ATHENAI
Technological Business School

CESN
COOPERACIÓN ESTRATÉGICA EN SEGURIDAD NACIONAL

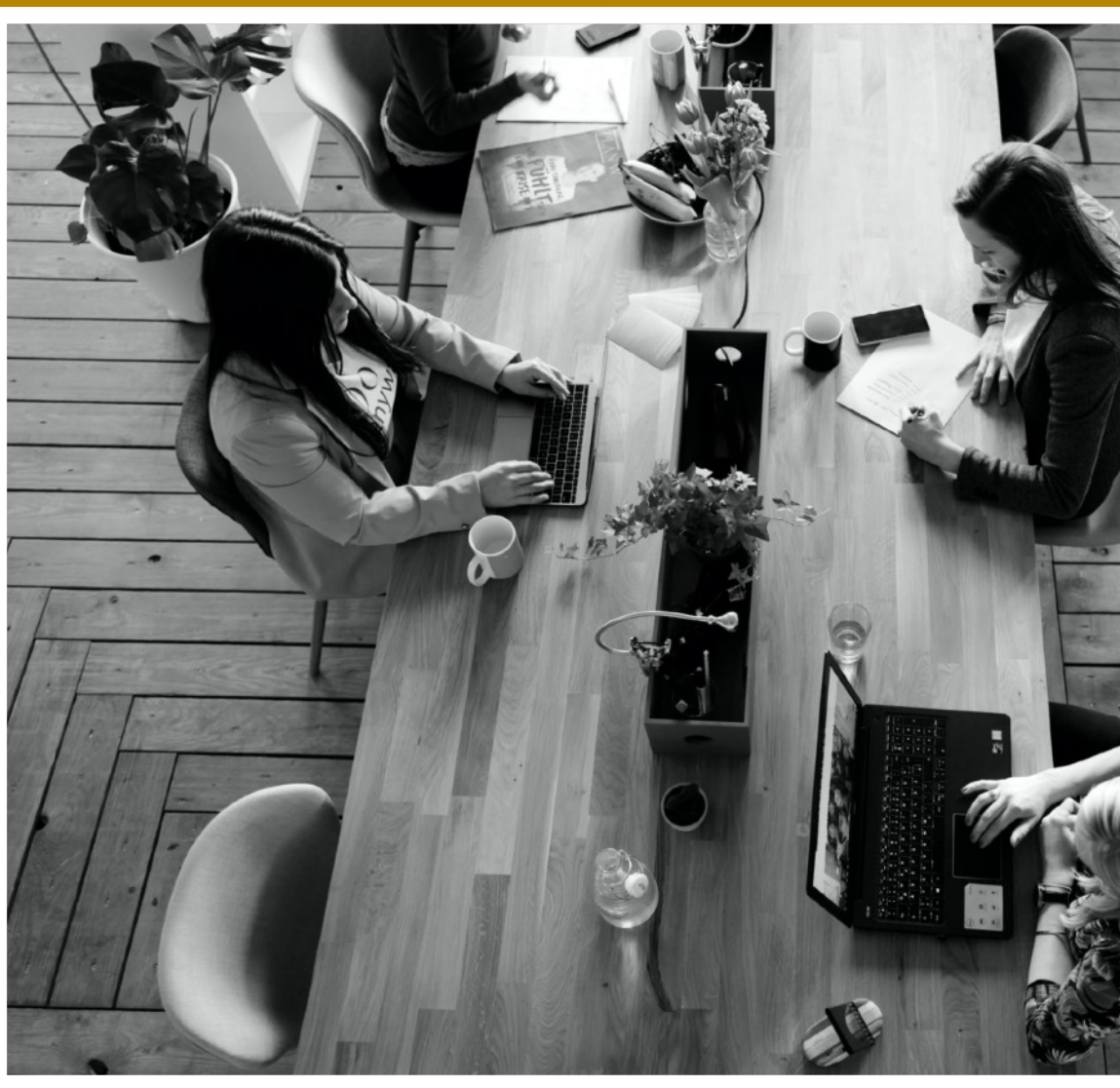
Top Level-C

Emerging Tech & Digital Executive Leadership

1ª Edición

CCSP ISC2
CISSP ISC2
CompTIA Security+
CompTIA CASP+
Google Cloud Certified PROFESSIONAL MACHINE LEARNING ENGINEER
Google Cloud Certified PROFESSIONAL DATA ENGINEER
Google Cloud Certified PROFESSIONAL CLOUD ARCHITECT

Contenido



ATHENAI
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 cumplir sus sueños a través del esfuerzo y el aprendizaje profundo, ya sea fundar **su propia start-up**, **crear un unicornio**, 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

Alcanza un Level-C especializándote en
Inteligencia Artificial aplicada a negocio.

