# MÁSTER SUPERIOR EN **CIBERSEGURIDAD y HACKING ÉTICO**


- **Presencial**
- **Virtual**
- **On-line**

# 1. INTRODUCCIÓN

El Máster Superior en Ciberseguridad y Hacking Ético, 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 Máster.

**IMQ Ibérica Business School** y **The Security Sentinel** ofrecen mediante este Máster 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

**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 Ibérica es empresa registrada en el INCIBE (Instituto Nacional de Ciberseguridad) 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 The Security Sentinel.

## 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. En el caso concreto del Máster en Sistemas de Gestión de Compliance y Antisoborno, permite implantar metodologías de gestión y control que evitan o minoran el riesgo de derivación de la responsabilidad penal a la empresa.

**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.

## 3. THE SECURITY SENTINEL

The Security Sentinel es una empresa 100% española, perteneciente al Grupo Hodei, grupo empresarial con presencia en España y Latinoamérica que tiene como misión, aportar soluciones encaminadas a optimizar la toma de decisiones de las empresas y a mejorar su productividad y su seguridad.

The Security Sentinel está especializada en proporcionar servicios y soluciones en el ámbito de la Seguridad de la Información y de las Comunicaciones, así como en formar a los mejores profesionales en Seguridad Informática.

The Security Sentinel está formada por profesionales con más de 20 años de experiencia acumulada en el sector. Auténticos expertos en hacking ético, seguridad perimetral, seguridad en redes y peritaje informático, pudiendo cubrir de esta forma todas las áreas de la seguridad informática, desde la asesoría personalizada hasta el desarrollo e instalación de elementos físicos para la Ciberseguridad.

En The Security Sentinel formamos a los mejores profesionales en Seguridad Informática, capacitándolos para prevenir y gestionar los incidentes de seguridad a través de una oferta formativa totalmente práctica, con entornos 100% reales y adaptados a sus necesidades y conocimientos de partida.

## 4. DESTINATARIOS

El Máster en Ciberseguridad y Hacking Ético 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 máster 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 correspondiente informes de valoración.

## 5. OBJETIVOS

El **objetivo general** de este Máster 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 **Máster en Ciberseguridad y Hacking Ético** 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 Máster 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 extra judiciales

## 6. PROGRAMA

**Módulo 1: Seguridad en Redes**

- Conceptos Básicos De Redes.
- Diseño De La Red.
- Direccionamiento.
- Simulador De Redes GNS3
- TCP/IP.
- Modelo De Capas OSI
- Infraestructura De Red
- Servicios De Red.
- Herramientas De Red (Nmap, Traceroute, Ping).
- Diseño De La Red (Factores Y Estructuración).
- Ethernet.
- Introducción Al Enrutamiento (Estático).

- Enrutamiento Dinámico.
- RIP, OSPF, EIGRP.
- Switch.
- Vlan
- Enrutamiento Inter-Vlan.
- Spanning.Tree.
- Etherchannel.
- SSH, Telnet Y DHCP.
- Reglas De Firewall En Routers (ACL).
- Wireless.
- Virus Y Antivirus.
- Ataques E Intrusiones.
- Firewalls.
- Contraseñas.
- Aaa (Radius Y Tacacs).
- VPN's.
- Análisis De Riesgos.
- Análisis De Vulnerabilidades.

**Módulo 2: Hacking Ético Nivel I**

- Introducción.
- Arquitectura De Redes.
- Kali Linux.
- Recolección De Información.
- Escaneo:
  - Análisis De Servicios Y Puertos.
  - Análisis De Vulnerabilidades.
- Explotación.
- Post-Explotación.
- Password Cracking.
- Auditoras Wifi.
- Malware:
  - Modding Desde 0.
- Forense.
- Auditorías Móviles.
- Auditorías Web.
- Creación De Un Informe De Pentest.

**Módulo 3: Hacking Ético A Móviles**

- Introducción.
- Herramientas.
- Sistemas Operativos.
- Tipos De Análisis OWASP.
- Top Ten Riesgos (OWASP).
- Método CPAM:

  - Root-Unroot.
  - Recolección De Información.
  - Escaneo De Servicios.
  - Vectores De Ataque.
    - Locales
    - Remotos
- Análisis De APK's Sospechosas.
- Ejemplos Prácticos (Ios Y Android).
- Realización Informe.

