THENAI
Technological Business School

CESN
COOPERACIÓN ESTRATÉGICA EN SEGURIDAD NACIONAL

Top CISO

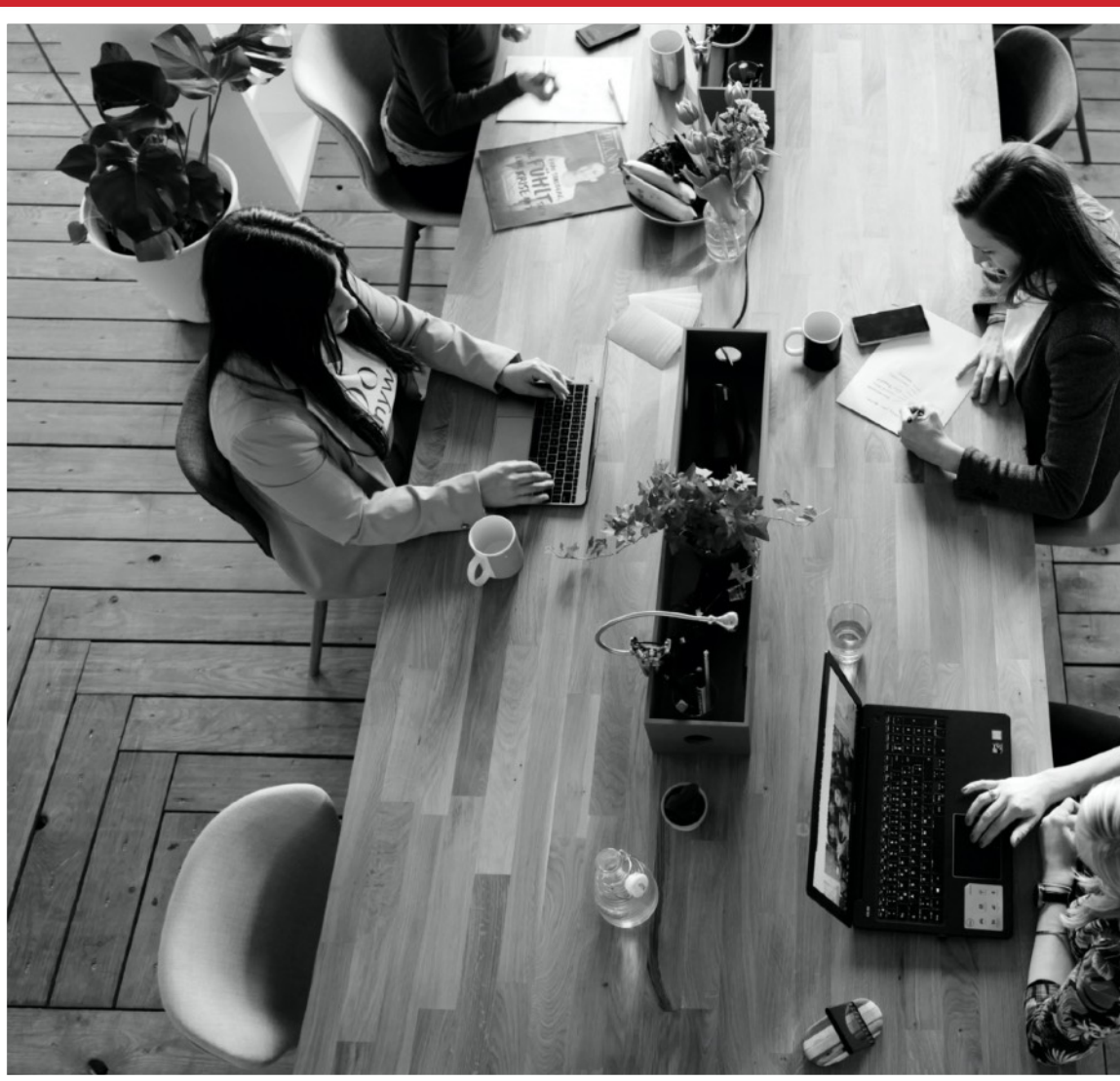
(Chief Information Security Officer)

Ciberseguridad en la era de la IA y la Computación Cuántica

1ª Edición

CCSP ISC2 · CISSP ISC2 · CompTIA Security+ · CompTIA CASP+ · Qiskit · Google Cloud Certified Professional Machine Learning Engineer · Google Cloud Certified Professional Data Engineer · Google Cloud Certified Professional Cloud Architect

Contenido



ΑTHENAI
Technological Business School

1

AthenAI Technological Business School

Una escuela para aquellos que realmente ***quieren aprender*** y están ***dispuestos a esforzarse***.

CESN: Cooperación Estratégica en Seguridad Nacional e infraestructuras críticas

Asociación dedicada a promover y apoyar el enfoque integral en seguridad Nacional y tecnologías emergentes, con un claro enfoque en la seguridad y protección de las infraestructuras criticas.

AthenAI Technological Business School

AthenAI es la escuela de excelencia tecnológica del CESN, especializada en formación avanzada en Inteligencia Artificial, Computación Cuántica, Blockchain, Servicios Cloud y Big Data.

¿Porqué estudiar en AthenAI?

AthenAI no es una escuela para cualquier estudiante,

AthenAI es una escuela para quienes realmente desean aprender y están dispuestos a asumir desafíos.

Aquí se profundiza, se debate y se investiga a fondo. Aquí **es posible suspender**, porque sin riesgo no hay aprendizaje auténtico. Porque los líderes no se forjan en aulas cómodas, sino en entornos exigentes que ponen a prueba su determinación y esfuerzo.

Una escuela para quienes no buscan títulos, sino trascender

AthenAI Technological Business School nació con la vocación de ser una knowledge and technology boutique: una institución selecta, rigurosa y profundamente conectada con los grandes desafíos del presente y del futuro.

En un contexto en el que abundan las fórmulas rápidas y los títulos superficiales, AthenAI se posiciona como la escuela de excelencia tecnológica para aquellos estudiantes dispuestos a recorrer un camino profundo, complejo y auténtico hacia un aprendizaje real. Aquí no se buscan atajos ni éxitos prefabricados, sino dejar huella a través del conocimiento, el esfuerzo y el compromiso genuino

Conocimiento, reputación y propósito: los tres pilares

En AthenAI no sólo se mide el conocimiento con **notas y certificaciones exigentes**, sino también con una métrica a largo plazo: la **reputación**. Cada alumno construirá su prestigio profesional dentro de una comunidad viva, donde la interacción constante con profesores, compañeros y egresados generará sinergias, oportunidades y desafíos. La reputación se podrá ganar, se podrá invertir en descuentos en programas, actualización de contenidos y accesos a conferencias, y también se podrá perder.

En AthenAI, el alumno es siempre el protagonista. Nuestro compromiso es **generar oportunidades reales** a través de proyectos exigentes y contactos estratégicos. Porque los estudiantes que llegan a AthenAI no vienen a conformarse con un empleo. Vienen decididos a **cambiar el curso de su vida**, a fundar **su propia start-up**, a **crear un unicornio**, a aparecer algún día en la **portada de Forbes**.

Una comunidad exclusiva, única en su especie.

AthenAI está diseñada como un **club selecto**, al estilo de instituciones como **Mensa** o **Forbes**. El acceso es restringido y la exigencia extremadamente alta. Aquí, la comunidad es una pieza esencial: alumnos, mentores y egresados interactúan en una red dinámica y transparente, donde el conocimiento y la reputación son visibles para todos.

Es un entorno en el que podrás colaborar, debatir, competir y crecer. Conocerás las fortalezas y debilidades de los demás, y ellos conocerán las tuyas. Aprenderás junto a ellos, competirás con ellos y, lo más importante, construirás relaciones profundas y duraderas que transformarán tu vida profesional y personal

Una escuela que es, en sí misma, un Unicornio

En esta escuela no vienes sólo a por un trabajo. Vienes a fundar tu unicornio. A crear algo de lo que puedas estar orgulloso el resto de tu vida. Porque el mundo necesita grandes ideas, y grandes personas.

AthenAI no sólo forma emprendedores, AthenAI es en sí misma un unicornio. Un modelo único, ambicioso, con vocación global y alma disruptiva. Es la escuela donde aprenden los líderes que cambiarán la sociedad a través de sus empresas y de su visión.

AthenAI: donde el fracaso es una posibilidad real.

A diferencia de otras escuelas, aquí puedes suspender, porque el verdadero aprendizaje implica asumir riesgos. Porque la mediocridad nace de la ausencia de consecuencias. Y porque quienes están destinados a liderar necesitan enfrentarse a la posibilidad real del fracaso antes de conquistar el éxito.

Inscribirse implica tener una oportunidad de superar el programa.
No la garantía de superarlo.

Una escuela con alma

AthenAI nació del cerebro de Zeus, combinando conocimiento, artes, justicia y estrategia. Su nombre no solo evoca sabiduría, sino también determinación y carácter.

Nuestra escuela nace con un propósito y un mensaje claro:

"Construye algo en lo que creas"

No se trata sólo de estudiar, sino de crear.

No se trata de trabajar, sino de liderar.

No se trata sólo de enseñar, sino de transformar al alumno en su mejor versión.

Se trata de separar a los líderes, de aquellos que no lo son.

Aquí empieza tu historia.

Bienvenido a AthenAI

ATHENAI
Technological Business School

2

Sobre el Máster

Lidera una nueva generación en sistemas de ciberseguridad a través de la ***Inteligencia Artificial*** y la ***Computación Cuántica***.

Top CISO: Dos másters que componen el programa más completo y exigente del mundo

Top CISO: la élite en ciberseguridad, Inteligencia Artificial y Computación Cuántica

Top CISO no es solo un programa formativo, es un reto intelectual de máxima exigencia diseñado para quienes aspiran a liderar el futuro de la ciberseguridad en la era de la Inteligencia Artificial y la Computación Cuántica. Con una estructura única en el mundo, combina excelencia académica, intensidad formativa y reconocimiento internacional, situándose como el estándar más alto en educación avanzada.

Cursando este programa, el alumno puede obtener dos títulos de máster:

- **CISO Essential**: 450 horas lectivas, equivalentes a 54 ECTS (primer año lectivo).
- **Top CISO**: 765 horas lectivas, equivalentes a 79 ECTS (segundo año lectivo).

Además, el programa **incorpora 8 certificaciones oficiales de primer nivel**, otorgadas por las entidades de referencia en cada disciplina:

Certificaciones CISO Essential:

- Certificación Security+ D5 (CompTIA Security+).
- Certificación CASP+ D5 (CompTIA Advanced Security Practitioner).
- Certificación CISSP D1 (Certified Information Systems Security Professional).
- Certificación CCSP D5 (Certified Cloud Security Professional).
- Professional Machine Learning Engineer (PMLE), emitida por Google.

Certificaciones Top CISO:

- Desarrollador en Computación Cuántica Qiskit 2, emitida por IBM.
- Professional Data Engineer (PDE), emitida por Google
- Professional Machine Learning Engineer (PMLE), emitida por Google

Los alumnos pueden decidir cursar únicamente el programa ***CISO Essential***, uno de los másteres más completos y exigentes disponibles en el mercado, capaz de transformar al alumno en un perfil altamente competitivo y diferencial.

Sólo quienes buscan trascender y convertirse en auténticos referentes globales, afrontarán el desafío del ***Top CISO***. Este programa integral exige haber superado previamente el Essential y representa la cumbre de la formación en Ciberseguridad, Computación Cuántica e Inteligencia Artificial Aplicada.

Top Quant no se estudia: SE CONQUISTA

Objetivo

El **objetivo por parte de la escuela** es hacer honor e la excelencia de la institución, ofreciendo a los alumnos el mejor programa del mundo en nuevas tecnologías aplicadas a la ciberseguridad.

El **objetivo** de cursar el máster **por parte de los alumnos** suele ser uno de los tres siguientes:

- Dar un salto cualitativo y cuantitativo, en salario, respecto a la situación anterior.
- Evitar la obsolescencia tecnológica teniendo un salario ya elevado.
- Entrar en el mercado laboral con una formación claramente diferencial.

Naturaleza del máster

El máster nace fruto de una necesidad empresarial.

No hay expertos con conocimientos en profundidad en: Programación, Ciberseguridad, Derecho tecnológico, ServiciosCloud & Big Data, Inteligencia Artificial, Blockchain y Computación Cuántica.

A las empresas les resulta **muy difícil contratar a un CISO (Chief Information Security Officer)** con certificaciones en ciberseguridad, conocimientos avanzados en Inteligencia Artificial, y con conocimientos profundos en Computación Cuántica. Por lo que es uno de los perfiles más demandados y mejor pagados, tanto en el sector financiero e infraestructuras críticas, como en el ministerio de Defensa.

La orientación no académica, sino profesional, es una de las principales diferencias con cualquier otro máster. No se busca cubrir un temario para otorgar un título. Se busca dotar a los alumnos de los conocimientos y habilidades más punteras de la industria, trabajando con las mismas herramientas y datos que usarán en los mejores laboratorios de ciberseguridad de la industria.

El objetivo es ***"identificar a quién hay que contratar"***.

Conocimientos previos necesarios

No se requiere experiencia previa para inscribirse en el máster, pero sí compromiso y mucha dedicación.

A lo largo del programa el estudiante desarrollará las habilidades y adquirirá conocimientos en programación, ciberseguridad, Big Data y servicios Cloud, Inteligencia Artificial Avanzada, Blockchain y Computación Cuántica.

Este máster es para ti si vas a dedicar un **mínimo de 4 horas de estudio al día**.

Perfiles de acceso

El máster está diseñado para formar a profesionales y estudiantes procedentes de distintos ámbitos, todos ellos con un denominador común: el deseo de convertirse en expertos en ciberseguridad avanzada, con competencias reales en Inteligencia Artificial, Blockchain y Computación Cuántica.

a) Perfil técnico (informáticos, ingenieros, físicos, matemáticos...)

Si vienes de una carrera técnica como ingeniería informática, telecomunicaciones, física o matemáticas, es probable que tengas una buena base en programación, cálculo y sistemas. Sin embargo, es probable que no hayas profundizado en:

- Normativas internacionales de ciberseguridad.
- Técnicas avanzadas de ciberdefensa ofensiva y defensiva.
- Inteligencia artificial aplicada a detección de amenazas.
- Seguridad cuántica, post-cuántica y blockchain.

Este máster es para ti si quieres liderar el desarrollo de soluciones seguras en entornos complejos (cloud, IoT, entornos regulados), con una visión integral y realista del ecosistema empresarial.

b) Perfil financiero, jurídico o de auditoría

Si vienes del mundo de la auditoría, compliance, finanzas, dirección de empresas o derecho, probablemente tengas sólidos conocimientos normativos y organizativos, pero una formación limitada en tecnología avanzada, ciberseguridad técnica e IA aplicada.

Este máster es para ti si quieres:

- Entender técnicamente los riesgos y controles que afectan a tu sector.
- Hablar el mismo lenguaje que los equipos técnicos y de defensa digital.
- Liderar la transformación segura en sectores como banca, aseguradoras o grandes despachos.

c) Perfil operativo o institucional (infraestructuras críticas, cuerpos del Estado, Defensa…)

Si trabajas en una infraestructura crítica, en el Ministerio de Defensa, Interior o servicios esenciales, probablemente ya tengas experiencia en gestión de incidentes, análisis de riesgos o entornos altamente regulados. Sin embargo, es frecuente que no hayas tenido acceso a:

- Herramientas ofensivas/defensivas de última generación.
- Aplicaciones de IA generativa y machine learning en defensa.
- Desarrollo de algoritmos post-cuánticos y seguridad criptográfica avanzada.

Este máster te dará acceso a conocimientos reservados a los laboratorios más avanzados de ciberinteligencia del mundo y te posicionará para diseñar y ejecutar proyectos de seguridad crítica a nivel nacional e internacional.

El programa del máster ha sido cuidadosamente diseñado para nivelar las competencias de los alumnos en los primeros módulos, garantizando que todos los perfiles alcancen una base común en programación, seguridad, IA y fundamentos cuánticos.

Metodología

El programa se fundamenta en el principio de: Se aprende con las manos.

Todas las clases tienen un enfoque práctico, huyendo del profesor que lee cientos de diapositivas y donde el alumno sale de clase sin haber aprendido realmente nada.

Todas las clases están sustentadas en un poco de teoría y muchos ejercicios de dificultad creciente.

Siguiendo este enfoque, el máster no tiene exámenes sino prácticas. Al finalizar cada bloque de conocimiento los alumnos reciben el enunciado de una práctica, el cual se llevan a casa durante 3 semanas.

El objetivo es simular un entorno de trabajo. En la vida real tu responsable no te quita los libros, ni internet, sino que viene con un problema complejo y necesita una solución.

Los alumnos contarán en todo momento con los apuntes, internet, foros, tutores, la grabación de las clases, acceso a ChatGPT, etc. Las mismas herramientas que tendrán en su vida profesional, una vez terminen el programa.

Las prácticas serán desafiantes y enfocadas en problemas reales del mundo de la ciberseguridad. Los alumnos deberán investigar y probar diversas aproximaciones hasta que consigan resolver cada ejercicio. Y ese aprendizaje se les quedará para toda la vida.

