE (Instituto Nacional de Ciberseguridad). IMQ además con gran experiencia en la certificación de Seguridad de la Información en el sector TI, lo que es un valor añadido complementario a la experiencia aportada por Hack by Security.

4. DESTINATARIOS

El Curso Especialista en Ethical Hacking y Ciberseguridad Legal está dirigido a diversos perfiles:

- Directivos de organizaciones con responsabilidad en Seguridad de la Información o Seguridad en la Tecnologías de Información y Comunicaciones.
- Profesionales TI, responsables de sistemas y redes, consultores.
- Responsables de empresas de Informática.
- Perfiles profesionales orientados a la Seguridad Informática que deseen adquirir nuevos conocimientos y competencias de gestión.

Perfiles sin experiencia profesional que deseen enfocar su carrera en la Ciberseguridad y Hacking Ético.

Los principales **perfiles profesionales** para los que este título cualifica son:

CISO (Chief Information Security Officer) director de seguridad de la información. Su función principal es la de alinear la seguridad de la información con los objetivos de negocio. De forma que garantice en todo momento que la información de la empresa está protegida adecuadamente.

CSO (Chief Security Officer) es el responsable de la seguridad de la organización.

CTO (Chief Technology Officer) en un rol similar al CIO pero más técnico. Director técnico, siendo su responsabilidad la gestión del día a día de las tecnologías de la información.

Perito en Informática Forense. Realización de informes y dictámenes periciales judiciales o extrajudiciales. Peritaciones Informáticas y Telemáticas.

Consultor: Permite desarrollar labores de consultoría técnica y de gestión, apoyando a empresas en el desarrollo e implantación de los sistemas de seguridad y riesgos.

Auditor: Capacita al alumno con competencias para evaluar a empresas y otras organizaciones sobre el grado de cumplimiento de los requisitos exigidos y emitir los correspondientes informes de valoración.

5. OBJETIVOS

El **objetivo general** de este curso especialista es facilitar a los participantes los conocimientos, herramientas, habilidades y competencias exigidas a los profesionales de Ciberseguridad y Hacking Ético.

Para conseguir ese objetivo, el **Curso Especialista en Ethical Hacking y Ciberseguridad Legal** tiene como **objetivos específicos**

- Proporcionar los conocimientos necesarios a nivel conceptual y práctico para implementar en empresas y negocios, un sistema Integral de seguridad informática integral y perimetral, apoyados por el uso de Software Libre.
- Desarrollar las habilidades prácticas para la realización de auditorías de sistemas intrusivas, usando las técnicas de la Auditoria de T.I del tipo "Hacking Ético y/o Test de Penetración".
- Conocer los tipos de atacantes, así como a usar las diferentes técnicas y herramientas de intrusión utilizadas por los delincuentes informáticos para lograr violentar la seguridad de un sistema de información.
- Realizar auditorías de Pentesting con su correspondiente informe profesional, además de conocer los métodos utilizados por los delincuentes cibernéticos para poder contrarrestar sus ataques.
- Orientar las auditorias intrusivas haciendo uso de las normas y buenas prácticas en seguridad de la información a nivel internacional.
- Aprender las técnicas de ataque y protección de las redes de datos y las aplicaciones web dinámicas.
- Adquirir los conocimientos necesarios a nivel conceptual y práctico para implementar en empresas y negocios, un sistema Integral de seguridad informática integral y perimetral.
- Desarrollar y adquirir las habilidades prácticas para la realización de Instalaciones y supervisión de redes de datos, mejorando y manteniendo la seguridad de las mismas.
- Conocer los diferentes tipos de sistemas de Seguridad, aprenderás a implantar un sistema de red seguro basado en configuraciones correctas y adaptando la Red corporativa a un nivel seguro.
- Realizar auditorías de Seguridad con su correspondiente informe de Red, además de conocer los métodos para realizar una auditoría de Red basada en un Sistema de Gestión de la Seguridad (SGSI).
- Crear correctamente con toda la documentación necesaria una Red de datos corporativa.
- Aprender a configurar correctamente dispositivos perimetrales, de forma segura y con un funcionamiento correcto dentro de una Red de datos Corporativa.
- Formar técnicos y auditores técnicos de Seguridad en Redes en el tema de seguridad de la información.