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

Top Level C: la élite en riesgos y gobernanza, ciberseguridad, Inteligencia Artificial y Computación Cuántica.

Top Level C no es solo un programa formativo, es un reto intelectual de máxima exigencia diseñado para quienes aspiran a liderar el futuro de los riesgos y la gobernanza 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:

- **Level C Essential**: 450 horas lectivas, equivalentes a 54 ECTS (primer año lectivo).
- **Top Level C**: 600 horas lectivas, equivalentes a 72 ECTS (segundo año lectivo).

Además, el programa **incorpora 7 certificaciones oficiales de primer nivel**, otorgadas por las entidades de referencia en cada disciplina:

Certificaciones Level C Essential:

- Professional Cloud Architect (PCA), emitida por Google.

Certificaciones Top Level C:

- 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 Data Engineer (PDE), emitida por Google.
- Professional Machine Learning Engineer (PMLE), emitida por Google.

Los alumnos pueden decidir cursar únicamente el programa ***Level C 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 Level C***. Este programa integral exige haber superado previamente el Essential y representa la cumbre de la formación en riesgos y gobernanza, ciberseguridad, Inteligencia Artificial y Computación Cuántica.

Top Level C no se estudia: SE CONQUISTA

Objetivo

El **objetivo de la escuela** es reflejar su compromiso con la excelencia académica y profesional, ofreciendo un programa integral y transformador que dote a los alumnos de las competencias necesarias para desempeñar con éxito el rol de Chief Artificial Intelligence Officer (CAIO) en entornos empresariales dinámicos y globalizados.

El propósito fundamental del máster es **otorgar a los alumnos una formación estratégica, avanzada y diferenciadora**, que les permita liderar con visión, rigor y responsabilidad, la adopción y gestión de soluciones de Inteligencia Artificial en sus organizaciones.

Al finalizar el programa, los participantes serán capaces de:

- **Comprender en profundidad los fundamentos técnicos de la IA, tanto de machine learning como de deep learning**, aplicados a contextos empresariales reales.
- **Diseñar y gobernar arquitecturas modernas basadas en tecnologías cloud**, integrando plataformas escalables de IA.
- **Dominar los principios de ética, regulación y gobernanza de la IA**, incluyendo el cumplimiento del AI Act y los marcos internacionales.
- **Evaluar, seleccionar e implementar tecnologías de IA** alineadas con los objetivos estratégicos de la empresa.
- **Definir, impulsar y alinear la estrategia corporativa de IA con los objetivos de negocio**, liderando su integración transversal en la organización.
- **Gestionar riesgos operativos, legales y reputacionales**, asociados al uso de la Inteligencia Artificial.
- **Fomentar una cultura organizativa orientada a la innovación responsable**, promoviendo la adopción ética de la IA.
- **Desarrollar pensamiento crítico y visión de futuro**, anticipando tendencias tecnológicas y su impacto en el negocio.
- **Participar en una comunidad global de expertos y líderes en IA**, creando redes de colaboración y oportunidades profesionales.

Naturaleza del máster

Conviértete en el Chief Artificial Intelligence Officer que toda organización necesita

Este máster está diseñado para formar a los futuros líderes en gobernanza de la Inteligencia Artificial, profesionales capaces de diseñar, desplegar y supervisar una estrategia de IA de extremo a extremo en cualquier organización. A lo largo del programa, adquirirás las competencias necesarias para construir un marco integral de gobernanza de IA, incluyendo políticas, procedimientos e instrumentos que aseguren un uso responsable, eficaz y alineado con los objetivos corporativos.

El itinerario formativo combina una profunda base técnica con un enfoque estratégico. Recorrerás el camino desde las matemáticas que sustentan los modelos de IA hasta su implementación práctica, incluyendo redes neuronales avanzadas y modelos fundacionales de última generación. Esta formación te permitirá no solo comprender y desarrollar modelos de IA, sino también evaluar soluciones externas con criterios técnicos y de negocio.

Además, el máster proporciona una sólida formación en gestión de riesgos y cumplimiento normativo, capacitándote para identificar, mitigar y gestionar los riesgos asociados al ciclo de vida completo de los modelos de IA. Aprenderás a reducir la incertidumbre en los procesos de evaluación y toma de decisiones, aportando rigor técnico y criterios éticos a cada iniciativa.

En un contexto donde la ciberseguridad es clave, también te formarás en los riesgos específicos de los sistemas de IA: cómo anticiparlos, prevenirlos, estresarlos y responder ante incidentes, garantizando la resiliencia tecnológica de tu organización.

Este máster transforma al alumno en un profesional con una visión integral de la IA, capaz de liderar tanto a nivel estratégico como operativo, y de colaborar con perfiles clave como CTOs, CISOs, responsables de riesgos, compliance u oficinas de transformación.