Los alumnos deberán tener la nota media de las prácticas aprobada para poder presentar el trabajo de fin de máster.

Todos los alumnos deberán defender su TFM ante un tribunal.

Atención tutorial: Al ser un programa de alto rendimiento, donde los alumnos deben utilizar constantemente los conocimientos adquiridos, la atención tutorial es fundamental.

Todos los alumnos tendrán acceso a la plataforma web, donde constará la documentación y ejercicios, así como un foro donde exponer sus inquietudes. Además de disponer del mail de todos los profesores, con los que cerrar tutorías libremente, también contarán con el teléfono móvil del director académico para solventar cualquier problema de manera inmediata.

Dado que las prácticas están diseñadas para que sean un reto, desde el profesorado se habla constantemente con todos los alumnos para medir el nivel de aprendizaje – frustración que están experimentando. En los casos en los que observamos un deterioro en la evolución de las notas, nos entrevistamos con el alumno para determinar si esa evolución responde a que no está estudiando a diario, u a otra razón.

Los alumnos contarán con un tutor que les oriente y guíe constantemente.

Dirección académica

Ginés Carrascal de las Heras

Ingeniero de Materiales y Licenciado en física, óptica y electrónica por la Universidad de Salamanca, donde también realizó cursos de Doctorado, Comunicaciones y Medio Ambiente. **Máster en Microanálisis espectral con LASER por la Universidad de Holguín**

Quantum Computational Scientist & Architect en IBM Quantum desde el año 2000, ayudando a hacer realidad la computación cuántica para mejorar el negocio de sus clientes:

- **IBM Quantum Ambassador**
  - Contribuye a la difusión y adopción de la computación cuántica en empresas y universidades.
  - Miembro destacado del laboratorio de Investigación Cuántica de IBM
  - Forma parte de los Servicios de Industria y Tecnología Cuántica de IBM.
- **IBM Architect**
  - Construye y lidera equipos de desarrollo de alto rendimiento con RTC, SOA, Java y web. Certificado como Scrum Master y en TOGAF 9.
  - Ha adquirido numerosas Licencias y certificaciones a lo largo de su carrera profesional, entre las que destacan:
    - IBM Certified Associate Developer - Quantum Computation using Qiskit v0.2X
    - Qiskit Advocate
    - IBM Quantum Machine Learning
    - IBM Variational Algorithm Design
    - Qiskit Global Summer School 2022 - Quantum Excellence
    - IBM Basics of Quantum Information
    - IBM Security and Privacy by Design Foundations
    - IBM Quantum-Safe Conversations
    - AWS Certified Solutions Architect – Associate

Posee más de 70 certificaciones, que podrá consultar en el siguiente enlace.

Apasionado por compartir su amplio conocimiento en Computación Cuántica y Machine Learning, trabaja como **Profesor** en:

- La Facultad de Matemáticas de la Universidad Francisco de Vitoria (desde 2021)
- El Centro Universitario CESTE, Escuela Internacional de Negocios (desde 2021)
- La Universidad Europea (desde 2022)
- En el Máster en Inteligencia Artificial aplicada a los Mercados Financieros (mIA-X) en el Instituto BME (desde 2022)
- La Universidad Carlos III de Madrid:
  - Departamento de Física - Quantum Computing (2022 - 2024)
  - Departamento de Informática - Applied Artificial Intelligence Group (2014 - 2022)
- La Facultad de Matemáticas de la Universidad Complutense de Madrid (2018 - 2024)

Dirección académica

Eva Álvarez del Manzano

Formación Académica:

- Licenciada en Filosofía y Psicología.
- Postgrado en Psicología, especializada en estrés postraumático en zonas de conflicto.
- Administración y Dirección de Seguridad, habilitada por el Ministerio del Interior.
- **Doctora Honoris Causa en Criminología**.
- Tecnologías de la Información y las Comunicaciones para la Alta Dirección, en áreas clave como ciberseguridad, transformación digital y el impacto de las TIC en la toma de decisiones estratégicas.

Trayectoria Profesional:

- **Fundadora y presidenta de CESN** (Cooperación Estratégica en Seguridad Nacional e Infraestructuras Críticas), asociación dedicada en promover y apoyar el enfoque integral en Seguridad Nacional y tecnologías emergentes.
- CEO y fundadora de Auralma Soluciones, consultora especializada en seguridad integral, inteligencia, cumplimiento normativo y gestión de crisis.
- Responsable de Proyectos Especiales en el Grupo Edefa, editorial técnica especializada en defensa, seguridad y geoestrategia (defensa.com).
- **Más de 20 años de experiencia como Asesora estratégica en proyectos de desarrollo tecnológico y operaciones de alta seguridad, incluyendo la colaboración con organismos internacionales y empresas del sector estratégico (Ministerio de Defensa, CNI, NASA…)**:
  - Jefa de Seguridad en el sector aeroespacial (ISDEFE - INSA - NASA), coordinando la seguridad en instalaciones estratégicas, así como el análisis y gestión de amenazas.
  - Ha diseñado la pala palpador de desminado Jimmy y el brazo robotizado de desactivación de explosivos aunav.CID, herramientas innovadoras para la detección y desactivación de artefactos explosivos improvisados (IEDs), en colaboración con el Centro Internacional de Desminado.
  - Asesora en Diseño de Vehículos Militares Ultraligeros.
  - Ha trabajado en proyectos de protección de infraestructuras críticas, diseño de planes de emergencia y análisis de amenazas híbridas y cibernéticas.

Reconocimientos y Méritos:

- Vicepresidenta de la Comisión de Méritos y Grados en la Asociación de Peritos de Nuevas Tecnologías (PETEC).
- Participante y organizadora en actos institucionales sobre ciberdefensa, incluyendo la Medalla al Mérito en la Ciberdefensa.
- Invitada frecuente a foros de alto nivel sobre seguridad nacional, defensa, crimen organizado y ciberinteligencia.

Presencia en medios y divulgación:

- Colaboradora en entrevistas y reportajes sobre ciberacoso, protección digital y amenazas híbridas en medios como EITB, Defensa.com y TecFuturo.
- Defensora del enfoque humano y psicológico en la gestión de riesgos tecnológicos.
- Ponente en eventos nacionales e internacionales de ciberseguridad, abordando:
  - C1b3rWall: temas relacionados con la ciberseguridad y la protección de infraestructuras críticas.
  - CSI Radar 2023 (organizado por el Grupo Edefa): temas de seguridad y defensa.

Estructura del programa

Cada 6 meses actualizamos los contenidos del máster, ofreciendo ***SIEMPRE*** contenidos realmente punteros.

Estructura del Programa completo

Módulos	Horas lectivas	Peso	Horas estudio	Horas totales	ECTS
0. Presentación y sesiones TFM	30	2 %	60	90	**3,6**
1. Fundamentos de programación	55	5 %	110	165	**6,6**
2. Fundamentos de IA, Machine Learning y Deep Learning	110	9 %	220	330	**13,2**
3. Ciberseguridad y Hacking Ético	315	26 %	630	945	**37,8**
4. Derecho tecnológico	55	5 %	110	165	**6,6**
5. Ciberseguridad Cuántica	245	20 %	490	735	**29,4**
6. Servicios Cloud y Big Data	180	15 %	360	540	**21,6**
7. Inteligencia Artificial Aplicada a la Ciberseguridad	225	19 %	450	675	**27**
Total	**1.215**	**100 %**	**2.430**	**3.645**	**146**

Estructura del Máster ESSENTIAL

Módulos	Horas lectivas	Peso	Horas estudio	Horas totales	ECTS
0. Presentación y sesiones TFM	15	3 %	30	45	**1,8**
1. Fundamentos de programación	55	12 %	110	165	**6,6**
2. Fundamentos de IA, Machine Learning y Deep Learning	105	23 %	210	315	**12,6**
3. Ciberseguridad y Hacking Ético	205	46 %	410	615	**24,6**
4. Servicios Cloud y Big Data	70	16 %	140	210	**8,4**
Total	**450**	**100 %**	**900**	**1.350**	**54**

Estructura del Máster TOP

Módulos	Horas lectivas	Peso	Horas estudio	Horas totales	ECTS
0. Presentación y sesiones TFM	15	2 %	30	45	**1,8**
1. Ciberseguridad y Hacking Ético	110	14 %	220	330	**13,2**
2. Servicios Cloud y Big Data	110	14 %	220	330	**13,2**
3. Derecho tecnológico	55	7 %	110	165	**6,6**
4. Ciberseguridad Cuántica	245	32 %	490	735	**29,4**
5. Inteligencia Artificial Aplicada a la Ciberseguridad	230	30 %	460	675	**27,6**
Total	**765**	**100 %**	**1.530**	**2.295**	**92**

Programa ESSENTIAL

Módulo 1 | Fundamentos de programación
55 horas lectivas

Visión General del programa
- Presentación y alineación de objetivos
- Tecnologías emergentes en ciberseguridad
- Business case (búsqueda de coherencia en la aplicación tecnológica)

Fundamentos de programación en Python I
- Instalación
- Jupyter Notebooks
- Sintaxis básica, operaciones y tipos básicos
- Strings
- Estructuras de datos: Lists, Tuples, Sets y Diccionarios

Fundamentos de programación en Python II
- Control Flow
- Dict and List comprehensions
- Exceptions
- Funciones
- Modulos y Scripts
- Escritura de ficheros de texto y guardado de variables

Fundamentos de programación en Python III
- Librería Numpy

Fundamentos de programación en Python IV
- Librería Pandas

Fundamentos de programación en Python V
- Tratamiento de series temporales
- Simulación para medición de riesgos (VaR)
- Optimización de carteras

Fundamentos de programación en Python VI
- Visualización de datos con Matplotlib
- Visualización de datos con Pandas
- Visualización de datos con Seaborn
- Visualización de datos financieros
- Visualización interactiva con ipywidgets
- Adquisición y guardado de datos.

Fundamentos de programación en Python VII
- Programación orientada a objetos
- Herencia
- Decoradores

Fundamentos de programación en Python VIII
- Introducción a HTML
- Web Scraping

Fundamentos de programación en Python IX
- Fundamentos de bases de datos relacionales
  - Creando y manipulando sus propias bases de datos
  - Importación de datos relacionales en Python
  - Filtros, ordenamientos y agrupamientos en las consultas
- Consultas avanzadas de SQLAlchemy
- Introducción a MongoDB en Python

Fundamentos de programación en Python X
- Análisis de eficiencia
- Gestión de errores, Testing y Debugging
  - Tipos de pruebas (unitarias, integración, funcionales y pruebas de aceptación)
  - Herramientas de testing (pytest y unittest)
  - Debugging (stack traces, breakpoints y observación de variables)
- IDEs, más allá de JupyterLab

Técnicas de visualización avanzadas
- Introducción a HTML
- Introducción a CSS
- Introducción a Flask
- Interfaces interactivas con Dash

Módulo 2 | Fundamentos de Inteligencia Artificial, Machine Learning y Deep Learning
105 horas lectivas

Algoritmos genéticos
- Función objetivo
- Estrategias de selección
- Cruzamiento
- Mutación
- Reemplazo generacional

Algoritmos enjambre
- Colonia de hormigas (algoritmo ACO)
  - Construcción del entorno
  - Selección del camino
  - Cantidad de feromona
  - Evaporación
  - Poda de la solución óptima

Lógica difusa
- Conjuntos difusos y grados de pertenencia
- Operadores difusos
- Creación de reglas
- Fuzzificación
- Defuzzicación

Machine Learning I
- Introducción al ML
  - IA vs ML
  - Supervisado vs no supervisado
  - Clasificación vs Regresión
  - Modelos Paramétricos vs No Paramétricos
  - Modelos Lineales vs No Lineales
- Ejemplos de aplicaciones financieras usando ML
- K-Nearest Neighbors (KNN)
- Árboles de decisión
  - Ejemplo sencillo con árboles
  - XAI de árboles aplicados a finanzas

Machine Learning II
- Preprocesado y métricas de evaluación
  - Normalización y estandarización
  - Codificación, etiquetado y discretización (dummies)
  - Missing values, outliers y NaNs
  - Aproximación a series temporales como bloques de secuencias
  - Métricas de evaluación: Matriz de confusión. Precisión, recall.
  - Validación simple y cruzada
- Reducción de la dimensión
  - La maldición de la dimensión
  - Reducción de dimensionalidad: Selección de atributos y componentes principales: PCA y LDA

Machine Learning III
- Modelos de clasificación más complejos
- Teoría Bayesiana: Naive Bayes
- Conjuntos de clasificadores: Bagging, boosting, random forest y gradient boosting
- Máquinas de Soporte Vectorial (SVMs)

Machine Learning IV
- Clustering jerárquico aglomerativo
  - Definición (tipos de linkage)
  - Implementación manual
  - Ejemplo sencillo con clustering aglomerativo
- Clustering basado en centroides: K-Means y K-Medoids
  - Definición e implementación manual
  - Ejemplo sencillo con K-Means
  - Interpretación de los centroides como representantes
- Clustering basado en Gaussianas: EM
  - Definición (generalización de K-Means)
- Clustering basado en densidades: DBSCAN
  - Definición y ejemplo sencillo con DBSCAN
- Comparación de algoritmos de clustering
  - Métricas de comparación
  - Selección del algoritmo de clustering apropiado
  - Ejemplos de comparación
- Clustering de activos mediante correlaciones y mediante momentum

Machine Learning V
- Caso práctico: Clustering de fondos de inversión mediante atributos cuantitativos
  - Generación de características
  - Extracción de atributos relevantes
  - Reducción de dimensionalidad incorporando XAI
  - Clustering de fondos de inversión
  - Graphext (No-Code para data analysis)
  - XAI de los resultados obtenidos

Redes Neuronales I: Redes neuronales densas
- Introducción
- Entorno de trabajo
- Conceptos básicos
- Regresión lineal
- Descenso por gradiente
- Regresión logística
- Modelos no lineales

Redes Neuronales II
- Introducción a las redes neuronales
- Redes neuronales feedforward
- Implementación de una red neuronal (parte forward)
- Regla de la cadena de la derivada
- Retropropagación

Redes Neuronales III
- Implementación de una red neuronal (parte backward)
- Introducción a Keras y PyTorch
- Diferenciación automática

Redes Neuronales IV
- Implementación de una red neuronal con Keras y PyTorch
- Entrenamiento de una red neuronal
- Descenso por gradiente estocástico
- Función de coste
- Función de activación
- Optimización de carteras usando el descenso por gradiente

Redes Neuronales V
- Regularización
- Inicialización de los pesos
- Batch normalization
- Otras técnicas de optimización
- Métodos de segundo orden

Redes Neuronales VI
- Optimización de Hiperparámetros
- Métricas de evaluación
- Validación cruzada
- Grid search
- Keras Tuner
- HParams dashboard

Redes convolucionales I
- Tamaño del kernel
- Tamaño del paso y padding
- Maxpooling
- Número de filtros y características
- Dropout

Redes convolucionales II
- Construcción en Keras
- Optimización del kernel
- Optimización del paso y padding
- Maxpooling
- Optimización del filtros y características
- Dropout
- Redes 1D, 2D, 3D

Redes convolucionales III
- Medidas de distancia entre imágenes
- Redes siamesas y filtrado de imágenes basado en contenido (CBIR)
- Aprendizaje de representaciones por CNN
- Aplicaciones en búsqueda de imágenes
- Robustez de las redes

- Adversarial examples

Redes convolucionales IV

- Ataques basados en perturbaciones de entradas: one-pixel-attack
- Métodos de entrenamiento adversarial: evolución diferencial (DE)
- Aplicaciones en generación de modelos robustos
- Redes Yolo
- RAM (Recognize Anything)

Redes recurrentes I

- Redes con memoria
- El problema de las dependencias a largo plazo
- Redes LSTM en Tensorflow y Keras
- Variantes de LSTM

Redes recurrentes II

- Backpropagation truncada
- Acumulando LSTM
- LSTM bidireccionales
- Forecasting con LSTM: time series, secuencias y predicciones

Estado del arte de la Inteligencia Artificial

- Inspiración y lineas de Investigación para los proyectos de fin de máster

Módulo 3 | Ciberseguridad y Hacking Ético
205 horas lectivas

Fundamentos de Seguridad I: Conceptos Básicos de Seguridad

- Tríada CIA (Confidencialidad, Integridad, Disponibilidad)
- Términos y definiciones fundamentales
- Evolución de la seguridad de la información
- Marco regulatorio y estándares internacionales
  - Relevancia: CISSP (D1), Security+ (D1), CASP+ (D5), CCSP (D1)

Fundamentos de Seguridad II: Gestión de Riesgos Fundamentales

- Identificación y análisis de riesgos
- Evaluación de vulnerabilidades
- Gestión de amenazas y contramedidas
- Análisis de impacto en el negocio (BIA)
  - Relevancia: CISSP (D1), Security+ (D5), CASP+ (D1), CCSP (D1)