- El curso proporciona los conocimientos necesarios a nivel conceptual y práctico para desarrollar en empresas y negocios, un peritaje Informático completo.
- Desarrollar y adquirir habilidades prácticas para la realización de todo lo que conlleva un Peritaje.
- Iniciación del alumno en la ejecución de un análisis informático forense con el fin de poder realizar periciales judiciales y extrajudiciales

6. PROGRAMA

Módulo 1: Concienciación

- INTRODUCCIÓN: Apartado teórico, Conceptos generales, Tipos de ataque, Efectos de un ataque, La red oscura, Prevención = formación + concienciación, Ejercicio práctico
- PHISHING: Apartado teórico, Introducción, Reglas de ciberseguridad, Ejercicio práctico
- SEGURIDAD EN EL PUESTO DE TRABAJO: Apartado teórico Introducción, Reglas de ciberseguridad, Ejercicio práctico
- CONCIENCIACIÓN DE USO DE TECNOLOGÍA SMARTPHONE: Apartado teórico, Introducción, Reconocimiento local del dispositivo, Reconocimiento de red del dispositivo, APK maliciosas, Ingeniería social, Ejercicio práctico

Módulo 2: Ciberinteligencia

- Conceptos generales de ciberinteligencia.
- Ciclo de inteligencia.
- Anonimización.
- Deep Web.
- Conceptos generales de Ingeniería social.
- Tipos de ataque utilizados en ingeniería social.
- Técnicas basadas en contacto humano real.
- Técnicas basadas en conocimientos informáticos.
- Técnicas basadas en tecnología smartphone.
- Conceptos generales de Phishing.
- Tipos de técnicas de Phishing.
- Identificación de mails maliciosos.
- Creación de campañas de Phishing.
- Contramedidas para contrarrestar campañas de Phishing.

Módulo 3: Hacking Ético Nivel I

- Introducción.
- Recopilación de Información.
- Análisis de puertos y vulnerabilidades.
- Creación y uso de diccionarios.
- Herramientas de explotación.
- Evasión de detección.
- Redes Wireless.
- Envenenar y/o suplantar servicios
- Ingeniería social.
- Hacking de aplicaciones web.
- Telefonía móvil.
- Post-Explotación.

Módulo 4: Forense nivel I

- INTRODUCCIÓN: Apartado teórico, Introducción Internet, Volatilidad de la huella digital, Legaltech, WhatsApp como fuente de prueba, Ejercicio práctico
- REGULACIÓN DE LA PRUEBA TECNOLÓGICA: Apartado teórico, Fuentes y medios de la prueba electrónica, Derechos del entorno digital, Prueba digital ilícita, Ejercicio práctico
- FASES PROBATORIAS: Apartado teórico Licitud y autenticidad, Presentación y valoración Cadena de custodia, Ejercicio práctico
- INFORME PERICIAL: Apartado teórico, Metodología, Conclusiones y defensa en sala, El perito, Ejercicio práctico
- EL PERITO EN EL ENTORNO LABORAL, Apartado teórico, Especialidades del orden laboral, Acceso a la información y principios rectores, Jurisprudencia en el orden laboral, Ejercicio práctico

Módulo 5: Cloud Computing

- Conceptos y arquitecturas de la computación en la nube.
- Gobierno y gestión del riesgo corporativo.
- Cuestiones legales, contratos y descubrimiento electrónico.
- Cumplimiento y gestión de auditoría.
- Gobierno de la información.
- Gestión y continuidad del negocio.
- Seguridad de la infraestructura.
- Respuesta ante incidentes.

- Seguridad de aplicaciones.
- Seguridad y cifrado de datos.
- Gestión de identidades, derechos y accesos.
- Seguridad como servicio.
- Tecnologías relacionadas.

Módulo 6: Hacking Ético nivel II

- Introducción.
- Conceptos de debugging y fuzzing
- Introducción al buffer overflow (Smashing Stack)
- Sobreescritura de SEH (Buffer overrun).
- Bypass de DEP.
- Bypass de NX y ASLR.
- Buffer overflow en entornos de 64 bits.