**Módulo 4: Hacking Ético Nivel II**

- Introducción Y Objetivos Del Módulo.
- Herramientas A Utilizar:
  - Vmware.
  - Virtualbox.
  - TPS (Tutorial De Herramientas, Kali).
- Linux 100%.
- Metasploit 100%:
  - Repaso a La Herramienta.
  - Fases Del Hacking.
  - Adicionales.
  - Creación De Exploits.
- Introducción Python-Hacking:
  - Introducción A La Programación Python.
  - Uso De Librerías Específicas.
- Introducción Ruby-Hacking:
  - Introducción A La Programación Ruby.
  - Implementación A Metasploit.

- Hacking Web:
  - Taxonomía De Un Ataque.
  - Ejemplos De Vulnerabilidades Y Ataques.
    - Inyección SQL
    - XSS
    - LFI
    - Inyección De Código
    - RFI
    - Phising

- Hacking Infraestructuras:
  - Redes.
  - Linux
  - Windows
  - OS
  - Escalada De Privilegios De Cero A 100.

- Shell Scripting
- Linux
- Windows

- Malware:
  - Crypter.
  - Creación De Un Crypter
  - Fudear Crypter.
  - Análisis De Malware.
  - Sandbox.
  - Botnet.

- Crear Un Botnet
  - Troyano.
- Crear Un Troyano (Cliente, Servidor)
- La Auditoría:
  - Presupuesto.
  - Contrato.
  - Alcance.
  - Ejemplo De Auditoría.

**Módulo 5: Informática Forense**

- Introducción.
- Entornos De Trabajos:
  - Laboratorios Forense Bajo Entorno Windows.
  - Laboratorios Forense Bajo Entorno Linux.

- Recolección De Evidencias:
  - Asegurar La Escena.
  - Identificar Las Evidencias.
  - Preservar Las Evidencias (Cadena De Custodia).

- Tareas Y Dependencias De Las Mismas:
  - Estado Del Arte.
  - Buenas Prácticas.
  - Análisis De Riesgos.
- Análisis De La Línea De Tiempo (Timestamp):
  - Definición De Línea De Tiempo.

- Osforensic
- Deft

- Proceso Manual Con Ayuda De Comandos Para La Obtención De La Línea De Tiempo.
- Análisis De Volcado De Memoria:
    - Volatility: Extracción De Información En Volcado Windows.
    - Volatility: Extracción De Información En Volcado Linux.

- Análisis De Una Imagen Sobre Plataforma Microsoft:
    - Análisis De Escritorios Y Papelera De Reciclaje (Windows)
    - Hibernación Y Paginación.
    - Recuperación De Ficheros.
    - Información Basada En Firmas.
    - Análisis De Directorios.
    - Análisis De Aplicaciones.
    - Análisis De Colas De Impresión.
    - Análisis De Metadatos.
- Análisis De Una Imagen Sobre Plataforma Linux:
    - Estructura De Directorios En Linux.
    - Sistemas De Archivos.
    - Particiones.
    - Inode.
    - Antivirus En Linux.
    - Detección De Rootkits.
    - Ficheros Ocultos.
    - Análisis De Directorios.
    - Recuperación De Ficheros.

- Análisis De Una Imagen Con Autopsy:
    - Autopsy Para Windows.
    - Autopsy Para Linux.

- Análisis De Logs:
    - Análisis De Logs En Windows.
    - Análisis De Logs En Linux.
    - Herramientas Para Analizar Logs.
- Análisis Del Uso De Internet:
    - Análisis De Navegadores Web.
        - Internet Explorer
        - Mozilla Firefox
        - Google Chrome
- Análisis De Correos Electrónicos.
- El Informe Pericial:
    - Objeto.
    - Alcance.
    - Antecedentes.
    - Fuentes De Información Y Datos De Partida.

- Estándares Y Normas.
- Declaraciones.
- Limitaciones.
- Resolución.

**Módulo 6: 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.…)

## 7. METODOLOGÍA.

Con el fin de asegurar el máximo aprovechamiento del Máster, los alumnos tienen a su disposición la plataforma virtual específica para esta formación de The Security Sentinel 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 Máster.
- 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.

Tanto en la versión con sesiones presenciales como en la versión online, el Máster 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.

El módulo 6 de ISO 27001 se realiza en el Campus Virtual de IMQ Ibérica Business School.

**Proyecto Fin de Máster:** 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 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 Máster.

El objetivo del Proyecto Fin de Máster 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 Máster.