Fundamentos de Seguridad III: Arquitectura y Modelos de Seguridad

- Modelos de referencia (OSI, TCP/IP)
- Modelos de control de acceso (DAC, MAC, RBAC, ABAC)
- Arquitecturas de defensa en profundidad
- Zonificación y segmentación de redes
  - Relevancia: CISSP (D3), Security+ (D3), CASP+ (D1), CCSP (D1)

Fundamentos de Seguridad IV: Controles de Seguridad y Categorización

- Tipos de controles (administrativos, técnicos, físicos)
- Controles preventivos, detectivos y correctivos
- Implementación de controles basados en riesgos
- Evaluación de efectividad de controles
  - Relevancia: CISSP (D1, D8), Security+ (D5), CASP+ (D5), CCSP (D1)

Seguridad en Redes e Infraestructura I: Fundamentos de Seguridad de Redes

- Protocolos de seguridad de red
- Diseño seguro de redes
- Dispositivos de seguridad de red (firewalls, IDS/IPS)
- Defensa contra ataques comunes de red
  - Relevancia: CISSP (D4), Security+ (D3), CASP+ (D2)

Seguridad en Redes e Infraestructura II: Seguridad de Endpoints y Sistemas

- Hardening de sistemas operativos
- Protección de endpoints
- Sistemas de detección y prevención de intrusiones
- Gestión de parches y actualizaciones
  - Relevancia: CISSP (D3), Security+ (D2), CASP+ (D2)

Seguridad en Redes e Infraestructura III: Arquitecturas Avanzadas de Seguridad

- Implementación de arquitecturas Zero Trust
- Microsegmentación
- SDN (Software Defined Networking)
- Arquitecturas de red adaptativas
  - Relevancia: CISSP (D3), Security+ (D3), CASP+ (D1)

Seguridad en Redes e Infraestructura IV: Criptografía y PKI

- Principios criptográficos fundamentales
- Algoritmos y protocolos criptográficos
- Infraestructura de clave pública (PKI)
- Gestión de certificados digitales
  - Relevancia: CISSP (D3), Security+ (D6), CASP+ (D2), CCSP (D2)

Seguridad en Redes e Infraestructura V: Seguridad Física y Ambiental

- Controles de acceso físico
- Protección ambiental
- Seguridad del personal
- CCTV y sistemas de vigilancia
  - Relevancia: CISSP (D7), Security+ (D3), CASP+ (D1), CCSP (D3)

Seguridad en la Nube y Virtualización I: Fundamentos de Computación en la Nube

- Modelos de servicio (IaaS, PaaS, SaaS)
- Modelos de despliegue (público, privado, híbrido)
- Arquitecturas de referencia para la nube
- Responsabilidades compartidas
  - Relevancia: CISSP (D3), Security+ (D3), CASP+ (D2), CCSP (D1)

Seguridad en la Nube y Virtualización II: Seguridad en Arquitecturas Cloud

- Diseño de arquitecturas seguras en la nube
- Contenedores y microservicios
- Orquestación y seguridad
- DevSecOps en entornos cloud
  - Relevancia: CISSP (D3), Security+ (D3), CASP+ (D2), CCSP (D3)

Seguridad en la Nube y Virtualización III: Virtualización y Seguridad
- Hipervisores y seguridad de máquinas virtuales
- Ataques específicos a entornos virtualizados
- Controles de seguridad en virtualización
- Seguridad de contenedores
  - Relevancia: CISSP (D3), Security+ (D3), CASP+ (D2), CCSP (D3)

Seguridad en la Nube y Virtualización IV: Gestión de Identidades y Accesos en la Nube
- IAM en entornos cloud
- Single Sign-On y federación de identidades
- Gestión de privilegios en la nube
- Autenticación multifactor en entornos cloud
  - Relevancia: CISSP (D5), Security+ (D6), CASP+ (D2), CCSP (D3)

Seguridad en la Nube y Virtualización V: Operaciones de Seguridad en la Nube
- Monitoreo y logging en entornos cloud
- Automatización de seguridad en la nube
- Respuesta a incidentes en la nube
- Backup y recuperación en entornos cloud
  - Relevancia: CISSP (D7), Security+ (D4), CASP+ (D3), CCSP (D4)

Seguridad de Datos y Aplicaciones I: Protección de Datos
- Clasificación de datos
- Controles de protección de datos
- Ciclo de vida de los datos
- DLP (Data Loss Prevention)
  - Relevancia: CISSP (D2), Security+ (D2), CASP+ (D1), CCSP (D2)

Seguridad de Datos y Aplicaciones II: Criptografía Aplicada a la Protección de Datos
- Cifrado de datos en reposo
- Cifrado de datos en tránsito
- Gestión de claves
- Tokenización y enmascaramiento
  - Relevancia: CISSP (D2), Security+ (D6), CASP+ (D2), CCSP (D2)

Seguridad de Datos y Aplicaciones III: Seguridad en el Desarrollo de Software
- SDLC seguro
- Evaluación de seguridad de aplicaciones
- Análisis de código estático y dinámico
- DevSecOps
  - Relevancia: CISSP (D8), Security+ (D2), CASP+ (D4), CCSP (D4)

Seguridad de Datos y Aplicaciones IV: Seguridad de Aplicaciones Web y APIs
- Vulnerabilidades comunes (OWASP Top 10)
- Seguridad de APIs
- Servicios web seguros
- WAF y controles de aplicación
  - Relevancia: CISSP (D8), Security+ (D2), CASP+ (D4), CCSP (D3)

Operaciones de Seguridad y Respuesta a Incidentes I: Gestión de Operaciones de Seguridad
- SOC (Centro de Operaciones de Seguridad)
- SIEM y herramientas de monitoreo
- Gestión de logs y eventos
- Gestión de vulnerabilidades
  - Relevancia: CISSP (D7), Security+ (D4), CASP+ (D3), CCSP (D4)

Operaciones de Seguridad y Respuesta a Incidentes II: Respuesta a Incidentes
- Planes y procedimientos de respuesta
- Contención, erradicación y recuperación
- Análisis post-incidente
- Equipos de respuesta (CSIRT)
  - Relevancia: CISSP (D7), Security+ (D4), CASP+ (D3), CCSP (D4)

Operaciones de Seguridad y Respuesta a Incidentes III: Análisis Forense Digital
- Adquisición y preservación de evidencia
- Análisis forense de redes
- Análisis forense de sistemas
- Análisis forense en la nube
  - Relevancia: CISSP (D7), Security+ (D4), CASP+ (D3), CCSP (D4)

Operaciones de Seguridad y Respuesta a Incidentes IV: Continuidad del Negocio y Recuperación ante Desastres
- Planificación de continuidad del negocio
- Estrategias de recuperación ante desastres
- Pruebas y ejercicios de DR/BC
- Continuidad en entornos cloud
  - Relevancia: CISSP (D1), Security+ (D5), CASP+ (D3), CCSP (D4)

Gobierno, Riesgo y Cumplimiento I: Gobierno de Seguridad
- Políticas, estándares y procedimientos
- Marcos de gobierno de TI
- Métricas y KPIs de seguridad
- Comités de seguridad
  - Relevancia: CISSP (D1), Security+ (D5), CASP+ (D5), CCSP (D5)

Gobierno, Riesgo y Cumplimiento II: Gestión Avanzada de Riesgos
- Análisis cuantitativo vs. cualitativo
- Estrategias de mitigación de riesgos
- Riesgos de terceros y cadena de suministro
- Comunicación de riesgos
  - Relevancia: CISSP (D1), Security+ (D5), CASP+ (D5), CCSP (D5)

Gobierno, Riesgo y Cumplimiento III: Cumplimiento y Aspectos Legales
- Regulaciones clave (GDPR, HIPAA, PCI-DSS, etc.)
- Auditorías de seguridad
- Contratos y acuerdos (SLA, DPA)
- Privacidad de datos
  - Relevancia: CISSP (D1), Security+ (D5), CASP+ (D5), CCSP (D5, D6)

Preparación para la Certificación Security+
- Revisión de los 6 dominios del Security+
- Estrategias para el examen
- Preguntas prácticas
- Simulacro de examen

Security+ - 6 Dominios:

- D1: Ataques, Amenazas y Vulnerabilidades
- D2: Arquitectura y Diseño
- D3: Implementación
- D4: Operaciones y Respuesta a Incidentes
- D5: Gobierno, Riesgo y Cumplimiento
- D6: Criptografía y PKI

Preparación para la Certificación CISSP

- Revisión de los 8 dominios del CISSP
- Estrategias para el examen
- Preguntas prácticas
- Simulacro de examen

CISSP - 8 Dominios:

- D1: Gestión de Seguridad y Riesgos
- D2: Seguridad de Activos
- D3: Arquitectura e Ingeniería de Seguridad
- D4: Seguridad de Comunicaciones y Redes
- D5: Gestión de Identidades y Accesos
- D6: Evaluación y Pruebas de Seguridad
- D7: Operaciones de Seguridad
- D8: Seguridad en el Desarrollo de Software

Preparación para la Certificación CASP+

- Revisión de los 5 dominios del CASP+
- Estrategias para el examen
- Preguntas prácticas
- Simulacro de examen

CASP+ - 5 Dominios:

- D1: Arquitectura de Seguridad
- D2: Operaciones e Infraestructura de Seguridad
- D3: Integración de Seguridad de Sistemas y Aplicaciones
- D4: Respuesta a Incidentes y Gestión de Riesgos
- D5: Gobierno, Riesgo y Cumplimiento

Preparación para la Certificación CCSP

- Revisión de los 6 dominios del CCSP
- Estrategias para el examen
- Preguntas prácticas
- Simulacro de examen

CCSP - 6 Dominios:

- D1: Conceptos, Arquitectura y Diseño de Computación en la Nube
- D2: Seguridad de Datos en la Nube
- D3: Seguridad de Plataforma e Infraestructura en la Nube
- D4: Seguridad de Aplicaciones en la Nube
- D5: Operaciones de Seguridad en la Nube
- D6: Legal, Riesgo y Cumplimiento

Operaciones – Threat

- Modelado de Amenazas y Comprensión de Adversarios
- Técnicas y Procedimientos (TTPs)
- STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)
- DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability)
- Fases de un ataque cibernético: reconocimiento, obtención de acceso inicial, ejecución de código, persistencia, escalada de privilegios, movimiento lateral, exfiltración de datos y la evasión de defensas
- Framework MITRE ATT&CK: mapear y analizar las TTPs de los adversarios, identificando patrones de ataque y desarrollando estrategias de mitigación y defensa
  - Adversarios Relevantes: Adversarios Estatales y No Estatales

DFIR – Respuesta (Digital Forensics and Incident Response)

- Tipos de incidentes: malware, ataques de denegación de servicio (DDoS), intrusiones de red, robo de datos y abuso interno
- Preparación, identificación, contención, erradicación, recuperación
- Políticas de seguridad, procedimientos operativos estándar (SOP) y equipos de respuesta a incidentes (IRT)
- Sistemas de detección y prevención de intrusiones (IDS/IPS)
- Sistemas de gestión de eventos e información de seguridad (SIEM)
- Estrategias para limpiar sistemas infectados

Operaciones – Red Team

- Reconocimiento, enumeración, explotación, escalada de privilegios, movimiento lateral, persistencia y exfiltración de datos
- Metasploit, Cobalt Strike y PowerShell Empire
- Ingeniería Inversa y Exploiting
  - Desensambladores (IDA Pro, Ghidra) y depuradores (OllyDbg, x64dbg)
  - Ingeniería inversa de malware (comportamiento y características)
  - Técnicas de explotación: desbordamiento de búfer, inyección de código y escalada de privilegios
  - Compiladores y reconstrucción de código
  - Formatos de ficheros binarios y enlazadores dinámicos
  - Análisis dinámico: Depuradores de código
  - Caja Negra: Análisis de comportamiento
  - Caja Blanca: Depuradores de código

Operaciones – Blue Team

- Estrategias, técnicas y herramientas para defender una organización contra amenazas cibernéticas
  - Seguridad Perimetral On-Premise
  - Seguridad en la Nube
- Detección, Correlación y Acción
  - SIEM, EDR y NDR
- Protección de Infraestructuras Críticas
- Gestión de Identidad y Autenticación
- Centro de Operaciones de Seguridad (SOC)

Hacking Ético I: Introducción al Hacking Ético

- Definición y alcance del hacking ético
- Diferencias entre hacker ético, white hat, black hat y grey hat
- Marco legal y consideraciones éticas
- Metodologías y estándares (OSSTMM, PTES, OWASP)

Hacking Ético II: Reconocimiento y Recolección de Información

- Técnicas de footprinting pasivo
- OSINT (Open Source Intelligence)
- Herramientas de reconocimiento (Shodan, Maltego,

theHarvester)
- Análisis de metadatos y fuentes públicas

Hacking Ético III: Escaneo de Redes y Enumeración
- Descubrimiento de hosts y servicios
- Técnicas de escaneo de puertos
- Identificación de vulnerabilidades con Nmap y Nessus
- Enumeración de usuarios, servicios y recursos

Hacking Ético IV: Vulnerabilidades en Aplicaciones Web
- Metodología de pruebas en aplicaciones web
- OWASP Top 10 - Principales vulnerabilidades
- Inyecciones SQL y XSS (Cross-Site Scripting)
- Herramientas para pruebas web (Burp Suite, OWASP ZAP)

Hacking Ético V: Técnicas de Explotación y Escalada de Privilegios
- Identificación de vectores de ataque
- Explotación de vulnerabilidades conocidas
- Uso de frameworks de explotación (Metasploit)
- Técnicas de escalada de privilegios en Windows y Linux

Hacking Ético VI: Pruebas de Seguridad en Redes
- Ataques de Man-in-the-Middle
- Sniffing y captura de tráfico
- Análisis de protocolos inseguros
- Bypass de mecanismos de seguridad perimetral

Hacking Ético VII: Ingeniería Social y Análisis Forense
- Principios y técnicas de ingeniería social
- Phishing y ataques de suplantación de identidad
- Fundamentos de análisis forense digital
- Captura y análisis de evidencias

Hacking Ético VIII: Informes y Mejores Prácticas
- Documentación de vulnerabilidades y pruebas realizadas
- Estructura y redacción de informes técnicos
- Estrategias de mitigación y recomendaciones
- Planificación de pruebas recurrentes y seguimiento

Módulo 4 | Servicios Cloud y Big Data
70 horas lectivas

Google Cloud I. Cloud Basics
- IAM, Console
- Cloud shell
- Authentication, permissions

Google Cloud II. Compute
- Compute Engine
- App Engine
- Cloud GPU
- Spot VMs
- Bare Metal
- Disks

Google Cloud III. Storage. Databases
- AlloyDB for PostgreSQL
- Cloud SQL
- Firestore
- Spanner
- Memorystore

Google Cloud IV. Kubernetes I
- Google Kubernetes Engine
- Artifact Registry
- Cloud Build

Google Cloud V. Kubernetes II
- Migrate to Containers
- Knative
- Deep learning Containers

Google Cloud VI. Security and Identity
- Sensitive Data protection
- Google Threat Intelligence
- Security Conmmand Center
- Assured workloads

Google Cloud VII. Networking
- Cloud CDN
- Load balancing
- Cloud NAT
- Virtual Private Cloud
- Private Service Connect

Google Cloud VIII. Developer Tools
- Cloud Workstations
- Cloud SDK
- Cloud Code
- Cloud Deploy

Google Cloud IX. Serverless
- Cloud Run
- Cloud Functions
- Workflows
- API Gateway

Google Cloud X. Operations
- Cloud Logging
- Cloud monitoring
- Error reporting
- Cloud Trace
- Cloud Profiler

Preparación certificación profesional Cloud Architect

CI/CD I
- Introducción y configuración avanzada de Git
- Gestión avanzada de ramas, merges y resolución de conflictos
- Colaboración en GitHub: pull requests, revisión de código, acciones
- Proyecto colaborativo usando Git y GitHub (workflow completo)
- Feedback y evaluación de proyecto colaborativo

CI/CD II
- Introducción a Docker, imágenes y contenedores
- Práctica supervisada: creación de imágenes Docker personalizadas
- Docker Compose: orquestación básica de contenedores
- Despliegue práctico aplicación web multi-contenedor

Examen certificado profesional Cloud Architect

Defensa de TFM I

Defensa de TFM II

Programa TOP

Módulo 1 | Ciberseguridad y Hacking Ético
110 horas lectivas

Visión General del programa
- Presentación y alineación de objetivos
- Tecnologías emergentes en ciberseguridad
- Business case (búsqueda de coherencia en la aplicación tecnológica)

Be Hacker. Otras Aproximaciones a la Ciberseguridad I
- La Ciberseguridad es un problema de todos
- El equipo de ciberseguridad no es la policía, no podemos delegar la ciberseguridad
- Lo que conoces y lo que no conoces de Internet. ¿Quién eres en Internet?, Deep Web.
- No se sabe de ciberseguridad, se sabe de desarrollo, se sabe de infraestructuras, se sabe de arquitecturas
- La seguridad es una característica intrínseca no un añadido posterior. Desarrollo seguro.