En definitiva, este programa te prepara para asumir el rol de Chief Artificial Intelligence Officer (CAIO), la figura esencial en cualquier organización que aspire a utilizar la IA de forma segura, responsable y competitiva.

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 habilidades y adquirirá conocimientos en diversos aspectos clave para convertirse en el CAIO de una organización.

Esto incluye conocimientos profundos en Inteligencia Artificial tanto desde el punto de vista de modelos, infraestructuras, arquitecturas y casos de uso, marcos de gobierno, marcos regulatorios y estrategia, gestión de proyectos de IA, gestión de riesgos derivados de la inteligencia artificial, marcos de gobierno del dato, fundamentos de seguridad incluyendo conocimientos profundos de ciberseguridad e IA aplicada a la ciberseguridad y evaluación de proveedores.

Este máster es para ti si vas a dedicar un **mínimo de 3 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: pasión por la innovación y adquirir las competencias y habilidades necesarias para asumir el rol de un CAIO en las empresas.

Así, este máster está especialmente dirigido a profesionales con interés por la tecnología, la ciencia de datos, la estrategia y la innovación, a directivos que quieran evolucionar hacia roles Level-C con foco en IA, y a emprendedores que buscan liderar negocios basados en IA.

a) Actuales perfiles Level-C

Si ya ocupas un cargo de alta dirección (como CDO, CTO, CIO, CRO, CISO, CCO o CDO Digital) o estás en proceso de transición hacia una posición ejecutiva, probablemente ya cuentes con una visión estratégica del negocio y experiencia liderando equipos, proyectos o áreas tecnológicas clave.

Este máster es para ti si quieres:

- Actualizarte en Inteligencia Artificial avanzada y sus aplicaciones reales en entornos corporativos.
- Dominar la integración estratégica de la IA en todas las áreas del negocio.
- Liderar la transformación digital desde la alta dirección, impulsando la innovación responsable.
- Entender los marcos normativos clave (como el AI Act europeo) y su impacto organizativo.
- Establecer una gobernanza efectiva de la IA, asegurando escalabilidad, ética y cumplimiento.
- Interactuar con equipos técnicos con mayor profundidad, desde una perspectiva ejecutiva y de negocio.
- Consolidar tu perfil como Chief Artificial Intelligence Officer (CAIO) y formar parte de una comunidad de líderes en IA empresarial.

b) 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:

- Inteligencia Artificial Avanzada y machine learning, herramientas tecnológicas y aplicaciones de negocio.
- Modelos de negocio, roles y estrategia empresarial que integren la IA en todos los niveles organizativos.
- Gestión y dirección de proyectos de IA.
- Gestión y evaluación de proveedores.
- Implementación de Marcos y Estándares normativos.
- Normativas internacionales de IA y derecho aplicado a la IA.
- Gestión del riesgo inherente a la IA.
- Fundamentos de ciberseguridad.

Este máster es para ti si quieres liderar la gestión y dirección de proyectos de Inteligencia Artificial en las empresas con una visión integral y realista de todo el ecosistema.

c) Perfil jurídico, riesgos o de auditoría

Si vienes del mundo de la auditoría, cumplimiento o riesgos, probablemente tengas sólidos conocimientos normativos y organizativos, pero una formación limitada en tecnología avanzada e IA aplicada.

Este máster es para ti si quieres:

- Profundizar en el mundo de la programación y las técnicas de Inteligencia Artificial.
- Modelos de negocio, roles y estrategia empresarial que integren la IA en todos los niveles organizativos.
- Gestión y dirección de proyectos de IA.
- Normativas internacionales de IA y derecho aplicado a la IA
- Fundamentos de ciberseguridad.

d) Perfil con conocimientos en Inteligencia Artificial

Si ya estás familiarizado con la programación y la Inteligencia Artificial, pero te falta la visión global de cómo gestionar y dirigir de manera transversal proyectos de IA en el seno de una empresa, este máster es para ti, adquirirás conocimientos en:

- Modelos de negocio, roles y estrategia empresarial que integren la IA en todos los niveles organizativos.
- Gestión y dirección de proyectos de IA.
- Gestión y evaluación de proveedores.
- Implementación de Marcos y Estándares normativos.
- Normativas internacionales de IA y derecho aplicado a la IA.
- Gestión del riesgo inherente a la IA.
- Fundamentos de ciberseguridad.

Los primeros módulos del programa están diseñados para equilibrar los conocimientos y la forma de trabajar de dichos perfiles.

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 una parte teórica y ejercicios de alta intensidad.

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 LLMs, etc. Las mismas herramientas que tendrán en su vida profesional, una vez terminen el programa.