Módulo 7: Forense Nivel II

- Introducción y herramientas
- Extracción de información en sistemas encendidos
- Extracción de información en sistemas apagados
- Líneas de tiempo
- Sistemas de ficheros
- Otros sistemas de ficheros
- Artefactos de los sistemas de ficheros

Módulo 8: Forense Nivel III

- INTRODUCCIÓN: Análisis forense en dispositivos móviles.
- INTRODUCCIÓN IOS: Introducción a IOS
- EXTRACCIÓN DE INFORMACIÓN: Contexto Jailbreak Extracción manual
- HERRAMIENTAS: UFED I, UFED II, Mobiledit I, Mobiledit II, Otras herramientas
- ANÁLISIS: Análisis manual I, Análisis manual II, Análisis manual III, UFED cellebrite Mobiledit

Módulo 9: Sistemas de Gestión de la Seguridad de la Información ISO/IEC 27001: 2017

- Terminología
- Conceptos de la seguridad de la información y de su gestión
- El Modelo de Gestión ISO 27001: 2017
- Implantación Sistemas de Gestión de la Seguridad de la Información
- Auditoría Sistema de Gestión de la Seguridad de la Información
    - Anexos (Auditorías IMQ, casos prácticos, checklists, etc.)

Se incluyen libros de 0xWORD, 1000 tempos en la plataforma de Mypublicinbox y vouchers de Singularity Hackers:

MYPUBLICINBOX: https://mypublicinbox.com/

0XWORD: https://0xword.com/

SINGULARITY HACKERS: https://singularity-hackers.com/

7. METODOLOGÍA.

Con el fin de asegurar el máximo aprovechamiento del Curso, los alumnos tienen a su disposición la plataforma virtual específica para esta formación de Hack by Security a través de la que podrán acceder a:

- Archivos digitales en PDF con las prácticas de laboratorios.
- Archivos digitales con las presentaciones en PowerPoint y vídeos en todos los módulos.
- Archivos en PDF con la documentación de buenas prácticas y ejemplos de reportes de auditoría técnica intrusiva del tipo Hacking Ético.
- Suministro de las máquinas virtuales usadas en el Curso.
- Vídeos de las clases de forma grabada, para su visionado online.
- Realización de talleres y laboratorios prácticos orientados al ataque y defensa de redes y servidores.
- Pruebas prácticas con puntuación para la nota final.
- Utilización de máquinas virtuales víctimas, previamente preparadas, que simulan sistemas operativos y servicios de red vulnerables, para poder hacer los laboratorios intrusivos.
- Se llevará a la práctica laboratorios con redes, máquinas y aplicaciones web vulnerables.
- Tutorización directa mediante correo electrónico (online).

En esta modalidad, el curso virtual está diseñado y planeado para realizarse de forma offline, con las ayudas online, por lo que cada alumno puede avanzar a su propio ritmo, pero sin pasarse de las actividades programadas.

Proyecto Fin de Curso: Consiste en la realización de un proyecto original en el que con una actitud investigadora se promueva la creatividad. Para la realización de este proyecto, se proveerá al alumno de una serie de máquinas virtuales durante la duración de los diferentes módulos que componen el Curso, emulando diversos Sistemas Informáticos (servidores, webs, equipos, etc.), con una serie de vulnerabilidades específicamente diseñadas al efecto de que el alumno aplique los conocimientos adquiridos en el curso.

El objetivo del Proyecto Fin de Curso es que el alumno realice la investigación y detección de vulnerabilidades existentes en las máquinas virtuales, y reporte, mediante el Informe Técnico Correspondiente, las consecuencias y riesgos tecnológicos de las mismas, así como realice una propuesta técnica de resolución de cada una de las vulnerabilidades, según los esquemas y procedimientos identificados en los respectivos módulos del Curso.

A través del Proyecto Final se integran, aplican y desarrollan los conocimientos, habilidades y actitudes adquiridos. El proyecto final es la culminación del Curso.

MODALIDAD ONLINE. Es indudable que la enseñanza online requiere por parte del alumno/a mayor disciplina y constancia, independientemente del tiempo que pueda invertir en el estudio, es fundamental adquirir por medio de la disciplina personal, un hábito de estudio diario; la continuidad es un aspecto esencial para obtener un rendimiento exitoso en la realización del Curso.

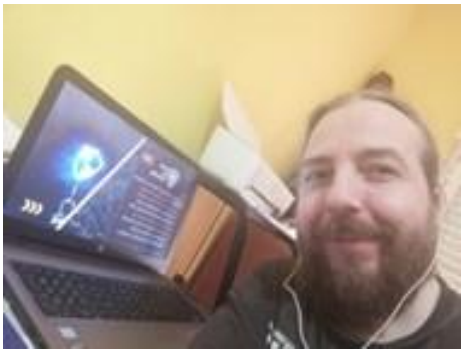
8. Dirección del curso y claustro de profesores.