Be Hacker. Otras Aproximaciones a la Ciberseguridad II
- No existen redes seguras, existen identidades seguras el paradigma de la defensa por la ubicación ha muerto.
- Tienes un monto de documentos, planes y herramientas, pero ¿está tu compañía segura?
- ¿Quién es el eslabón más débil de la cadena?
- Nadie reacciona bien ante lo que no conoce

Análisis Forense I:
Fundamentos del Análisis Forense Digital
- Principios y objetivos de la informática forense
- Marco legal y cadena de custodia
- Tipos de evidencia digital y su admisibilidad
- Ciclo de vida del análisis forense

Análisis Forense II:
Adquisición y Preservación de Evidencia
- Procedimientos de respuesta a incidentes
- Técnicas de adquisición de datos (imágenes forenses)
- Herramientas para captura de evidencia volátil y no volátil
- Verificación de integridad y documentación del proceso

Análisis Forense III: Sistemas de Archivos
- Estructura de sistemas de archivos (NTFS, FAT, ext4)
- Recuperación de archivos eliminados
- Análisis de metadatos y timestamps
- Carving de archivos y fragmentos de datos

Análisis Forense IV: Sistemas Windows
- Registro de Windows y sus artefactos forenses
- Análisis de logs y eventos de seguridad
- Artefactos de navegación web y comunicaciones
- Correlación de evidencias en sistemas Windows

Análisis Forense V: Sistemas Unix/Linux
- Estructura de directorios y permisos
- Análisis de logs y auditoría
- Artefactos forenses en entornos Linux
- Análisis de memoria en sistemas Unix

Análisis Forense VI: Memoria y Procesos
- Captura de memoria RAM
- Análisis de procesos, conexiones y sockets
- Detección de rootkits y malware en memoria
- Herramientas de análisis de memoria (Volatility)

Análisis Forense VII: Dispositivos Móviles y Redes
- Adquisición forense de dispositivos iOS y Android
- Análisis de aplicaciones y almacenamiento
- Análisis de tráfico de red y capturas de paquetes
- Correlación entre evidencias de red y sistemas

Análisis Forense VIII:
Reconstrucción de Incidentes y Elaboración de Informes
- Técnicas de timeline y reconstrucción de eventos
- Análisis de causalidad y atribución
- Elaboración de informes periciales
- Presentación de evidencias y testimonio experto

Análisis de Malware I:
Introducción al Análisis de Malware
- Taxonomía y clasificación de malware
- Ciclo de vida de una infección
- Motivaciones y actores de amenazas
- Configuración de laboratorios seguros de análisis

Análisis de Malware II: Análisis Estático Básico
- Inspección de propiedades de archivos
- Técnicas de fingerprinting y hashing
- Análisis de strings y recursos embebidos
- Identificación de patrones y firmas

Análisis de Malware III: Análisis Estático Avanzado
- Ingeniería inversa y desensamblado
- Análisis de código fuente y pseudocódigo
- Identificación de funciones y algoritmos
- Herramientas de análisis estático (IDA Pro, Ghidra)

Análisis de Malware IV: Análisis Dinámico Básico
- Monitorización de procesos y cambios en el sistema
- Análisis de comportamiento en sandbox
- Captura y análisis de tráfico de red generado
- Identificación de indicadores de compromiso (IoCs)

Análisis de Malware V: Análisis Dinámico Avanzado
- Depuración y análisis de ejecución paso a paso
- Manipulación de memoria y hooks
- Análisis de inyección de código y técnicas de ofuscación
- Herramientas de análisis dinámico (OllyDbg, x64dbg)

Análisis de Malware VI: Técnicas Anti-Análisis y Evasión
- Detección de entornos virtuales y sandbox
- Ofuscación y empaquetado de código
- Anti-debugging y anti-VM
- Técnicas de persistencia y ocultamiento

Análisis de Malware VII: Análisis de Malware Específico
- Ransomware y análisis de algoritmos de cifrado
- Botnets y comunicaciones C&C

- Rootkits y malware a nivel de kernel
- Malware para dispositivos móviles y IoT

Análisis de Malware VIII:
Inteligencia de Amenazas y Reporting

- Extracción y correlación de indicadores
- Atribución y análisis de campañas
- Elaboración de informes técnicos de análisis
- Integración con sistemas de detección y prevención

Taller de Hacking Etico I

Taller de Hacking Etico II

Taller de Hacking Etico III

Taller de Hacking Etico IV

Módulo 2 | Servicios Cloud y Big Data
110 horas lectivas

BigData y procesado de datos I

- Analítica de datos: visión end-to-end de todos los servicios
  - Collect: Pub/sub, VerneMQ
  - Process: dataflow, Dataproc (spark)
  - Store: GCS, BigQuery, BigQuery ML, BigTable
  - Analyze: BigQuery SQL, Dataproc (spark)

BigData y procesado de datos II. Collect I

- Google Cloud Pub/sub
- Messages, Topics
- Best practices
- VerneMQ
- Apache Kafka

BigData y procesado de datos III. Process I

- Dataflow
- Templates
- I/O connectors best practices
- Dataflow runner

BigData y procesado de datos IV. Process II

- Dataproc (spark)
- Dataproce serverless
- Clusters
- Toubleshooting

BigData y procesado de datos V. Store I

- Google Cloud Storage
- BigQuery
- BigTable

BigData y procesado de datos VI. Analyze I

- BigQuery SQL
- Storage/compute separation
- Dataform

BigData y procesado de datos VII. Analyze II

- Looker
- Looker Studio
- Visualization

BigData y procesado de datos VIII

- Data lakes
- Linage, automatizations
- Dataplex

Preparación certificación profesional BigData engineer

Google Vertex AI I

- Vertex AI intro
- MLOps
- Methodology and technical components
- Customer references

Google Vertex AI II

- Training a custom model in Vertex AI
- Distributed training in Vertex AI
- Hyperparameter tuning in Vertex AI
- Hardware accelerators for training

Google Vertex AI III

- Vertex AI Prediction
- Batch predictions
- Model Monitoring
- Explainable AI

Google Vertex AI IV

- Vertex AI Model registry
- Vertex AI Experiments
- Model cards

Google Vertex AI V

- Vertex AI Pipelines
- Kubeflow Pipelines
- Components
- Pipelines
- I/O v2

Google Vertex AI VI

- Tabular workflows
- Hands-on Pipelines I
- Hands-on Pipelines II

Google Vertex AI VII

- ML Metadata
- Low-code/No-code
- AutoML
- BQML

Google Vertex AI VIII

- Model Garden. LLMs/LRMs in Vertex AI
- LLMOps in Vertex AI
- Vertex AI Workbench
- Colab Enterprise

Preparación certificado profesional ML Engineer

CI/CD III

- Conceptos esenciales de Kubernetes
- Instalación y configuración ikube o entorno local
- Despliegue, escalado y actualización de aplicaciones en Kubernetes
- Introducción al monitoreo (Prometheus + Grafana)
- Implementación básica de monitoreo en Kubernetes

CI/CD IV

- Jenkins y GitHub Actions
- Configuración práctica de pipelines automatizados
- Integración CI/CD con Docker/Kubernetes
- Proyecto final: pipeline completo con integración Git, Docker, Kubernetes, monitoreo

Examen certificado profesional BigData engineer
Examen certificado profesional ML Engineer

Módulo 3 | Derecho tecnológico
55 horas lectivas

Derecho aplicado a la IA I

- Marcos jurídicos de la Inteligencia Artificial en Europa, EEUU, Asia y oriente.
- Responsabilidad asociada a sistemas de IA artificial (i)
- Las figuras del operador/productor/ y sus implicaciones legales
- El caso de sistemas de aprendizaje autónomo y los casos de aprendizaje online y offline

Derecho aplicado a la IA II

- Responsabilidad asociada a sistemas de inteligencia artificial (ii)
- El Nuevo Reglamento de Inteligencia Artificial
  - Marco jurídico asesoramiento / algoritmos de inversión / MIFID II
  - Requisitos asociados a los algoritmos de alta y baja frecuencia
  - Trazabilidad y responsabilidades asociadas
- Protección de datos
- Casos prácticos sobre responsabilidad en el uso de IA

Derecho aplicado a la IA III

- La importancia de la ética en la regulación de la inteligencia artificial
- Normativa en materia de protección de datos personales en sistemas de IA
- El Sandbox en Inteligencia Artificial
- La Agencia Española de Supervisión de la IA
- Malfuncionamiento vs rentabilidades pasadas no garantizan rentabilidades futuras

Derecho aplicado a los servicios de plataforma y distribuidos I

- Los servicios en la nube y la seguridad de los datos
- Tipos de servicios de cloud computing
  - Construcción de servicios desde la nube: prestadores de servicios de confianza (Reglamento eIDAS2)
- Aspectos regulatorios y contractuales del almacenamiento en la nube
  - Términos y condiciones: versionado aplicable
  - Estándares y su verificación
  - Plurijurisdiccionalidad y protección de datos: la virtualización
  - La protección de datos en la nube

Derecho aplicado a los servicios de plataforma y distribuidos II: DSA, ¿a quién se aplica?

- La irresponsabilidad de los prestadores por contenidos: cláusula de buen samaritano
- Obligaciones de diligencia debida
  - Universales
  - Para todos los servicios de hosting, incluidas las plataformas en línea
  - Adicionales para los prestadores de plataformas online.
  - Especiales y adicionales para las plataformas y los motores de búsqueda de muy gran tamaño
    - VLOP, VLSE
    - Evaluación anual de riesgos sistémicos
    - Medidas de reducción de riesgos específicas
    - Mecanismos de respuesta a crisis
    - Sistemas de recomendación
    - Transparencia adicional sobre la publicidad online
    - Acceso a datos
    - Funciones de comprobación y cumplimiento
    - Auditoría independiente
    - Informes de Transparencia
- Aplicación de la norma, autoridades competentes y sanciones.

Derecho aplicado a la criptografía y a los prestadores de servicios de confianza

- Firma electrónica: definición y propiedades. Tipos (avanzada, probabilística, ciega, múltiple, delegada, etc.)
- Firma de un documento: elaboración y verificación de una firma electrónica.
- Algoritmos estándares de firma: RSA, DSA, ECDSA.
- Certificados electrónicos (con/sin clave privada). Autoridades de Certificación y Estructuras relacionales.
- Revocación de certificados.
- Sellos de tiempo. Autoridades de sellado de tiempo. Requisitos.
- Proveedores de Servicios de Confianza.
- Vulnerabilidades y Evaluación de riesgos.

Derecho aplicado a la ciberseguridad

- Seguridad v. gestión de la seguridad: el modelo ISO/IEC 27001
- Normativa de Ciberseguridad y administración competente
  - Infraestructuras críticas
  - NIS1 y NIS2
  - Cybersecurity Act
  - Conexión códigos penales.

Derecho aplicado a la Identidad Digital I: Identidad y medios de identificación conforme el Reglamento eIDAS

- Qué es la identidad
- La identidad presunta y el análisis de riesgos: Zero trust vs. Friction
- Diferencias entre identidad, identificación, verificación de la identidad y autenticación
  - PSD2, EBA y factores de autenticación.
- El modelo de identidad en el Reglamento eIDAS1
  - Documentos nacionales de identidad analógicos y digitales
  - Certificados de firma: tipologías de firma y su valor probatorio de la identidad

Derecho aplicado a la Identidad Digital II

- El proceso de verificación y sus cinco fases: procesos presenciales y online
  - Normativa aplicable: España y UE
  - Estándares aplicables: España y UE
- El modelo de la identidad en el Reglamento eIDAS
  - El EDIW (European Digital identity Wallet)
    - Regulación, funcionamiento
    - Interoperación con terceras partes confiables

    - Seguridad del Wallet
  - Las atestaciones de atributos:
    - Prestadores de servicios de confianza de atestación de atributos
    - Regulación y funcionamiento
    - Similitudes y diferencias con los emisores de certificados cualificados y con los modelos basados en SSI y DIDs
    - Interacciones con otros prestadores/operadores
  - Los servicios de confianza y sus prestadores tras la reforma: que cambia y qué se queda
  - Cambio de los requisitos de Ciberseguridad: cómo es el nuevo esquema y cuáles los nuevos requisitos

Aspectos Legales (IA Abierta)

- IA Abierta
- Tipos de Licencias para componentes de IA
- Model Cards
- Rol de los derechos y la propiedad intelectual
- Impacto de la regulación den los modelos
- Casos de Estudio

Marco jurídico de la Defensa Nacional en el Ciberespacio

- La ciberseguridad dentro del Sistema de Seguridad Nacional
- El Mando Conjunto de Ciberdefensa de las Fuerzas Armadas
- Principios de soberanía, diligencia, jurisdicción y responsabilidad internacional en el ciberespacio
- Ius ad bellum: Uso de la fuerza armada en el ciberespacio
- Ius in bello: aplicación del Derecho Internacional de los Conflictos Armados en el ciberespacio
- Organismos de normalización en ciberseguridad
- Normativa ISO IEC/JTC1 27035

Módulo 4 | Ciberseguridad Cuántica
245 horas lectivas

Fundamentos de Computación Cuántica I: Mecánica Cuántica Básica

- Principios de mecánica cuántica
- Superposición y entrelazamiento
- Fundamentos matemáticos

Fundamentos de Computación Cuántica II: Qubits y Puertas

- Estados cuánticos
- Representación de Dirac
- Puertas de un qubit (X, Y, Z, H)
- Puertas controladas (CNOT, Toffoli)
- Construcción de circuitos
- Estados Bell y GHZ
- Mediciones proyectivas
- Phase Kickback

Fundamentos de Computación Cuántica III: Algoritmos básicos

- Bernstein-Vazirani
- Teleportación
- Dense encoding

Fundamentos de Computación Cuántica IV: Hardware Cuántico

- Tecnologías de qubits superconductores
- Iones atrapados
- Fotónica cuántica
- Control y medición
- Corrección de errores cuánticos
- Arquitecturas escalables

Algoritmos Cuánticos I: Algoritmo de Shor

- Fundamentos matemáticos
- Transformada cuántica de Fourier
- Estimación de fase
- Implementación detallada
- Análisis de complejidad
- Implicaciones criptográficas

Algoritmos Cuánticos II: Algoritmo de Grover

- Búsqueda cuántica
- Oracle cuántico
- Amplificación de amplitud
- Optimización del algoritmo
- Aplicaciones prácticas
- Casos de uso

Optimización cuántica

- VQE
- QAOA
- Grover Adaptive Search

Simulación de Escenarios con Cuántica

- Quantum Random Walks
- Redes bayesianas cuánticas

Preparación certificación IBM Qiskit Developer

Infraestructura de Clave Pública Cuántica I: Diseño de PKI Híbrida

- Arquitectura de CA híbrida
- Jerarquías de certificación
- Políticas de certificación
- Gestión de múltiples algoritmos
- Períodos de transición
- Interoperabilidad

Infraestructura de Clave Pública Cuántica II: Gestión de Certificados

- Ciclo de vida de certificados
- Sistemas de revocación
- OCSP y CRL cuánticos
- Formatos de certificados híbridos
- Almacenamiento seguro
- Auditoría y logging

Infraestructura de Clave Pública Cuántica III: Firma Digital Post-Cuántica

- Esquemas de firma híbridos
- Estándares emergentes
- Validación a largo plazo
- Sellado de tiempo cuántico
- Preservación de evidencias

Infraestructura de Clave Pública Cuántica IV: Migración de Sistemas

- Análisis de sistemas legacy
- Estrategias de migración
- Compatibilidad backwards
- Testing de integración

- Gestión de riesgos
- Plan de contingencia

Algoritmos y Protocolos Cuánticos Básicos I: Criptografía Basada en Retículos

- Learning With Errors (LWE)
- Ring-LWE
- Module-LWE
- NTRU
- CRYSTALS-Kyber
- Optimizaciones prácticas

Algoritmos y Protocolos Cuánticos Básicos II: Sistemas Multivariantes

- Oil-Vinegar
- Rainbow
- HFE variants
- UOV schemes
- Implementaciones eficientes
- Análisis de seguridad

Algoritmos y Protocolos Cuánticos Básicos III: Criptografía Basada en Hash

- Hash-based signatures
- SPHINCS+
- XMSS
- Merkle trees
- One-time signatures
- Few-time signatures

Algoritmos y Protocolos Cuánticos Básicos IV: Criptografía Basada en Códigos

- Classic McEliece
- Códigos Goppa
- QC-MDPC
- Decodificación de síndromes
- Optimización de parámetros
- Implementación práctica

Implementación Segura de Sistemas Cuánticos I: Desarrollo Seguro

- Ciclo de vida de desarrollo seguro
- Buenas prácticas de programación
- Testing de implementaciones PQC
- Gestión segura de memoria
- Control de versiones y auditoría
- DevSecOps para sistemas PQC

Implementación Segura de Sistemas Cuánticos II: Side-Channel Attacks

- Ataques de tiempo
- Análisis de consumo energético
- Ataques electromagnéticos
- Fault injection
- Cache attacks
- Microarquitectura y side-channels

Implementación Segura de Sistemas Cuánticos III: Contramedidas

- Implementaciones constant-time
- Enmascaramiento aritmético
- Protección contra fallos
- Randomización
- Validación de implementaciones
- Testing de resistencia