Las prácticas serán desafiantes y enfocadas en problemas reales relacionados con la implementación de modelos de IA, gobernanza y gestión de los riesgos inherentes a la Inteligencia Artificial en el seno de una organización. 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, por lo que los alumnos contarán con la orientación de un tutor.

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 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, o a otra razón.

Dirección académica

Miguel García Cordo

Apasionado por la resolución de problemas y el diseño, desarrollo e implementación de ideas y proyectos innovadores, es un experto multidisciplinar con una carrera forjada en la intersección entre las finanzas y la tecnología. Su sólida base académica, que combina estudios superiores en **Ciencias Económicas (Licenciatura) y en Ciencias Matemáticas** por la Universidad Complutense de Madrid, enriquecida con un **Máster en Inteligencia Artificial aplicada a los Mercados Financieros (mIA-X)** y un **Máster en Inteligencia Artificial, impartido por el Instituto de Inteligencia Artificial**, y acreditada con las certificaciones internacionales **ISO 42001 AI Management Leader e ISO 38507 AI Governance Leader**, constituye el pilar de una trayectoria de más de quince años en el sector financiero. Su perfil aúna el conocimiento de la gestión de riesgos y los mercados financieros con una especialización avanzada en Inteligencia Artificial, lo que le confiere una posición privilegiada en la transformación digital.

Actualmente desarrolla la posición de **Chief Risk Officer (CRO)**, donde sobre él recae la responsabilidad de la estrategia y supervisión integral de los riesgos de la entidad. Su carrera se ha consolidado a través del desempeño de funciones de alta responsabilidad, incluyendo la de **Head of Risk Management and Middle Office en March Asset Management**, donde lideró el diseño y desarrollo de modelos propietarios para el análisis de liquidez y ESG, incluyendo ratings internos, criterios de exclusión, indicadores de apoyo a la sostenibilidad, análisis ESG ex-ante y modelización integrada de la sostenibilidad, y la de **Head of Risk Management en Nordkapp S.A.**

Con un firme compromiso hacia la sinergia entre el ámbito académico y el sector privado, participa activamente en la capacitación de las futuras generaciones de profesionales. Ejerce como **profesor, miembro del tribunal evaluador y tutor de trabajos de fin de máster en el Máster en Inteligencia Artificial aplicada a los Mercados Financieros (mIA-X) del Instituto BME**. Asimismo, contribuy´ como miembro del **Instituto para el Desarrollo de la Inteligencia Artificial en el Sector Financiero (IDIASEF)**, al avance y la correcta gobernanza de la IA en la industria.

Formación Complementaria y de Especialización

- Programas Directivos y Avanzados en Finanzas y Riesgos:
  - Programa Directivo en Finanzas Sostenibles.
  - Cursos Avanzados en Derivados y Riesgo de Contrapartida.
  - Programa Avanzado de Renta Fija.
  - Programa Avanzado de Financial Risk Management.
- Programas de Especialización en Tecnología y Ciencia de Datos:
  - Máster en Inteligencia Artificial aplicada a los Mercados Financieros (mIA-X)
  - Máster en Inteligencia Artificial, impartido por el Instituto de Inteligencia Artificial
  - Programa de Experto en Machine Learning.
  - Especialización en Lenguajes de Programación y Software: Matlab, Python, R, VB.Net y C#.
  - Certificación internacional ISO 42001 AI Management Leader e ISO 38507 AI Governance Leader.

Dominios de Especialización

- Gestión Integral de Riesgos Financieros (Mercado, Crédito y Contrapartida).
- Inteligencia Artificial y *Machine Learning* aplicados.
- Gobernanza de la Inteligencia Artificial (AI Governance).
- Finanzas Sostenibles e Inversión bajo criterios Ambientales, Sociales y de Gobernanza (ESG).
- Valoración de Instrumentos Financieros Derivados y de Renta Fija.
- Ciencia de Datos con Rstudio y Modelización Cuantitativa con Matlab.

Dirección académica

Raquel Hernández Falcón

Matemática especializada en finanzas, con más de diez años de trayectoria profesional en la intersección entre la modelización cuantitativa, la Inteligencia Artificial y los mercados financieros. Aúna una formación académica rigurosa con una **sólida experiencia práctica en valoración de instrumentos financieros, gestión integral de riesgos y desarrollo de soluciones algorítmicas**. Su perfil destaca por su capacidad para traducir problemas complejos en herramientas robustas, aplicables en entornos reales y regulados.

Graduada en Matemáticas, Máster en Finanzas Cuantitativas de Afi y **Máster en Inteligencia Artificial aplicada a los Mercados Financieros (mIA-X)**, cuenta además con formación especializada **riesgos financieros y programación**. Ha participado en proyectos de referencia tanto a nivel nacional como internacional, trabajando con diferentes entidades financieras, organismos reguladores y plataformas de compensación.