Dirección:

MIGUEL ÁNGEL MARTÍN PEÑA

Curso en Hacking Ético CEO de Hack by Security Hacker ético. Docente de ciberseguridad, director de TI en distintas compañías con más de 15 años de experiencia. Ponente en institutos y universidades. Poseedor de diferentes certificaciones en ciberseguridad y redes. https://mypublicinbox.com/MiguelAngelMartin	

RAFAEL GARCÍA LÁZARO

Curso en Hacking Ético COO-CTO de Hack by Security Hacker ético. Red Team Leader. Docente de ciberseguridad y ciberinteligencia con más de 20 años de experiencia en TI. Ponente en institutos y universidades. Poseedor de diferentes certificaciones en ciberseguridad, Microsoft, SCRUM e ITIL. https://mypublicinbox.com/Gwalrock	

FRANCISCO NADADOR SÁNCHEZ-SECO

Ingeniero en Informática Docente en Hack by Security Máster en Seguridad Informática con especialidad en Auditoría de Seguridad Analista informático forense y perito informático. Director Pedagógico en Salesianos Alcalá. https://mypublicinbox.com/Alkalinas	

PABLO GONZALEZ

Docente en Hack by Security Ingeniero Informática y Máster en Seguridad Informática. Trabaja en Telefónica en el departamento de Ideas Locas de CDCO. MVP de Microsoft desde el año 2017 https://mypublicinbox.com/PabloGonzalez	

JUAN CARLOS FERNÁNDEZ

Graduado en Derecho Docente en Hack by Security Profesor en los Cursos de Ciberseguridad de la UCLM y en el Excutive en Derecho Digital de Garrigues, así como docente en el curso de Peritaje en Ingeniería Informática del Colegio de Ingenieros de Madrid. Ponente en diversas Universidades y en los principales Congresos de Seguridad Informática en España. https://mypublicinbox.com/Tecnogados	

9. Calendario y duración.

La duración del Curso es de **900 horas (36 ECTS)**, estimadas entre 9 y 12 meses de duración, disponiendo de una prórroga de 4 meses para la finalización de los casos prácticos y la realización del proyecto fin de Curso.

10. Costes de inscripción

Puede consultar el precio actual en nuestra página web: www.imqibericaformacion.com así como las promociones vigentes de descuentos en la ficha del Curso / Curso

IMQ Ibérica Business School es Entidad Organizadora Acreditada para la impartición de Formación bonificable hasta el 100% para trabajadores que quieran matricularse en nuestros cursos en cualquiera de sus modalidades.

11. Titulación y certificaciones

Títulos de **"Especialista en Ethical Hacking y Ciberseguridad Legal"**

de *IMQ Ibérica Business School* y *Hack by Security*

900 Horas (30 ECTS)

Diploma **"Especiaista en Ethical Hacking y Ciberseguridad Legal"**
emitido por la Universidad Católica de Ávila

Certificaciones profesionales de Hack by Security: Certificaciones tecnológicas que se ofrece a los profesionales en el área de las tecnologías de la información. Certificación orientada hacia la Seguridad Informática integral en los niveles, defensivo y de gestión de redes de datos:

- **Certificación CCIT** (Curso en concienciación y ciberseguridad IT). Prevención.

- **Certificación CTEC** (Curso Técnico de Especialista en Ciberinteligencia). Defensa en profundidad.
- **Certificación CSIO** (Curso Seguridad informática Ofensiva) Hacking Ético, Seguridad Web y Seguridad en redes inalámbricas.
- **Certificación BLPI** (Básicos Legales del Perito Informático) La participación en Juicios de faltas relacionadas con la Seguridad de la Información.
- **Certificación CNCC** (Curso de Ciberseguridad y Normativa en Cloud Computing). Seguridad en Cloud Computing.
- **Certificación CSCE** (Curso Seguridad Creación Exploits) Depuración y análisis de software y binarios. Desarrollo de informes de seguridad sobre vulnerabilidades localizadas en software.
- **Certificación CAIFOR** (Curso de Análisis Informático Forense) Peritaje de entornos Informáticos
- **Certificación CAIFIOS** (Curso de Análisis Informático Forense en iOS) Peritaje de entornos Informáticos de Apple.

· **Auditor Interno en Ciberseguridad y Hacking Ético de IMQ**

· **Auditor Interno en ISO 27001:2017 de IMQ**