Implementación Segura de Sistemas Cuánticos IV: Integración de Sistemas

- APIs criptográficas seguras
- Bibliotecas PQC
- Integración con TLS/SSL
- Testing y benchmarking
- Monitorización de rendimiento
- Gestión de incidentes

Blockchain y Criptografía Cuántica I: Fundamentos de Blockchain

- Arquitectura blockchain
- Consenso distribuido
- Smart contracts
- Criptografía en blockchain

Blockchain y Criptografía Cuántica II: Amenazas Cuánticas

- Impacto en firmas ECDSA
- Vulnerabilidades en Bitcoin
- Timeframes de amenazas
- Estrategias de migración

Blockchain y Criptografía Cuántica III: Soluciones Post-Cuánticas

- Firmas cuánticas en blockchain
- Actualización de protocolos
- Migración de carteras
- Smart contracts quantum-safe

Blockchain y Criptografía Cuántica IV: Implementación Práctica

- Hyperledger Fabric
- IBM Blockchain Platform
- Ethereum cuántico
- Testing y validación

IoT Security en la Era Cuántica I: Arquitectura IoT Segura

- Protocolos IoT
- Gestión de identidad
- Arquitecturas edge-fog-cloud
- Seguridad en sensores

IoT Security en la Era Cuántica II: Criptografía Ligera

- Algoritmos lightweight
- Optimización de recursos
- Gestión de energía
- Protocolos eficientes

IoT Security en la Era Cuántica III: Soluciones PQC para IoT

- Implementaciones optimizadas
- Bootstrapping seguro
- Actualizaciones seguras
- Gestión de claves

IoT Security en la Era Cuántica IV: Casos Prácticos

- Industrial IoT
- Smart cities
- Healthcare IoT
- Redes de sensores

Cloud Security y Computación Cuántica I: Seguridad Cloud
- Modelos de servicio
- Arquitecturas multicloud
- Gestión de secretos
- Zero Trust en cloud

Cloud Security y Computación Cuántica II: Amenazas Cuánticas
- Vulnerabilidades en APIs
- Almacenamiento a largo plazo
- Comunicaciones cloud
- Análisis de riesgos

Cloud Security y Computación Cuántica III: Soluciones PQC
- Migración de servicios
- Gestión de certificados
- Automatización

Cloud Security y Computación Cuántica IV: DevSecOps
- CI/CD cuántico
- Seguridad automatizada
- Monitorización
- Respuesta a incidentes

Algoritmos y Protocolos Cuánticos Avanzados I: CRYSTALS Suite
- CRYSTALS-Kyber en profundidad
- CRYSTALS-Dilithium
- Optimizaciones AVXII
- Implementación en hardware
- Integración en protocolos
- Análisis de rendimiento

Algoritmos y Protocolos Cuánticos Avanzados II: Falcon y SPHINCS+
- Falcon signature scheme
- SPHINCS+ en detalle
- Comparativa de rendimiento
- Optimizaciones prácticas
- Casos de uso específicos
- Integración en sistemas reales

Algoritmos y Protocolos Cuánticos Avanzados III: Protocolos Híbridos
- Diseño de protocolos híbridos
- TLS cuántico
- SSH cuántico
- IKE/IPSec cuántico
- Análisis de seguridad
- Rendimiento y optimización

Algoritmos y Protocolos Cuánticos Avanzados IV: Aplicaciones Especializadas
- IoT cuántico
- Blockchain cuántico
- Cloud computing cuántico
- Sistemas embebidos
- Dispositivos móviles
- Infraestructuras críticas

Seguridad en Comunicaciones Cuánticas I: QKD
- Protocolos BB8IV y E9I
- Hardware QKD
- Limitaciones prácticas
- Ataques y defensas

Seguridad en Comunicaciones Cuánticas II: Redes Cuánticas
- Repetidores cuánticos
- Routing cuántico
- Memoria cuántica
- Protocolos de red

Seguridad en Comunicaciones Cuánticas III: Sistemas Híbridos
- Integración QKD-PQC
- Nodos de confianza
- Gestión de claves
- Arquitecturas híbridas

Seguridad en Comunicaciones Cuánticas IV: Aplicaciones
- Redes metropolitanas
- Comunicación satelital
- Backbone cuántico
- Casos de uso

Auditoría de Sistemas Criptográficos I: Marco de Auditoría
- Estándares internacionales
- Metodologías de evaluación
- Documentación técnica
- Reporting profesional

Auditoría de Sistemas Criptográficos II: Herramientas y Técnicas
- Análisis de código
- Testing de implementaciones
- Auditoría de protocolos
- Herramientas automatizadas

Auditoría de Sistemas Criptográficos III: Evaluación PQC
- Validación de algoritmos
- Análisis de transición
- Verificación de sistemas
- Testing de resistencia

Auditoría de Sistemas Criptográficos IV: Casos Prácticos
- Sector financiero
- Infraestructuras críticas
- Sistemas gubernamentales
- Compliance regulatorio

Taller de Criptografía Cuántica I
Taller de Criptografía Cuántica II
Taller de Criptografía Cuántica III
Taller de Criptografía Cuántica IV

Módulo 5 | Inteligencia Artificial Aplicada a la Ciberseguridad
230 horas lectivas

Quantum Machine Learning I
- Quantum Support Vector Machines
- Implicaciones criptográficas

Quantum Machine Learning II
- Variational Quantum Circuits
- Quantum Neural Networks

- Implicaciones criptográficas

Redes de Kohonen

- Redes competitivas no supervisadas
- Mapas autoorganizados 2D
- Mapas autoorganizados 3D
- Resolución del problema del viajante con redes auto-organizadas

Procesamiento de lenguaje natural I

- Corpus y stopwords
- Modelos Word to Vector. Representación del lenguaje.
- Modelos en NLP y Sequential to Sequential models
- Bucketing & Padding

Procesamiento de lenguaje natural II

- Aprendizaje supervisado en NLP. Definición del dominio del lenguaje
- Name Entity Recognition. Detección de entidades y aplicación en finanzas
- Clasificación de texto. Titulares, reportes, noticias.
- Análisis de Sentimiento:. Noticias y Redes Sociales.

Procesamiento de lenguaje natural III

- Transfer learning en NLP. TensorFlow Hub.
- Modelos pre-entrenados BERT, ELMO.
- Re-entrenamiento de los modelos pre-entrenados para tareas especificas

Procesamiento de lenguaje natural IV

- Capas de atención
- Modelos con atención
- Introducción a los modelos transformer

Procesamiento de lenguaje natural V

- Modelos transformer avanzados
- Generative Pre-Training: GPT models
- PaLM, Chinchilla, Flamingo, Minerva, Gato

Modelos generativos I

- Reducción de dimensionalidad y factores. PCA
- Autoencoders. Modelos no lineales
- Maximum likelihood y GMM
- Generación de cotizaciones de bolsa con PCA + GMM
- GANs, modelos de difusión y modelos condicionados

Modelos generativos II

- Modelos generativos profundos
- Variational autoencoders (VAE)
- Autoencoder con memoria (MAAE)
- Autoencoder sparse
- Generative adversarial networks (GAN)
- Modelos generativos recurrentes
- Normalizing Flows

Modelos generativos III

- Pretraining de Large Language Models
- Tuning
- PEFT (Parameter Efficient Fine-Tuning)
- Distillation
- Frameworks: T5X, PAX, otros
- Arquitecturas de TPUs

Modelos generativos IV

- Introducción a LangChain
- Componentes I: memoria, modelos y prompt
- Componentes II: retrievals, chains y agentes
- Técnicas RAG (Retrieval Augmented Generation)

Sistemas de recomendación

- Clusterización de perfiles y activos
- Sistemas de generación y asignación de recomendaciones
- TensorFlow Recommenders
- Sistemas basados en similitud,
- Sistemas basados en factorización
- Sistemas basados en deep-learning

Aprendizaje por transferencia y modelos avanzados

- Inception V3, VGG16, Resnet, Bert
- Reutilización de modelos
- Concatenación de modelos
- Solventando el problema de rotaciones
- Solventando el problema de escalado
- Mejora de redes convolucionales y generativas
- Solventando el desvanecimiento del gradiente
- Resnet
- Redes de capsula

LLM (Large Language Model)

- Transformers
- Bert
- LaMDA & LLaMA2
- GPT
- YaLM
- LLaMA
- PaLM2
- Meta-Transformer
- Uso de los modelos pre-entrenados.
- APIs y Reentrenamiento.
- QA en bases de datos propias.

Detección de Amenazas Asistida por IA I: Sistemas de Detección de Anomalías

- Sistemas de detección de anomalías
- Análisis de comportamiento mediante aprendizaje automático
- Detección de amenazas persistentes avanzadas (APT)
- Descubrimiento de vulnerabilidades de día cero
- Sistemas de monitoreo y alerta en tiempo real

Research with Google Deepmind I

- Federated Learning
- Gemini model family: 1.0, 1.5 and 2.0 (review of 4 papers)
- Multimodality

Research with Google Deepmind II

- Gemma model family (review of 11 papers)
- Models: Gemma-1, RecurrentGemma, CodeGemma, PaliGemma, ShieldGemma, DataGemma and ColPali
- Innovations: SigLIP, Griffin, and Gemma Scope
- Llama model family (review of 4 papers from Meta)
- STaR: Bootstrapping Reasoning With Reasoning
- Human-like systematic generalization through a meta-learning neural network
- Towards Self-Assembling Artificial Neural Networks through Neural Developmental Programs

Agentic AI - I
- Deterministic AI agents. Dialogflow
- Generative AI agents. Playbooks
- Agentic architectures
- Data stores for agents

Agentic AI - II
- ADK (Agent Development Kit)
- MCP (Model Context protocol)
- A2A (Agent to Agent protocol)
- LangChain intro

Agentic AI - III
- Agents Foundational conecpts
- Start to build agents in Google Cloud
- Agentic Memory
- Memory management. LLM as operating systems
- Labs

Agentic AI - IV
- Agent Engine and Agent Garden
- Evaluation/Improvement of Agents
- AgentOps
- Labs

LRM - Large Reasoning Models
- Architectures
- Differences LLM - LRM
- Gemini 2.5 vs OpenAI o3, o4
- Evaluation methodology
- Use cases

Herramientas GRC IA
- Inventario y clasificación de sistemas de IA
- Catálogo de riesgos y controles asociados a IA
- Seguimiento de proyectos, casos de uso y cuadros de mando
- Evaluación de los sistemas en base a la regulación
- Flujos de trabajo

Taller de riesgos y gobernanza
- Aplicación a Smart Due Diligence
- Cloude + mcp + grafos
- Capacidad de detectar errores y que el modelo automodifique el pront para completar la tarea

Detección de Amenazas Asistida por IA II: Analítica de Datos para Seguridad
- Procesamiento de big data para registros de seguridad
- Análisis de series temporales para inteligencia sobre amenazas
- Procesamiento de lenguaje natural para informes de amenazas
- Análisis de grafos para comportamiento de red
- Técnicas de visualización para operaciones de seguridad

Técnicas avanzadas de IA y Computación Cuántica I: Vectores de Ataque contra Sistemas de ML, Aprendizaje Automático Adversarial
- Vectores de ataque contra sistemas de aprendizaje automático
- Ataques de envenenamiento y evasión
- Generación y defensa de ejemplos adversariales
- Robustez y verificación de modelos
- Implementación segura de modelos de aprendizaje automático

Técnicas avanzadas de IA y Computación Cuántica II: Aprendizaje Automático Preservando la Privacidad
- Técnicas de privacidad diferencial
- Aprendizaje federado para colaboración segura
- Encriptación homomórfica para entrenamiento de modelos
- Computación segura multiparte
- Estrategias de minimización de datos

Técnicas avanzadas de IA y Computación Cuántica III: Sistemas de IA Resistentes a la Computación Cuántica
- Algoritmos de aprendizaje automático seguros frente a amenazas cuánticas
- Protección de infraestructura de IA contra amenazas cuánticas
- Aprendizaje automático adversarial cuántico
- Mecanismos de defensa híbridos clásico-cuánticos
- Técnicas de preservación de privacidad mejoradas con tecnología cuántica

Técnicas avanzadas de IA y Computación Cuántica IV: Detección Avanzada de Amenazas Cuánticas
- Detección de intrusiones mediante sensores cuánticos
- Aprendizaje automático cuántico para detección de anomalías
- Reconocimiento de patrones mejorado con tecnología cuántica para inteligencia de amenazas
- Protocolos de seguridad basados en entrelazamiento
- Redes cuánticas para comunicaciones seguras

Automatización y Orquestación de Seguridad con IA I: Orquestación de Seguridad - Plataformas y Flujos de Trabajo
- Plataformas SOAR e implementación
- Flujos de trabajo automatizados de respuesta a incidentes
- Sistemas de apoyo a la decisión impulsados por IA
- Integración con infraestructura de seguridad existente
- Medición de la efectividad de la automatización de seguridad

Automatización y Orquestación de Seguridad con IA II: Hacking Ético con IA
- Pruebas de penetración mejoradas con IA
- Escaneo automatizado de vulnerabilidades
- Aprendizaje por refuerzo para simulación de ataques
- Ampliación de operaciones del equipo rojo
- Prácticas de divulgación responsable

Automatización y Orquestación de Seguridad con IA III: Clasificación y Modelado de Malware
- Clasificación automatizada de malware
- Técnicas de análisis dinámico y estático
- Modelado de comportamiento de software malicioso
- Modelos generativos para descubrimiento de vulnerabilidades
- Técnicas anti-evasión

Automatización y Orquestación de Seguridad con IA IV: Análisis Forense Digital Avanzado con IA
- Recolección y procesamiento inteligente de evidencias
- Descubrimiento y extracción automatizada de

artefactos
- Aprendizaje automático para reconstrucción de fragmentos de archivos
- Procesamiento de lenguaje natural para análisis de registros
- Reconstrucción inteligente de líneas de tiempo forenses

IA para Remediación de Criptografía Heredada I: Análisis Automatizado de Código Criptográfico
- Análisis automatizado de código criptográfico
- Técnicas de aprendizaje automático para detección de vulnerabilidades en código
- Análisis estático y dinámico de implementaciones criptográficas
- Reconocimiento de patrones para identificar funciones y algoritmos obsoletos
- Desarrollo de herramientas para escaneo de bases de código grandes

IA para Remediación de Criptografía Heredada II: Refactorización Criptográfica Inteligente
- Migración de código asistida por IA de criptografía obsoleta a moderna
- Enfoques basados en aprendizaje para preservación de funcionalidad equivalente
- Generación automatizada de pruebas para corrección criptográfica
- Técnicas de verificación de transformación de código
- Evaluación de riesgos durante transiciones criptográficas

IA para Remediación de Criptografía Heredada III: Gestión de Deuda Técnica Criptográfica
- Algoritmos de priorización para vulnerabilidades criptográficas
- Análisis de impacto usando modelado predictivo
- Análisis costo-beneficio para esfuerzos de remediación
- Enfoques basados en ML para identificar activos criptográficos críticos
- Seguimiento de dependencias criptográficas en sistemas

IA para Remediación de Criptografía Heredada IV: Compatibilidad con Protocolos Heredados
- Soluciones de IA para desafíos de compatibilidad hacia atrás
- Mecanismos inteligentes de negociación y regresión de protocolos
- Estrategias de transición segura usando sistemas de apoyo a la decisión basados en ML
- Frameworks automatizados de pruebas de compatibilidad
- Enfoques de implementación híbrida para soporte de sistemas heredados

Ciencia Forense Digital Avanzada con IA I: Aprendizaje Profundo
- Detección de manipulación de imágenes y videos
- Análisis forense de audio y análisis de voz
- Detección y atribución de DeepFakes
- Detección de esteganografía mediante redes neuronales
- Identificación y correspondencia de fuentes de cámara

Ciencia Forense Digital Avanzada con IA II: Redes con IA
- Análisis automatizado de tráfico de red
- Perfilado de comportamiento de red
- Investigación forense de amenazas persistentes avanzadas (APT)
- Detección y análisis de redes de bots
- Análisis forense de tráfico encriptado

Ciencia Forense Digital Avanzada con IA III: Memoria y Malware
- Análisis de volcados de memoria asistido por IA
- Detección automatizada de rootkits y puertas traseras
- Análisis de comportamiento de malware desconocido
- Análisis de similitud y atribución de código
- Asistencia a la ingeniería inversa con aprendizaje automático

Ciencia Forense Digital Avanzada con IA IV: IA para Construcción de Casos Forenses
- Reconocimiento de entidades en evidencia digital
- Mapeo de relaciones a través de fuentes de datos dispares
- Técnicas inteligentes de correlación de evidencias
- Modelado predictivo para pistas de investigación
- Sistemas expertos para evaluación de casos

Taller de IA aplicada a criptografía I

Taller de IA aplicada a criptografía II

Taller de IA aplicada a criptografía III

Taller de IA aplicada a criptografía IV

Defensa de TFM I

Defensa de TFM II

ATHENAI
Technological Business School

4

Certificaciones

Podrás obtener hasta ***seis certificaciones***. Todo ello mientras estudias este máster.