Actualmente desempeña el rol de **Trader de crédito**, donde, además de su actividad operativa, **se especializa en el desarrollo de modelos y algoritmos orientados al análisis, valoración y optimización de estrategias de inversión en productos de crédito**.

Comprometida con la transferencia de conocimiento y la formación de nuevas generaciones de profesionales, **participa activamente como docente** en másters de referencia, cursos expertos y programas corporativos impartidos por diferentes escuelas e institutos de finanzas.

Trayectoria profesional

- Trading de crédito en CecaBank
- Docencia en múltiples programas especializados
- Control de riesgos y cumplimiento normativo March Asset Management
- Consultoría cuantitativa y financiera en Afi (Analistas Financieros Internacionales)

Áreas de especialización

- Aplicación de la Inteligencia Artificial y Machine Learning en los mercados financieros
- Programación y ciencia de datos: Python, R, Matlab, VBA .NET, SQL
- Tecnologías y plataformas: AWS, Azure, Google Cloud
- Análisis e implementación de estrategias óptimas de inversión en productos de crédito
- Identificación, medición y control de riesgos financieros
- Modelización y análisis cuantitativo para la valoración de instrumentos financieros complejos

Estructura del programa

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

Estructura del Máster completo

Módulos	Horas lectivas	Peso	Horas estudio	Horas totales	ECTS
0. Presentación y sesiones TFM	30	3 %	60	90	**3,6**
1. Fundamentos de programación	55	5 %	110	165	**6,6**
2. Gobernanza y Fundamentos Estratégicos	70	7 %	140	210	**8,4**
3. Machine Learning y Deep Learning	105	10 %	210	315	**12,6**
4. Servicios cloud y big data	195	18 %	390	585	**23,4**
5. Deep Learning avanzado y generativo	175	17 %	350	525	**21**
6. Derecho tecnológico	60	6 %	120	180	**7,2**
7. Ciberseguridad y Hacking Ético	225	21 %	450	675	**27**
8. Riesgos y gobernanza	75	7 %	150	225	**9**
9. Computación Cuántica	40	4 %	80	120	**4,8**
10. Lanzamiento de tu propia startup	30	3 %	60	90	**3,6**
Total	**1.060**	**100 %**	**2.120**	**3.180**	**127**

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. Machine Learning y Deep Learning	105	23 %	210	315	**12.6**
3. Gobernanza y Fundamentos Estratégicos	70	16 %	140	210	**8,4**
4. Derecho tecnológico	60	13 %	120	180	**7,2**
5. Riesgos y gobernanza	75	17 %	150	225	**9**
6. 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. Servicios cloud y big data	125	20 %	250	375	**15**
2. Deep Learning avanzado y generativo	175	29 %	350	525	**21**
3. Ciberseguridad y Hacking Ético	225	37 %	450	675	**27**
4. Computación Cuántica	40	7 %	80	120	**4,8**
5. Lanzamiento de tu propia startup	30	5 %	60	90	**3,6**
Total	**610**	**100 %**	**1.220**	**1.830**	**73**

Programa ESSENTIAL

Módulo 1 | Fundamentos de programación
55 horas lectivas

Visión General del programa
- Presentación y alineación de objetivos
- Tecnologías emergentes
- 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 | 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
- Otros algoritmos de enjambre (ABC, crecimiento bacteriano, manada, PSO, ...)

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

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. Precision, 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
- Generación de características
- Extracción de atributos relevantes
- Reducción de dimensionalidad incorporando XAI
- Clustering
- Graphext (No-Code para data analysis)
- XAI de los resultados obtenidos

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

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

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

Redes Neuronales densas 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

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

Redes Neuronales densas 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 | Gobernanza y Fundamentos Estratégicos

70 horas lectivas

Introducción e historia de la IA - Enfoque Técnico

- ¿Qué es la IA?
- Historia de la IA
- Diferentes tipos de IA
- Técnicas y herramientas
- Algoritmos clásicos
- Desafíos éticos y sociales

Evolución de la IA y su impacto empresarial

- Principales etapas: IA simbólica, machine learning, deep learning, IA generativa
- Casos de uso representativos en cada etapa
- Efectos en eficiencia, productividad y modelos de negocio
- Cambios organizativos impulsados por la IA
- Nuevos riesgos y retos: éticos, regulatorios, tecnológicos

Estrategia Empresarial

- IA en las Organizaciones
- Modelos de Negocio
- Decisiones estratégicas
- Transformación Digital