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

**7.1. MODALIDAD PRESENCIAL.** En la modalidad presencial las sesiones presenciales son eminentemente prácticas, el alumno cuenta con el apoyo de profesionales en activo que le guían y comparten su experiencia profesional. Método del caso, análisis y estudio de casos, como técnica de aprendizaje.

Al ser grupos reducidos, los alumnos reciben los conocimientos y punto de vista del profesor al mismo tiempo que interactúan con él y entre ellos mismos.

Los alumnos realizan un trabajo previo a las sesiones presenciales a través de la plataforma virtual. De esta forma, comprenden mejor los contenidos que comparte el ponente y pueden generar un debate más enriquecedor en un contexto creativo que ayuda a optimizar las sesiones presenciales. Los debates forman parte esencial de la metodología del Máster, como lo forman de la vida profesional del alumno.

El trabajo de investigación es primordial en la metodología del Máster y en el futuro profesional del alumno, potenciarán la dinámica de ampliar y reciclar los conocimientos y habilidades profesionales. El profesorado dará apoyo y guiará en los casos propuestos y el *feedback* sobre el trabajo realizado.

**7.2. METODOLOGÍA. Modalidad Virtual**

Llevamos a cabo la misma metodología que en el presencial, pero hacemos uso de la tecnología para poder asistir a clase a través de herramientas de videollamada en combinación con nuestro campus virtual (hecho en Moodle).

**7.3. 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 Master.

IMQ no establece ningún parámetro de calidad diferente para sus alumnos formados en modalidad presencial y para los alumnos formados en modalidad online. No existen diferencias entre los niveles de calidad exigidos a los participantes en ambas modalidades, tan solo los diferencia sus particularidades y necesidades.

## 8a. Calendario y duración. Modalidad Presencial/Virtual

**Duración:** 650 horas de clases teórico-prácticas. (equivalente a 40 ECTS)

Los alumnos de este Máster accederán a módulos complementarios y de refuerzo de formación online a través de la plataforma online de TSS. 200h se realizan de manera presencial en el aula de TSS. El modulo de ISO 27001 se realiza en el Campus Virtual de IMQ Ibérica Business School.

200h presenciales. Dedicación estimada fuera de aula: 350 horas de dedicación a trabajos prácticos y aula virtual y 100 horas al proyecto final.

**Número de Plazas:**

Con el objetivo de garantizar la calidad académica, el límite de plazas para el formato presencial se fija en un **mínimo de 6** y un máximo de 12.

En caso de no alcanzarse el número mínimo de plazas en el formato presencial/virtual, se pospondrá al alumno para la próxima convocatoria o se le dará la opción de realizar la versión online.

## 8b. Calendario y duración. Modalidad online

La duración del Máster en Sistemas de Gestión es de 650 horas, estimadas en 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 Máster. (40 ECTS)

**En el formato online no hay límite de plazas.**

## 9. Costes de inscripción

***Puede consultar el precio actual de cada modalidad en nuestra página web: www.imqibericaformacion.com así como las promociones vigentes de descuentos en la ficha del Máster / 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 Másteres y Cursos en cualquiera de sus modalidades.

## 10. Titulación y certificaciones

**"Máster Superior en Ciberseguridad y Hacking Ético"** *IMQ Ibérica Business School* con la colaboración de la Cátedra de Prevención de Riesgos Laborables y Salud Pública de la **Universidad de Córdoba y *The Security Sentinel***

· **Certificaciones profesionales:** 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 CPHEE** (Certificado Profesional de Hacking Ético Experto). Hacking Ético, Defensa en profundidad, Seguridad Web y Seguridad en redes inalámbricas.
- **Certificación CPAM** (Certificado Profesional de Auditoría Móviles) Auditorias móviles: análisis de APKs, recolección de información, rooteo del dispositivo.
- **Certificación CPSR** (Certificado Profesional de Seguridad en Redes) Configuración de Sistemas de Red, Defensa, Seguridad Perimetral y Seguridad en redes inalámbricas, así como la implantación de un Sistema de gestión de la Seguridad.
- **Certificación CPPP** (Certificado Profesional de Python para Pentesters) Programación de scripts basados en Python.
- **Certificación CPAIF** (Certificado Profesional de Análisis Informático Forense) Peritaje de entornos Informáticos como la participación en Juicios de faltas relacionadas con la Seguridad de la Información.

· **Auditor Interno en Ciberseguridad y Hacking Ético.**

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