Certificación Security+ D5 (CompTIA Security+)

La certificación ***Security+***, emitida por **CompTIA**, está diseñada para validar las competencias básicas en ciberseguridad necesarias para identificar, mitigar y responder a amenazas comunes. Es una certificación ideal para perfiles técnicos que buscan establecer una base sólida en seguridad informática, y está ampliamente reconocida en entornos empresariales, gubernamentales y del sector financiero.

Esta certificación demuestra que los profesionales son capaces de:

- Detectar y responder ante incidentes de seguridad con eficacia.
- Aplicar principios de ciberseguridad en redes, dispositivos, usuarios y aplicaciones.
- Implementar controles de seguridad acordes con políticas organizativas y normativas.

Contenido del Certificado

Fundamentos de seguridad:

- Principios de confidencialidad, integridad y disponibilidad (CIA).
- Gestión de riesgos y controles de seguridad básicos.

Amenazas, vulnerabilidades y ataques:

- Tipos de amenazas (malware, phishing, ransomware, etc.).
- Análisis y mitigación de vulnerabilidades.

Arquitectura y diseño de seguridad:

- Diseño de redes seguras.
- Seguridad en entornos híbridos y cloud.

Gestión de identidad y acceso (IAM):

- Métodos de autenticación y control de acceso.
- Aplicación de políticas de seguridad sobre usuarios y dispositivos.

Gestión de riesgos y cumplimiento:

- Políticas, procedimientos y normativa relevante (como GDPR o ISO/IEC 27001).
- Seguridad física y medioambiental.

Operaciones de seguridad:

- Detección de amenazas, respuesta a incidentes y continuidad del negocio.
- Monitorización de seguridad y gestión de logs.

Beneficios para los Estudiantes

- Certificación muy adecuada para perfiles técnicos en fases iniciales o intermedias de su carrera.
- Acreditación con reconocimiento global, ampliamente utilizada en empresas tecnológicas, de servicios financieros y organismos públicos.
- Aplicación práctica enfocada a tareas operativas reales, desde la protección de redes hasta la gestión de incidentes.

Para obtener esta certificación será necesario aprobar un examen de 90 minutos, compuesto por un máximo de 90 preguntas de tipo test y escenarios prácticos interactivos (PBQs), realizado en formato remoto supervisado o en centros autorizados.
La tasa del examen es de 392 USD, importe que será abonado directamente a CompTIA por el estudiante.
No se requieren requisitos previos, aunque se recomienda tener conocimientos generales en TI.

Certificación CASP+ D5 (CompTIA Advanced Security Practitioner)

La certificación ***CASP+***, emitida por **CompTIA**, valida habilidades avanzadas en ciberseguridad para profesionales que diseñan, implementan y gestionan soluciones complejas de seguridad en grandes organizaciones. A diferencia de otras certificaciones orientadas a gestión, CASP+ se centra en habilidades técnicas a nivel experto, lo que la convierte en una credencial clave para arquitectos de seguridad, ingenieros senior y técnicos especializados en entornos críticos.

Esta certificación demuestra que los profesionales son capaces de:

- Diseñar arquitecturas de seguridad complejas e integradas en entornos empresariales.
- Implementar soluciones criptográficas, de red y de resiliencia frente a amenazas avanzadas.
- Evaluar riesgos, gestionar vulnerabilidades y asegurar el cumplimiento normativo en sistemas distribuidos.

Contenido del Certificado

Seguridad empresarial:

- Evaluación de requisitos técnicos y de negocio para soluciones de seguridad.
- Diseño de estrategias de seguridad alineadas con el ciclo de vida organizativo.

Gestión de riesgos y cumplimiento:

- Evaluación y tratamiento de riesgos avanzados.
- Integración de marcos regulatorios (como NIST, ISO, GDPR) en arquitecturas de seguridad.

Arquitectura de seguridad:

- Diseño de arquitecturas seguras en entornos on-premise, cloud e híbridos.
- Aplicación de técnicas avanzadas de segmentación, virtualización y control de acceso.

Operaciones de seguridad:

- Gestión de eventos e incidentes complejos.
- Automatización de respuestas con herramientas de orquestación y análisis forense.

Criptografía y gestión de identidad:

- Selección e implementación de algoritmos criptográficos.
- Integración de soluciones IAM, MFA y federación de identidades.

Beneficios para los Estudiantes

- Perfil técnico experto: Recomendado para profesionales senior que deseen profundizar en el diseño técnico y táctico de soluciones de ciberseguridad.
- Enfoque operativo avanzado: Aporta experiencia práctica en entornos reales, especialmente en sectores críticos como banca, defensa y telecomunicaciones.
- Reconocimiento profesional: Muy valorada por empleadores que requieren habilidades técnicas más allá de la gestión de seguridad.

Para obtener esta certificación será necesario aprobar un examen de 165 minutos, compuesto por un máximo de 90 preguntas que combinan tipo test y simulaciones prácticas (PBQs), realizado en formato presencial o remoto supervisado.
El coste del examen es de 494 USD, importe que será abonado directamente a CompTIA por el estudiante.
No tiene requisitos obligatorios, pero se recomienda contar con al menos 5 años de experiencia en ciberseguridad, especialmente en roles técnicos o de arquitectura.

Certificación CISSP D1 (Certified Information Systems Security Professional)

La certificación *CISSP*, emitida por **(ISC)²**, está diseñada para validar los conocimientos y habilidades avanzadas en el diseño, implementación y gestión de programas de ciberseguridad. Es una credencial de prestigio internacional, especialmente valorada por empresas del sector financiero, tecnológico y gubernamental, y está orientada a profesionales que desean asumir roles estratégicos en la protección de activos críticos de información.

Esta certificación demuestra que los profesionales son capaces de:

- Diseñar y gestionar arquitecturas de seguridad integrales y resilientes.
- Identificar y mitigar riesgos de ciberseguridad en organizaciones complejas.
- Alinear las políticas y controles de seguridad con los objetivos de negocio y requisitos regulatorios.

Contenido del Certificado

Seguridad y gestión de riesgos:

- Evaluación de riesgos y análisis de impacto.
- Gobernanza, cumplimiento y políticas de seguridad.

Seguridad de activos:

- Clasificación y gestión del ciclo de vida de la información.
- Protección de la privacidad y la propiedad intelectual.

Arquitectura y diseño de seguridad:

- Diseño de arquitecturas seguras.
- Principios de diseño seguro en entornos cloud, on-premise e híbridos.

Seguridad de redes y comunicaciones:

- Protocolos de red seguros.
- Detección, prevención y respuesta ante amenazas en redes complejas.

Gestión de identidad y control de acceso:

- Sistemas de autenticación, autorización y federación.
- Implementación de políticas de acceso basado en roles.

Evaluación y pruebas de seguridad:

- Auditorías, pruebas de penetración y análisis de vulnerabilidades.

Operaciones de seguridad:

- Monitorización de eventos, respuesta a incidentes y continuidad de negocio.

Seguridad del desarrollo de software:

- Principios de desarrollo seguro (SDLC).
- Gestión de vulnerabilidades en aplicaciones.

Beneficios para los estudiantes

- Certificación expedida por (ISC)², reconocida como estándar de excelencia en seguridad informática.
- Muy valorada en sectores regulados como banca, seguros, defensa y consultoría.
- Adquieren competencias para liderar programas de ciberseguridad y gestionar riesgos organizativos a gran escala.

Para obtener esta certificación será necesario aprobar un examen de 4 horas, compuesto por 100-150 preguntas adaptativas (CAT) tipo test, realizado en centros autorizados o en formato remoto supervisado. El coste del examen es de 749 USD, importe que será abonado directamente a (ISC)² por el estudiante. Se requiere acreditar 5 años de experiencia profesional en al menos 2 de los 8 dominios del CBK de CISSP. En caso de no contar con la experiencia, el alumno puede obtener el estatus de *"Associate of (ISC)²"* hasta completar los años requeridos.

Certificación CCSP D5 (Certified Cloud Security Professional)

La certificación *CCSP*, emitida por **(ISC)²**, está diseñada para validar las competencias avanzadas en seguridad en entornos cloud. Es una credencial internacionalmente reconocida, ideal para profesionales que gestionan, diseñan o auditan arquitecturas y operaciones de seguridad en la nube. Combina un enfoque técnico y estratégico, integrando aspectos legales, regulatorios y de gobierno de datos.

Esta certificación demuestra que los profesionales son capaces de:

- Diseñar e implementar arquitecturas seguras en entornos cloud públicos, privados e híbridos.
- Evaluar riesgos, aplicar controles técnicos y asegurar la conformidad con normativas en la nube.
- Gestionar identidades, datos y operaciones de seguridad de forma eficiente en entornos distribuidos.

Contenido del Certificado

Conceptos arquitectónicos de la nube:

- Modelos de entrega (IaaS, PaaS, SaaS).
- Principios de arquitectura segura en la nube.

Gobernanza, riesgo y cumplimiento:

- Evaluación de riesgos en entornos cloud.
- Cumplimiento con marcos regulatorios (GDPR, ISO/IEC 27017, PCI DSS, etc.).

Seguridad en la infraestructura cloud:

- Diseño de arquitecturas resilientes.
- Controles de red, virtualización y protección de entornos multicloud.

Seguridad de datos:

- Cifrado en tránsito y en reposo.
- Gestión del ciclo de vida y clasificación de la información.

Gestión de identidades y accesos (IAM):

- Federaciones, autenticación multifactor (MFA) y control de acceso granular.

Operaciones de seguridad en la nube:

- Monitorización, respuesta ante incidentes y continuidad del negocio.
- Automatización y DevSecOps en entornos cloud.

Beneficios para los estudiantes

- Alta especialización en cloud security, ideal para arquitectos cloud, responsables de cumplimiento y auditores de entornos cloud.
- Certificación respaldada por (ISC)² y alineada con las mejores prácticas internacionales.
- Muy valorada en banca, seguros, fintech y administración pública por su enfoque normativo y técnico.

Para obtener esta certificación será necesario aprobar un examen de 4 horas, compuesto por 125 preguntas tipo test, realizado en centros autorizados o en formato remoto supervisado.

La tasa del examen es de 599 USD, importe que será abonado directamente a (ISC)² por el estudiante.

Se requiere acreditar al menos 5 años de experiencia profesional en seguridad de la información, incluyendo 1 año en alguno de los dominios de seguridad cloud definidos por el CBK de CCSP. Quienes aún no cumplan los requisitos pueden obtener el estatus de "Associate of (ISC)²" hasta completar la experiencia necesaria.

Desarrollador en Computación Cuántica Qiskit 2, IBM

El certificado está diseñado para desarrolladores interesados en profundizar en la computación cuántica.

El certificado se enfoca en la programación y conceptualización de circuitos y algoritmos cuánticos, así como en la comprensión de las operaciones matemáticas detrás de los sistemas cuánticos.

Contenido del Certificado

Conceptos Fundamentales de Computación Cuántica:

- Qubits y operaciones básicas.
- Puertas cuánticas y creación de circuitos.

Algoritmos Cuánticos:

- Algoritmos de Deutsch-Jozsa, Grover, y Shor.

Qiskit 2:

- Uso de Qiskit para construir y simular circuitos cuánticos.
- Manejo de simuladores y computadoras cuánticas reales.

Aplicaciones Cuánticas:

- Optimización y finanzas.

A través de IBM dispondremos de acceso prioritario a dispositivos cuánticos reales de 154 qubits para poder poner en práctica los conocimientos adquiridos en clase.

Beneficios para los estudiantes

La certificación no sólo es una inversión en conocimientos avanzados sino también un trampolín hacia oportunidades profesionales únicas en un campo disruptivo, y con demanda creciente:

- Diferenciación Competitiva
- Acceso a Oportunidades Especializadas
- Desarrollo de Habilidades Técnicas Avanzadas
- Credenciales Reconocidas por la Industria

Para la obtención de esta certificación, será necesario superar la prueba práctica en la plataforma de IBM (Pearson VUE).

Esta certificación tiene un coste adicional de 200$ en concepto de tasa de examen, el cual IBM cobrará directamente a los alumnos.

Professional Machine Learning Engineer (PMLE), Google Cloud

La certificación de ***Professional Machine Learning Engineer (PMLE)***, emitida por Google, pretende ser una certificación fundamental para estudiantes, desarrolladores y científicos de datos que desean demostrar habilidades de aprendizaje automático, puesta de producción de modelos, gobierno del dato e infraestructura de inteligencia artificial.

Esta certificación está diseñada para validar que los profesionales pueden:

- Diseñar soluciones de ML que sean escalables y mantenibles.
- Implementar modelos de ML utilizando las mejores prácticas de Google Cloud.
- Evaluar la efectividad y los riesgos de los modelos de ML implementados

Contenido del certificado

Marco conceptual de Machine Learning:

- Selección de técnicas de modelado y datos.
- Evaluación y ajuste de hiperparámetros.

Desarrollo de modelos de ML:

- Creación de pipelines de datos.
- Implementación de algoritmos y técnicas para problemas supervisados y no supervisados.

Implementación en producción:

- Automatización de modelos de ML.
- Supervisión y mejora continua de modelos desplegados.

Herramientas de Google Cloud:

- Uso de Vertex AI, TensorFlow, y BigQuery ML.

Beneficios para los Estudiantes

- Reconocimiento global por parte de Google.
- Mayor empleabilidad y credibilidad: Las habilidades de ML y Google Cloud son altamente demandadas en diversas industrias, finanzas entre ellas.
- Acceso a un ecosistema de innovación: Los productos de GCP y las tecnologías de IA están en constante evolución. Esta certificación demuestra que el estudiante está preparado y certificado por Google.

Para obtener esta certificación será necesario aprobar un examen de aproximadamente 2 horas, compuesto por 50-60 preguntas tipo test, realizado de forma remota, supervisado y sin acceso a materiales de apoyo.

La tasa del examen es de 200 USD, importe que será abonado directamente a Google por el estudiante.

Professional Data Engineer (PDE), Google Cloud

La certificación de ***Professional Data Engineer (PDE)***, expedida por Google Cloud, está orientada a profesionales que diseñan, construyen y optimizan sistemas de procesamiento de datos escalables, seguros y orientados a valor. Esta credencial certifica habilidades clave para convertir datos en información útil para la toma de decisiones, algo fundamental en el sector financiero.

Esta certificación valida que los profesionales pueden:

- Diseñar y construir sistemas de procesamiento de datos eficaces y escalables.
- Integrar y transformar grandes volúmenes de datos estructurados y no estructurados.
- Garantizar la seguridad, integridad y gobernanza del dato.
- Aplicar técnicas de machine learning para obtener insights avanzados.

Contenido del Certificado

Diseño de sistemas de datos:

- Arquitecturas de ingesta, almacenamiento y análisis de datos.
- Elección de tecnologías para datos en streaming y batch.

Construcción de pipelines de datos:

- Implementación de flujos de procesamiento con herramientas como Dataflow, Pub/Sub, Dataproc y Apache Beam.
- Limpieza, transformación y enriquecimiento de datos.

Modelado y análisis de datos:

- Uso de BigQuery para análisis en tiempo real.
- Aplicación de modelos de machine learning sobre conjuntos masivos de datos.

Seguridad y cumplimiento:

- Gestión de acceso, auditorías y cumplimiento normativo en entornos regulados.

Herramientas clave de Google Cloud:

- BigQuery, Cloud Composer, Dataflow, Dataproc, Pub/Sub, Vertex AI.

Beneficios para los Estudiantes

- Certificación con aval global de Google Cloud, reconocida por empresas líderes del sector financiero y tecnológico.
- Alta empleabilidad: El rol de Data Engineer es uno de los más demandados por su papel clave en la transformación digital.
- Habilidades prácticas para el sector financiero: Preparación específica para trabajar con datos financieros de alta frecuencia, históricos de mercados, riesgo...

Para obtener esta certificación será necesario aprobar un examen de aproximadamente 2 horas, compuesto por 50-60 preguntas tipo test, realizado de forma remota, supervisado y sin acceso a materiales de apoyo.

La tasa del examen es de 200 USD, importe que será abonado directamente a Google por el estudiante.

Professional Cloud Architect (PCA), Google Cloud

La certificación de ***Professional Cloud Architect (PCA)***, emitida por Google, está diseñada para validar las habilidades necesarias para diseñar, desarrollar y gestionar infraestructuras seguras, escalables y altamente disponibles en Google Cloud Platform (GCP). Es una credencial esencial para profesionales que desean dominar la arquitectura en la nube con un enfoque práctico y estratégico.

Esta certificación demuestra que los profesionales son capaces de:

- Diseñar arquitecturas de nube robustas, eficientes y seguras.
- Gestionar soluciones de infraestructura que cumplan con requisitos técnicos, de negocio y normativos.
- Supervisar, optimizar y asegurar el rendimiento de los entornos cloud.

Contenido del Certificado

Diseño de arquitecturas en la nube:

- Selección de servicios adecuados para distintas necesidades empresariales.
- Definición de estructuras de red, almacenamiento, cómputo y bases de datos.

Seguridad y cumplimiento normativo:

- Implementación de políticas de control de acceso, cifrado y auditoría.
- Alineación con marcos regulatorios como GDPR o MiFID II.