Gestión de Proyectos de IA I

- Planificación y Gestión
- ML Ops
- Perfiles Técnicos

Gestión de Proyectos de IA II

- Cuando utilizar ML y problemas a resolver
- Software en Producción
- Infraestructura
- Mejores Prácticas en desarrollo
- Mejores prácticas en despliegue
- Herramientas

Etica Aplicada y principios responsables

- Principios clave: transparencia, justicia, no maleficencia, rendición de cuentas
- Evaluación del impacto social y ético de sistemas de IA
- Mitigación de sesgos y discriminación algorítmica
- Marcos regulatorios y normativos (UE, UNESCO, OCDE)
- Integración de la ética en el ciclo de vida del desarrollo de IA

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

Marcos regulatorios internacionales

- Reglamento de IA de la UE (AI Act): categorías de riesgo y obligaciones
- Normas ISO relevantes: 23894 (gestión de riesgos), 42001 (sistemas de gestión de IA), 22989 (terminología), entre otras
- Principios de la OCDE y directrices de UNESCO sobre IA responsable
- Comparativa de enfoques: UE, EE.UU., China, y otros bloques geográficos
- Tendencias globales hacia la gobernanza algorítmica y la interoperabilidad regulatoria

Introducción a las normas ISO I

- ISO 22989: Terminología fundamental para sistemas de IA y su entorno
- ISO 23894: Gestión de riesgos específicos en sistemas de IA
- ISO 42001: Sistema de gestión para el ciclo de vida de sistemas de IA (AI Management System)
- ISO 38507: Gobernanza de la IA en el contexto de la dirección corporativa (complementa ISO 38500)
- ISO 31000: Marco general para la gestión del riesgo aplicable también a proyectos de IA

Introducción a las normas ISO II - Sistema de gestión de IA (ISO/IEC 42001)

- Contexto en la organización (entendiendo a las organizaciones, terceras partes y los sistemas de gestión de la IA)
- Liderazgo
- Politicas
- Roles y Responsabilidades
- Planificación (Evaluación, tratamiento, impacto)
- Soporte (recursos, riesgos, comunicación, documentación)
- Operación (evaluación de riesgos y tratamiento)
- Mejora

Introducción a las normas ISO III - Gobierno de tecnologías disruptivas (ISO/IEC 38507)

- Alcance
- Terminos y Definiciones
- Implicaciones para la gobernanza del uso organizacional de la IA
- Visión general de la IA y de los sistemas de Inteligencia Artificial
- Políticas para abordar el uso de la Inteligencia Artificial

- Gobernabilidad y toma de decisiones organizacionales

Introducción a las normas ISO IV- Gestión del Riesgo en Sistemas de IA (ISO/IEC 23894 y 31000)

- Diseño, implementación y evaluación
- Proceso global de levantamiento y monitorización de riesgos
- Proceso de Reporte
- Objetivos
- Ciclo de vida de la IA

Certificación ISO - AI Management Leader (ISO/IEC 42001)

Certificación ISO - AI Governance Leader (ISO/IEC 38507)

Módulo 4 | Derecho tecnológico
60 horas lectivas

Reglamento de Inteligencia Artificial

- Enfoque basado en el riesgo: Clasificación de sistemas de IA en 4 niveles (riesgo inaceptable, alto, limitado y mínimo)
- Obligaciones para sistemas de alto riesgo: Evaluación de conformidad, documentación técnica, trazabilidad, supervisión humana
- Prohibiciones explícitas: Sistemas que manipulen el comportamiento, puntuación social, vigilancia biométrica en tiempo real sin autorización
- Requisitos para transparencia: Notificación clara al usuario cuando interactúa con sistemas de IA (chatbots, deepfakes, etc.)
- Impacto para empresas: Nuevas obligaciones para desarrolladores, importadores, distribuidores y usuarios de IA en el mercado europeo

Derecho aplicado a la IA I

- Marcos jurídicos de la Inteligencia Artificial en Europa, EEUU, Asia y oriente.
- Responsabilidad asociada a sistemas de Inteligencia 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 la 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 la transformación digital y sostenibilidad I

- Relación entre Fintech y sostenibilidad, y las diferentes áreas de colaboración entre Fintech
- Finanzas sostenibles, perspectiva teórica. Ejemplos prácticos
- Plan de acción de la UE financiación sostenible. Normativa antecedentes y contexto.
- Iniciativas regulatorias derivadas del plan de acción
- Compromiso de la Banca más allá de la regulación
- Crowdfunding Plataformas de financiación participativa
- Euro digital

Derecho aplicado a la transformación digital y sostenibilidad II

- Tecnología blockchain en el sector financiero relacionada con los aspectos ESG
  - Financiación verde, gestión de riesgos e informes:
  - Créditos de CO2:
  - Contabilidad y notificación del impacto de los gases de efecto invernadero (GEI)
  - Certificación ecológica de tokens no fungibles (NFT)
  - Incentivos y recompensas tokenizados