Gestión y optimización de soluciones en GCP:

- Supervisión de recursos y rendimiento.
- Automatización de tareas mediante herramientas como Cloud Deployment Manager y Terraform.

Casos de uso específicos:

- Implementación de soluciones de análisis financiero, big data e Inteligencia Artificial sobre GCP.

Herramientas de Google Cloud:

- Cloud Storage, Compute Engine, Kubernetes Engine, BigQuery, Cloud IAM, entre otros.

Beneficios para los Estudiantes

- Reconocimiento internacional: Certificación oficial expedida por Google Cloud.
- Alta empleabilidad: Las habilidades de arquitectura cloud son esenciales en banca, fintech y mercados de capitales.
- Preparación para liderar la transformación digital: El alumno estará capacitado para diseñar soluciones que cumplan con los más altos estándares del sector financiero.

Para obtener esta certificación será necesario aprobar un examen de aproximadamente 2 horas, compuesto por 50-60 preguntas tipo test, realizado de forma remota, supervisado y sin acceso a materiales de apoyo.

La tasa del examen es de 200 USD, importe que será abonado directamente a Google por el estudiante.

Salidas profesionales

Finalizado este Máster, serás ***CISO experto en ciberseguridad***, con IA y Computación Cuántica, uno de los perfiles más demandados y mejor pagados, tanto en el sector financiero, como en el ámbito del ministerio de Defensa.

Este máster ofrece múltiples salidas profesionales:

- **Arquitecto de Sistemas de IA Seguros**

Te dedicarás a diseñar sistemas de inteligencia artificial que integran la seguridad desde su concepción. Te encargarás de proteger los modelos de IA contra ataques adversarios, filtración de datos de entrenamiento y manipulación maliciosa, al tiempo que asegurarás el cumplimiento normativo. Esta especialización es particularmente valiosa porque las aplicaciones de IA se están integrando en todas las infraestructuras críticas, y un fallo de seguridad en estos sistemas podría tener consecuencias catastróficas. Además, a medida que las regulaciones sobre IA se vuelven más estrictas, las organizaciones necesitan expertos que puedan manejar este complejo panorama normativo.

- **Analista de Seguridad con Herramientas de IA y Tecnologías Cuánticas**

Este perfil es particularmente valioso porque combina capacidades operativas inmediatas (análisis de seguridad mediante IA) con preparación estratégica a largo plazo (defensa ante amenazas cuánticas). Las organizaciones necesitan profesionales que no solo puedan responder a los desafíos de seguridad actuales, sino que también estén preparados para la transición hacia un entorno donde la computación cuántica sea una realidad, especialmente en sectores como finanzas, salud, energía y , sobretodo, defensa. En este trabajo utilizarás herramientas de IA para detectar patrones anómalos, analizarás los sistemas críticos para determinar su resistencia ante futuros ataques con ordenadores cuánticos, priorizando la actualización de infraestructuras vulnerables, desplegarás soluciones de seguridad que combinan criptografía tradicional con algoritmos postcuánticos, asegurando la protección tanto contra amenazas actuales como futuras. Y utilizarás sistemas de IA predictiva para anticipar posibles vectores de ataque, pudiendo desarrollar las defensas antes de que las amenazas se materialicen.

- **Analista de Ciberinteligencia Militar**

Te dedicarás a detectar y analizar amenazas avanzadas contra infraestructuras críticas. Utilizarás IA para procesar grandes volúmenes de datos y detectar patrones de ataque, mientras implementas protecciones postcuánticas para la información. Esta labor es fundamental ya que las potencias extranjeras están invirtiendo en capacidades cuánticas con fines militares.

- **Especialista en Guerra Electrónica**

Serás el experto que desarrolla y protege sistemas de comunicaciones militares resistentes a la computación cuántica. Diseñando contramedidas contra interferencias y ataques, usando IA para adaptarte en tiempo real a las amenazas. Este rol es crucial porque los sistemas de comunicación seguros son, y serán, la columna vertebral de las operaciones militares modernas.

- **Auditor de Seguridad en Sistemas de Armamento Inteligente**

Serás el profesional que evalúa las vulnerabilidades en sistemas de armamento que incorporan IA, asegurando que no puedan ser comprometidos por adversarios. Verificarás la resistencia de estos sistemas ante futuros ataques cuánticos y garantizarás que cumplan con los protocolos de seguridad.

- **Desarrollador de Criptografía para Comunicaciones Tácticas**

Implementarás algoritmos postcuánticos en dispositivos de comunicación militar de campo, asegurando que las comunicaciones tácticas permanezcan seguras incluso ante capacidades de descifrado avanzadas. Este trabajo será vital porque la confidencialidad de las comunicaciones determinará el éxito de una operación.

- **Investigador en Defensa Contra Amenazas Cuánticas**

Analizarás las implicaciones de seguridad de las tecnologías cuánticas emergentes, desarrollando contramedidas preventivas y contribuyendo a la estrategia nacional de seguridad cuántica. Este trabajo es clave en la estrategia nacional ya que ayudará a mantener la ventaja tecnológica en el ámbito de la defensa.

Comparativa de perfiles tecnológicos

Contenido	Especialista en seguridad	Científico de datos	Especialista computación cuántica	CISO Essential	Top CISO
Fundamentos de programación	Experto	Experto	Experto	Experto	Experto
Fundamentos de Seguridad	Experto	—	—	Experto	Experto
Seguridad en Redes e Infraestructura	Experto	—	—	Experto	Experto
Seguridad en la Nube y Virtualización	Experto	—	—	Experto	Experto
Seguridad de Datos y Aplicaciones	Experto	—	—	Experto	Experto
Operaciones de Seguridad y Respuesta a Incidentes	Experto	—	—	Experto	Experto
Gobierno, Riesgo y Cumplimiento	Experto	—	—	Experto	Experto
Ciberseguridad y Hacking Ético	Experto	—	—	Experto	Experto
Fundamentos de Computación Cuántica	—	—	Experto	-	Experto
Algoritmos Cuánticos y Quantum Machine Learning	—	—	Experto	-	Avanzado
Ciberseguridad Cuántica	—	—	Básico	-	Experto
Infraestructura de Clave Pública Cuántica	Básico	—	—	-	Experto
Algoritmos y Protocolos Cuánticos	Básico	—	Básico	-	Experto
Derecho tecnológico	—	—	—	-	Avanzado
Implementación Segura de Sistemas Cuánticos	Básico	—	—	-	Experto
Blockchain y Criptografía Cuántica	Básico	—	—	-	Avanzado
IoT Security en la Era Cuántica	Básico	—	—	-	Avanzado
Cloud Security y Computación Cuántica	Básico	—	—	-	Avanzado
Seguridad en Comunicaciones Cuánticas	Básico	—	Básico	-	Avanzado
Auditoría de Sistemas Criptográficos	Experto	—	—	-	Experto
Inteligencia Artificial Aplicada a la Ciberseguridad	Básico	Básico	—	Avanzado	Experto
Fundamentos de Machine Learning	Básico	Experto	Básico	Avanzado	Experto
Fundamentos de Deep Learning	—	Experto	Básico	Avanzado	Experto
Fundamentos de IA Generativa	—	Experto	—	Experto	Experto
Detección de Amenazas Asistida por IA	Básico	—	—	Avanzado	Experto
Técnicas avanzadas de IA y Computación Cuántica	—	—	Avanzado	-	Avanzado
Automatización y Orquestación de Seguridad con IA	Básico	—	—	Avanzado	Avanzado
IA para Remediación de Criptografía Heredada	—	—	—	-	Avanzado
Ciencia Forense Digital Avanzada con IA	Básico	—	—	Básico	Avanzado

Toolbox al finalizar

Lenguaje de programación

Python

Arquitectura en la nube

Google Cloud

Computación Cuántica e IA Cuántica

- IBM Quantum
- Qiskit

Blockchain

Conseguirás:

Machine Learning (ML)

- Frameworks (Tensorflow, PyTorch, Keras)
- Evaluación de modelos
- Visualización de datos
- Algoritmos de Clustering

Deep Learning (DL)

- Redes Neuronales Convolucionales (CNN)
- Redes Neuronales Recurrentes (RNN)
- Análisis Componentes Principales (PCA)
- Procesamiento Lenguaje Natural (NLP)
- Modelos Gráficos Probabilísticos (PGM)
- Redes Bayesianas (BN)
- Redes Generativas Adversarias (GAN)
- Variational Autoencoder (VAE)
- Deep Autoencoders (AE)
- Aprendizaje por Refuerzo (RL)
- Sistemas de Recomendación
- Aprendizaje por Transferencia (TL)
- Large Learning Models (LLM)
- Inteligencia Artificial Explicable (XAI)
- ...

Derecho tecnológico

Aplicado a:

- La Inteligencia Artificial
- Los servicios de plataforma y distribuidos
- La criptografía y prestadores de servicios de confianza
- Derecho aplicado a la Identidad Digital
- Marco jurídico de la Defensa Nacional en el Ciberespacio

Ciberseguridad

- OpenVAS para análisis de vulnerabilidades
- Metasploit Framework
- IBM QRadar SIEM
- Wireshark y tcpdump
- OSSEC para detección de intrusiones

Infraestructura de Clave Pública Postcuántica

- OpenSSL con soporte PQC
- IBM PKI Suite
- IBM QRadar SIEM
- Wireshark y tcpdump
- OSSEC para detección de intrusiones

Infraestructura de Clave Pública Postcuántica

- OpenSSL con soporte PQC
- IBM PKI Suite
- NIST PQC reference implementations
- Bouncy Castle
- DigiCert PKI platform

Algoritmos y Protocolos Postcuánticos Básicos

- Liboqs
- Open Quantum Safe
- PQClean
- XMSS reference implementation
- IBM PQC Toolkit

Implementación Segura de Sistemas Postcuánticos

- IBM Security Remediator
- IBM Security AppScan
- ChipWhisperer
- Side-channel analysis tools
- Riscure Inspector

Algoritmos y Protocolos Postcuánticos Avanzados

- CRYSTALS-Kyber implementatio
- CRYSTALS-Dilithium tools
- Falcon signature implementation
- McEliece cryptosystem tools
- SPHINCS+ toolkit

Blockchain y Criptografía Postcuántica

- Hyperledger Fabric
- Quantum-safe crypto libraries
- IoT Security en la Era Postcuántica
- MQTT security tools
- Embedded crypto libraries

Seguridad en Comunicaciones Cuánticas

- QKD
- Quantum random number generators

Auditoría de Sistemas Criptográficos

- IBM Security Guardium
- OpenSCAP
- Compliance automation tools

Habilidades adquiridas

- **Desarrollo de algoritmos criptográficos cuánticos**: Capacidad para implementar y personalizar esquemas criptográficos resistentes a ataques cuánticos.
- **Análisis avanzado de amenazas con IA**: Habilidad para diseñar y utilizar sistemas de inteligencia artificial que detecten patrones de ataque complejos y anomalías en tiempo real.
- **Auditoría de seguridad cuántica**: Competencia para evaluar la resistencia de sistemas y aplicaciones ante potenciales ataques de computación cuántica.
- **Desarrollo de modelos adversarios en IA**: Capacidad para crear y defender contra ataques adversarios que manipulen sistemas de IA, incluyendo inyección de datos maliciosos y ataques de evasión.
- **Gestión de transición criptográfica**: Habilidad para diseñar e implementar planes de migración de infraestructuras criptográficas existentes hacia soluciones cuánticas, minimizando riesgos durante la transición.
- **Análisis forense avanzado**: Capacidad para utilizar técnicas de IA en la investigación de incidentes de seguridad y recuperación de evidencias digitales en entornos complejos.
- **Desarrollo de sistemas de autenticación resistentes**: Diseño de mecanismos de autenticación inmunes a las capacidades de la computación cuántica.
- **Privacidad diferencial**: Habilidad para implementar técnicas avanzadas de privacidad en sistemas de IA que protejan datos sensibles durante el entrenamiento y la inferencia.
- **Diseño de arquitecturas de seguridad híbridas**: Capacidad para diseñar infraestructuras que integren efectivamente seguridad tradicional, computación cuántica e inteligencia artificial.
- **Investigación en vulnerabilidades emergentes**: Habilidad para identificar, analizar y mitigar nuevas categorías de vulnerabilidades, en la intersección entre la inteligencia artificial y las tecnologías cuánticas.

Un programa ÚNICO

Nos diferenciamos del resto de programas de ciberseguridad ***por múltiples razones***, que lo convierten en un máster realmente ÚNICO.

Naturaleza del máster

La mayoría de másteres en ciberseguridad preparan perfiles operativos para ejecutar protocolos predefinidos y utilizar herramientas existentes. Este máster se centra en formar expertos capaces de diseñar nuevas herramientas, anticiparse a amenazas futuras y liderar la defensa en entornos críticos.

El objetivo no es formar usuarios de software de seguridad, sino arquitectos de soluciones avanzadas, que integren inteligencia artificial, criptografía postcuántica y análisis forense en sistemas reales. Profesionales que no reaccionan ante una amenaza, sino que se preparan antes de que ocurra.

Esta orientación eminentemente profesional, aplicada y estratégica, es la diferencia fundamental frente a cualquier máster académico. No nos limitamos a cubrir un temario, formamos a quienes serán contratados para defender infraestructuras críticas, desarrollar nuevos estándares de ciberdefensa y liderar la transición hacia entornos seguros frente a la computación cuántica.

Aquí no se estudia para superar exámenes, nos preparamos para anticipar ciberataques que aún no existen.

Se aprende con las manos

- Se huye del "profesor que lee cientos de diapositivas" y donde el alumno sale de clase sin haber aprendido realmente.
- Combina "un poco de teoría" y muchos ejercicios.
- Los alumnos tienen que resolver ejercicios de dificultad creciente.

No hay exámenes teóricos, sino prácticas

- Al finalizar cada bloque de conocimiento, los alumnos recibirán el enunciado de una práctica desafiante.
- Tendrán 3 semanas para completar y entregar dichas prácticas.
- El objetivo es simular un entorno de trabajo completamente real.

Posibilidad real de suspender

Este máster está diseñado para "separar el grano de la paja", con el objetivo de ser una cantera de excelencia. Y para conseguir dicha excelencia debe existir la posibilidad real de suspender.

Actualización constante de contenidos

Si bien, son muchas las escuelas de negocio que indican exactamente esto mismo, están lejos de lo que significa para nosotros actualizarse constantemente.

Éste es sin duda uno de los puntos más relevantes que diferencian a este máster. El contenido del programa es profundamente revisado en cada edición para ofrecer siempre los contenidos más punteros.

Los propios ingenieros de Google presentarán a los alumnos los últimos *papers* publicados, tanto por Google como por su competencia (Microsoft, Meta, Amazon), siendo el contenido de cada edición distinto y completamente actualizado.

Acceso a ordenadores cuánticos reales

Gracias a una estrecha colaboración con el laboratorio de cuántica de IBM, los alumnos tendrán acceso a ordenadores cuánticos de 154 Qbits.

La inmensa mayoría de másteres que imparten contenido de cuántica en España emplean simuladores cuánticos en Python.

Programa certificado por Google, IBM y las principales entidades de ciberseguridad

El máster está diseñado para que el alumno no solo adquiera conocimientos de vanguardia, sino que obtenga las certificaciones más reconocidas a nivel internacional en el ámbito de la ciberseguridad, la inteligencia artificial y la computación cuántica.

Durante el programa, los alumnos recibirán formación oficial alineada con los contenidos exigidos por las siguientes certificaciones profesionales:

- CompTIA Security+ (D5): Reconocida mundialmente como la puerta de entrada a la ciberseguridad profesional, esta certificación garantiza el dominio de los fundamentos de seguridad, criptografía, gestión de amenazas y cumplimiento normativo.
- CompTIA CASP+ (D5): Enfocada en profesionales senior, valida las capacidades para diseñar e implementar soluciones de ciberseguridad en entornos empresariales complejos, incluyendo entornos híbridos y multinube.
- CCSP – Certified Cloud Security Professional (D5): Acreditada por (ISC)², esta certificación avala la competencia para asegurar arquitecturas cloud complejas, tanto desde una perspectiva técnica como normativa.
- CISSP – Certified Information Systems Security Professional (D1): Considerada la certificación de referencia global para CISOs y responsables de seguridad, garantiza una visión integral de la seguridad en entornos críticos y altamente regulados.

En el ámbito de la Inteligencia Artificial, el máster incluye formación oficial impartida directamente por ingenieros de Google.

- Google Cloud – Professional Machine Learning Engineer (PMLE): Una de las credenciales más prestigiosas en el campo de la IA, que certifica la capacidad para diseñar, implementar y mantener modelos de aprendizaje automático escalables y robustos en entornos cloud.

En el módulo de computación cuántica, el máster cuenta con profesionales del equipo de IBM Quantum.

- IBM Qiskit Developer: Certificación que valida el conocimiento de los principios fundamentales de computación cuántica, así como la capacidad para desarrollar algoritmos cuánticos, poniendo en el máster especial énfasis en aplicaciones concretas para criptografía cuántica y análisis forense.

Empleabilidad y cantera de laboratorios de ciberseguridad

El perfil de experto en ciberseguridad avanzada con conocimientos en inteligencia artificial y computación cuántica es, actualmente, uno de los más escasos y estratégicos del mercado. Sectores críticos como defensa, infraestructuras esenciales, energía, banca, aseguradoras, centros de investigación y organismos internacionales necesitan profesionales capaces de anticiparse a amenazas complejas, incluyendo las derivadas del avance de la computación cuántica.

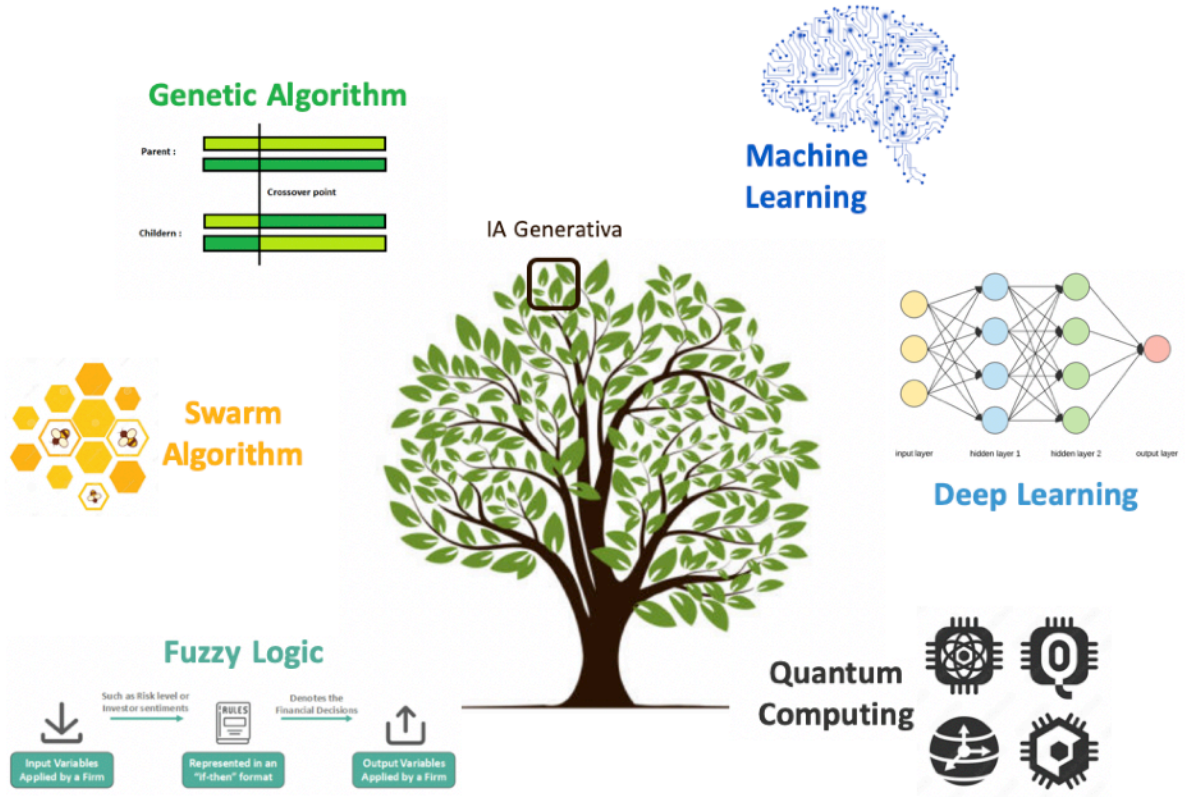
El máster está diseñado para ser una cantera directa de talento para laboratorios de ciberseguridad tanto del sector público como privado, incluyendo centros tecnológicos del Ministerio de Defensa, instituciones europeas, y divisiones de ciberinteligencia de grandes empresas. Gracias a la colaboración con estos laboratorios, los estudiantes podrán trabajar en proyectos reales y participar en retos estratégicos propuestos por las entidades colaboradoras, lo que aumenta significativamente las oportunidades de inserción laboral.

Nuestro objetivo es que el 100% de los egresados acceda a posiciones estratégicas, convirtiéndose en parte activa de la defensa tecnológica de nuestras infraestructuras críticas, en España y en el extranjero.

En el máster no se estudia únicamente Deep Learning

Existen 5 ramas de Inteligencia Artificial:

- Algoritmos Genéticos
- Algoritmos Enjambre
- Lógica Difusa
- Machine Learning y Deep Learning
- Modelos Híbridos Cuánticos



El programa de este máster es el único existente donde se profundizará en las 5 ramas de conocimiento de la Inteligencia Artificial. Ahondando en cada concepto y explicando lo que se está utilizando actualmente en la industria.

La IA no sólo es Generativa

El futuro pasa indudablemente por los modelos híbridos de IA cuántica, y su aplicación a la ciberseguridad. En el máster profundizaremos en estos modelos, y sus aplicaciones a la ciberseguridad y defensa.

Modelos híbridos de IA cuántica

- Quantum Support Vector Machine
- Quantum Convolutional Neural Networks
- Quantum Recurrent Neural Networks
- Quantum Generative Adversarial Network
- Quantum Reinforcement Learning
- Quantum Bayesian Networks
- Quantum Autoencoder
- Quantum Transfer Learning
- Quantum Transformer
- Quantum Genetic Algorithms
- Quantum Blockchain
- Quantum Swarms

Calidad de los profesores

El profesorado es el activo más valioso del máster, por lo que la selección de profesores es una de las partes a la que se dedica más tiempo y atención.

Todos los profesores han sido cuidadosamente seleccionados por:

- Sus profundos conocimientos en el área de conocimiento que imparten.
- Su capacidad de transmitir todos esos conocimientos a los alumnos.
- Su experiencia real en proyectos en empresas.

Comunidad y actualización de contenidos para los egresados

Para nosotros el máster no termina con la última clase.

Dado el ritmo acelerado de obsolescencia en muchas áreas de estudio de nuestros másters, nuestra plataforma innovadora ofrece a los egresados acceso a actualizaciones continuas y relevantes del contenido estudiado.

Los *alumni* son embajadores naturales de nuestros programas. Su éxito profesional y su satisfacción con la formación recibida refuerzan la reputación del máster y atraen a nuevos estudiantes.

Una vez finalizado un máster, las calificaciones pierden importancia; lo que realmente importa es la reputación, que debe continuar evolucionando, mostrándose y siendo utilizada como moneda de valor para el crecimiento profesional, obteniendo:

- Descuentos en futuras formaciones y másters
- Asistencia a conferencias internacionales
- Actualización gratuita de contenidos

Factores que influyen en la reputación

- Contribuir al aprendizaje de otros: Respondiendo dudas de alumnos en los foros de la escuela, ayudando a crear un ambiente de colaboración y apoyo mutuo.
- Publicar investigaciones o papers junto a la escuela, compartiendo tu conocimiento con la comunidad académica y profesional.
- Participar activamente en las competiciones de la escuela, demostrando tu capacidad y compromiso en contextos prácticos y desafiantes.
- Compartir tu experiencia personal en redes sociales, publicando videos y testimonios sobre tu recorrido en la escuela, inspirando a otros y posicionándote como referente.
- Desarrollar proyectos innovadores y servicios en colaboración con la escuela, aportando soluciones concretas que beneficien a la comunidad.
- Atraer nuevos estudiantes, recomendando la escuela a futuros aspirantes y siendo un embajador de la marca.
- Colaborar en eventos y actividades de la escuela, participando en conferencias, seminarios o mentorías que refuercen tu papel como líder dentro de la comunidad.

Factores que influyen en la ética

- Afectar negativamente la imagen de la escuela, ya sea a través de actitudes destructivas, comentarios malintencionados o acciones que dañen su prestigio.
- Mantener comportamientos poco éticos o violentos, como prácticas deshonestas, conflictos innecesarios o actitudes que comprometan la integridad personal o institucional.
- Ignorar las normas de la comunidad, violando las políticas académicas, éticas o de comportamiento que rigen la escuela.
- Desprestigiar a compañeros o miembros de la comunidad, generando conflictos sin justificación y contribuyendo a un ambiente tóxico.
- Desinterés o abandono de los compromisos adquiridos, dejando proyectos o tareas a medias y afectando el trabajo colectivo.

En la visualización de cualquier perfil se podrán consultar los conocimientos, reputación y certificaciones de la persona con la que estés interactuando. Asimismo, esa persona podrá ver los tuyos.

Los conocimientos mostrarán el año en que se adquirieron, por lo que es importante actualizar con recurrencia los mismos.

Conocimiento, reputación y propósito son los tres pilares fundamentales de AthenAI

7

Claustro de expertos y docentes

El profesorado es el ***activo más valioso del máster***, por lo que la selección de profesores es una de las partes a la que hemos dedicado más tiempo y atención.

Profesor		Especialidad	Formación	Puesto actual
	**Álvaro Suárez Bravo**	Blockchain	- Licenciado en ingeniería de la computación - Máster en ciencia de la computación	Principal Software Engineer **DLT Finance AG**
	**Ángel Luis Quesada Nieto**	Blockchain	- Licenciado en matemáticas - MBA, Máster en Dirección de Empresas para Emprendedores	Founder & CEO **Onyze, Kubide & Climbspot**
	**Christian Oliva**	Inteligencia Artificial	- Grado en Ingeniería Informática, Ingeniería informática - Master en Investigación e Innovación en Inteligencia Computacional y Sistemas Interactivos - Doctorando en Ingeniería Informática - Neurocomputación biológica y Machine learning	Profesor Ayudante e Investigador **Universidad Autónoma de Madrid (UAM)**
	**Eva Álvarez del Manzano**	Ciberseguridad **Dirección académica**	- Licenciada en filosofia y psicopedagogía - Máster de Director de seguridad - Medalla al mérito en Ciberdefensa. Asociación Profesional de Peritos de Nuevas Tecnologías (PETEC)	Responsable de proyectos especiales **defensa.com** Co CEO **CESN** Asesora Industria Militar **jaton racing**
	**Franco Dante Albareti**	Computación Cuántica	- Licenciado en Física (1º de promoción) - Máster en física teórica, cosmología y partículas elementales - Doctorado en física teórica y curvas espacio temporales (1º promoción) - Máster en Inteligencia Artificial Aplicada a los Mercados Financieros (mIAX)	Senior Software Engineer **Affirm**
	**Ginés Carrascal de las Heras**	Computación Cuántica **Dirección académica**	- Licenciado en física, óptica y electrónica - Máster en microanálisis espectral con láser	Quantum Computational Scientist **IBM Quantum**
	**Guillermo Meléndez Alonso**	Inteligencia Artificial	- Diplomado en Empresariales (1º de promoción) - Licenciado en dirección de empresas (1º de promoción) - Máster en auditoria - Máster en finanzas cuantitativas - Máster en Bolsa e inversiones alternativas - Máster en Data Science y Big Data (1º de promoción) - Máster en Deep Learning (1º de promoción)	CEO **AthenAI**
	**José Cándido Carballido López**	Computación Cuántica	- Ingeniero en Informática de sistemas - Master de seguridad de las tecnologías de la información y de las comunicaciones (MISTIC)	Cyberdefend Practice Leader & CTO **SPG**
	**Jose Zamora**	Inteligencia Artificial	- Doble Grado en Ingeniería Informática y Hardware - Master en Computer Vision - Máster en Digital Intelligence - MBA	Director de IA, GenAI y MLOps

Profesor		Especialidad	Formación	Puesto actual
	**Luis Fernando Lago Fernández**	Inteligencia Artificial + Matemáticas	- Licenciado en Física - Licenciado en Matemáticas - Doctor en informática	Departamento de Neurocomputación Biológica **Universidad Politécnica de Madrid**
	**Manuel Sánchez Montañés Isla**	Inteligencia Artificial	- Licenciado en física - Doctorado en ingeniería informática	Investigador **Universidad Autónoma de Madrid**
	**Minerva Rodríguez Cabrera**	Inteligencia Artificial	- Máster en Inteligencia Artificial Aplicada a los Mercados Financieros (mIAX)	Analista de Operaciones del Broker **Darwinex**
	**Paloma Llaneza González**	Derecho	- Licenciada en Derecho con Matrícula de honor, mientras cursaba un grado medio de programación de ordenadores - Diploma de Altos Estudios Europeos	Abogado, CISA y Socio Director **Razona Legaltech**
	**Pedro Ventura Gómez**	Inteligencia Artificial	- Máster en Inteligencia Artificial Aplicada a los Mercados Financieros (mIAX) (1º de promoción) - Experto en Gestión de Back Office, Servicios financieros y de gestión financiera - Ingeniero Técnico de Telecomunicaciones	Director de Proyectos **March Asset Management**
	**Rafael Sánchez**	Inteligencia Artificial + Big Data	- Licenciado en telecomunicaciones - Doctor en ingeniería y telecomunicaciones	Manager, Generative AI / ML, Southern Europe and Middle East **Google**
	**Ricardo Estefanescu Abad**	Computación Cuántica	- Grado en Ingeniería de Computadores - Profesor de Computación Cuántica Universidad Francisco de Vitoria - IBM Senior Quantum Ambassador	CTO **Puffin Security**
	**Roberto García Pérez**	Computación Cuántica	- Ingeniero en Informática	Security Specialist (27 años) **IBM**

ΑΘΗΝΑΙ
Technological Business School

8

Información general

Información General

Duración

Programa completo equivalente a 146 ECTS

CISO Essential

- Equivalente a 54 ECTS
- 450 horas lectivas
- 1.350 horas lectivas + estudio
- 12 meses

Fecha de inicio	*Fecha de finalización*
10 de abril de 2026	16 de marzo de 2027

Top CISO

- Equivalente a 92 ECTS
- 765 horas lectivas
- 2.290 horas lectivas + estudio
- 15 meses

Fecha de inicio	*Fecha de finalización*
2 de abril de 2027	27 de junio de 2028

Horario

Miércoles y jueves de 19 a 21:30 horas

Viernes de 16 a 21 horas

Sábados de 9 a 14 horas

* Las clases de los miércoles, jueves y viernes serán impartidas exclusivamente online.
* Las clases de los sábados serán impartidas de manera presencial y online.

Localización

Los másters Essential se imparten en formato 100% online.

Los másters Top combinan formación online con sesiones presenciales, aunque pueden realizarse 100% online. Todas las ediciones presenciales se realizan en Madrid.

Precio

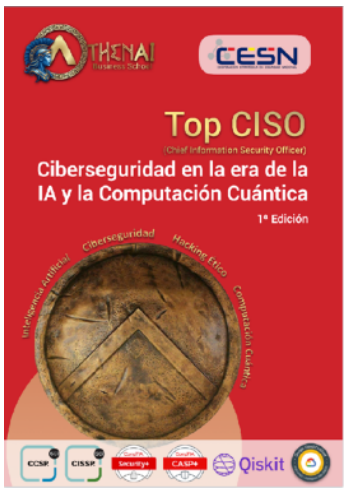
El precio del programa **CISO Essential** es de 11.000 €

El precio del programa **Top CISO** es de 19.000 €

El precio del **programa completo** es de 30.000 €

Convalidación de contenidos entre másters: una ventaja única

Centrado en Mercados Financieros, IA y Computación Cuántica



Centrado en Ciberseguridad, IA y Computación Cuántica

Centrado en la figura del Chief of Artificial Intelligence Officer (CAIO)

Centrado en Derecho y Nuevas Tecnologías

En nuestra escuela, cada máster está especializado en un área distinta, pero todos comparten una base de conocimientos común en los bloques de nuevas tecnologías: Python, IA, Servicios Cloud, Ciberseguridad, Computación Cuántica...

Esta estructura permite que los alumnos cursen las materias comunes sólo una vez, de modo que se beneficien de la **convalidación automática de contenidos en cualquier otro máster** que elijan.

Supongamos que cursas primero el Máster ***Top Quant*** cuyo precio es de **27.000€**. Al finalizarlo, habrás completado gran parte del contenido común de otros másters, por lo que:

- Podrás acceder a los demás másters convalidando automáticamente esos bloques de contenido ya cursados*.
- El precio de los siguientes másters se reducirá de forma significativa**.
- Podrías **cursar los 4 másters por solo 50.000€*****,** en lugar de pagar 108.000 € (27.000€ × 4 másters).

Esto genera un potente efecto apalancador en tu formación: más conocimiento, mayor especialización, menor coste.

* Si accedes a un máster con más del 50% de los contenidos convalidados, éste será exclusivamente online.

** El precio de cada máster será como mínimo del 20% de su valor inicial.

*** Este precio es un ejemplo aproximado, ya que varía en función de cada máster.

**** Las convalidaciones sólo podrán aplicarse en caso de haber superado con éxito el Máster de origen.

En 2025, AthenAI estableció un programa para formar a los mejores CISO del mundo. Su propósito era enseñar a combinar tecnologías avanzadas y estrategias de defensa para liderar los departamentos de ciberseguridad.

El nombre oficial del Máster era:

"Ciberseguridad en la era de la Inteligencia Artificial y la Computación Cuántica".

Los alumnos lo conocían como…

Top CISO