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

Módulo 5 | Riesgos y gobernanza
75 horas lectivas

Ciberseguridad en la IA

- Seguridad técnica
- Ataques adversarios & One pixel Attack
- Data Poisoning
- Pront Injection
- Defensa y resiliencia

Riesgos de modelo asociados con la integración de la IA en las infraestructuras tecnológicas actuales

- Riesgo de sesgo (BIAS)
- Riesgo de opacidad (caja negra), Explicabilidad y Reproducibilidad
- Riesgo de robustez
- Model Drift (deriva del modelo)
- Limitación de propósito
- Impronter Output Handling
- Excessive Agency
- System Propmt Leakage
- Vector & Embedding Weaknesses
- Unbounded Consuption
- Dependencia de terceros

Riesgos asociados a la IA, seguimiento y monitorización I

- Riesgo de Modelo
- Riesgos Operacionales

Riesgos asociados a la IA, seguimiento y monitorización II

- Riesgo de Cumplimiento
- Riesgos Legales
- Riesgos Éticos

Desafíos y Consideraciones en la Implementación de la IA para la Gestión de Riesgos

- Calidad y Disponibilidad de Datos
- Riesgo de Modelo (Incluyendo Explicabilidad y Transparencia)
- Sesgo Algorítmico y de Equidad
- Cumplimiento Regulatorio
- Seguridad de Datos y Privacidad
- Dependencia de Terceros (proveedores)
- Escasez de talento con conocimientos especializados
- Costes de Implementación
- Ritmo de innovación vs capacidad de supervisión

Roles Principales y Relación entre ellos en las Entidades y con el CAIO

- CISO (Chief Information Security Officer)
- DPO (Data Protection Officer)

- CTO (Chief Technology Officer)
- CIO (Chief Information Officer)
- CRO (Chief Risk Officer)

Gestión y Evaluación de Proveedores I

- Marco de Gestión de Terceros aplicable a la IA (TPRM)
- Criterios de homologación, evaluación y monitorización
- Marcos de gobernanza compartida y control de calidad

Gestión y Evaluación de Proveedores II

- Métricas de trazabilidad, seguridad y desempeño
- Supervisión continua
- Respuesta ante incidentes

Gobernanza Dato I

- Rol estratégico del CDO en la IA
- Gobierno del dato: Calidad y Sostenibilidad

Gobernanza Dato II

- Marco legal y regulatorio
- GDPR
- Principios de privacidad
- Derechos digitales

Gobernanza Dato III

- Técnicas avanzadas de protección de datos: anonimización, seudonimización, fedxeral learning, differenctial privacy
- Coordinación DPO, CISO y CAIO
- Transparencia, confianza y comunicación con stakeholders

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

Futuro de la gobernanza de modelos

- Model Context Protocol (MCP) y A2A
- Implicaciones para auditoría
- Explicabilidad y trazabilidad
- Cumplimiento normativo (AI Act, DORA)

Taller riesgos y gobernanza I

- Despliegue de un modelo completo de IA
- Establecimiento de KPIs/KRIs para su monitorización
- Construcción del dashboard de monitorización
- Simulación de un informe para comité de riesgos / comité ético.

Taller riesgos y gobernanza II

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

Módulo 6 | 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 | Servicios cloud y big data
125 horas lectivas

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

Fundamentos de infraestructura para despliegue de IA
- Introducción a GIT
- Introducción a la Terminal
- Python Virtual Enviroments
- Cronjobs
- Variables de Entorno
- Conceptos Básicos de Redes: OSI, puertos, protocolo ip etc.

Plataformas Data
- DataFabric
- SnowFlake
- DataSphere
- Principales arquitecturas Data (datalakes, datos federados, datos virtualizados, datamesh, ...)
- Capas de gobernanza del dato (esquemas, linajes, taxonomía, metadatos)

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

Otras plataformas Cloud
- Introducción general, servicios clave y comparativa con Google Cloud
  - AWS (Amazon)
  - Azure (Microsoft)

Examen certificado profesional BigData engineer
Examen certificado profesional ML Engineer

Módulo 2 | Deep Learning avanzado y generativo

175 horas lectivas

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

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 y análisis de anomalías
- Tipos de anomalías: puntuales, contextuales, colectivas
- Métodos Lineales: PCA, MCD, LMDD, One-class SVM
- Métodos por proximidad: Local Outlier Factor, Histogram-based Outlier Score
- Métodos probabilísticos: Angle-Based Outlier Detection, Stochastic Outlier Selection
- Métodos basados en ensembles: Isolation Forest, Feature Bagging, LSCP, LODA
- Métodos basados en IA: XGBOD (Extreme Boosting Based Outlier Detection), Deep Autoencoders

Graph Neural Networks
- Concepto de independencia
- Independencia condicional
- Geometric Neural Networks

Aprendizaje por refuerzo I
- Procesos de decisión de Markov
- Algoritmos de aprendizaje
- Function approximation
- Q-learning
- Doble Q-learning
- SARSA
- Métodos de búsqueda

Aprendizaje por refuerzo II
- Automated machine learning
- Selección de modelos
- Búsqueda de arquitecturas
- Full pipeline optimization
- Algoritmos basados en políticas
- Actor Critics (A2C, A3C)

Aprendizaje justo (fair learning)
- Métodos de ajuste de modelos mediante aprendizaje justo
- Teoría de la información
- Dependencia usando métodos kernel
- Dependencia usando Gaussianización multivariada

Explainable Artificial Intelligence (XAI) I
- Métodos de ingeniería inversa
- Explicabilidad en machine learning en general
- XAI en deep learning
- Herramientas de XAI

Explainable Artificial Intelligence (XAI) II
- Naturaleza de los algoritmos de XAI
  - Interpretar vs Explicar vs Transparencia ○ Explicabilidad local vs global
  - Explicabilidad específica vs genérica
  - Transparencia de un modelo
- Dificultades del eXplainable Deep Learning (XDL)
- Visualización/Explicabilidad de los datos
- Explicabilidad global
  - Análisis de los componentes de los modelos (redes neuronales, árboles, SVM)
- Explicabilidad local
  - Permutación
  - Reemplazo: LIME (Local Interpretable Model-agnostic Explanations)
- ¿Cómo medir el grado de explicabilidad?

Explainable Artificial Intelligence (XAI) III
- Estrategias de Explicabilidad de Deep Learning
  - Explicabilidad por perturbación
  - Explicabilidad local basada en gradientes
  - Explicabilidad local basada en relevancias: LRP
- Explicabilidad de Redes Recurrentes
  - Problema de vanishing gradient. ¿Por qué afecta a la explicabilidad?
  - Solución al vanishing gradient. Procesamiento de todos los instantes de tiempo.
  - Explicabilidad basada en gradientes y LRP con RNNs

Explainable Artificial Intelligence (XAI) IV
- Transparencia de las Redes Recurrentes
  - ¿Se puede interpretar una RNN como una máquina de estados?
  - ¿Se puede utilizar una RNN como oráculo para inferir máquinas de estados?
- Talleres
  - Ataques adversarios de imágenes a partir de la explicabilidad
  - Filtrado de una señal de audio a partir de la explicabilidad
  - Análisis espacio-temporal de procesamiento de señales biológicas (P300-ERPs) a partir de la explicabilidad

Explainable Artificial Intelligence (XAI) V
- Fundamentos de la inferencia causal
- Técnicas de estimación causal
- ML aplicado
- Razonamiento contractual y modelos estructurales

- Causalidad avanzada y aplicaciones reales

Inferencia causal

- Causalidad vs. predicción
- Datos experimentales vs. observacionalesDAGs
- D-separation, confusores/colisionadores/ mediadores
- Criterio back-door/front-door y notación do(·)
- De la identificación a la estimación
- Práctica guiada: construir y validar un DAG del caso

De la inferencia a Causal AI aplicada

- Estimación moderna y pipeline reproducible
- DoubleML, estimadores doblemente robustos (AIPW)
- ATE/CATE, intervalos y diagnósticos de balance/ positividad
- Implementación con DoWhy
- SCM, intervenciones y contrafactuales
- Algoritmo abduction–action–prediction
- Causal AI en acción: policy/uplift learning, conexiones con RL y aplicaciones con LLMs
- Práctica "end-to-end": diseño de una política y evaluación contrafactual con DoWhy/DoubleML

Taller de detección de brechas estructurales en series temporales

- Definición y tipologías de cambio de régimen (nivel, tendencia, varianza y dependencia)
- Métodos deterministas clásicos (Chow/Quandt-Andrews, CUSUM, Binary Segmentation, PELT)
- ML supervisado (XGBoost y ensembles)
- Deep Learning secuencial (LSTM/Transformers) para detección y anticipación

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

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

LRM - Large Reasoning Models

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

ML Ops y Ciclo de vida del Proyecto

- Introducción al ciclo de vida de modelos de ML (fases, diferencias frente al desarrollo tradicional, actores...)
- Preparación y gestión de datos (Data Ops)
- Entrenamiento
- Despliegue de modelos y automatización del ciclo de vida
- Monitorización, mantenimiento y gobernanza de los modelos

Casos de Negocio

- Identificación, priorización y evaluación de casos de uso
- Éxito de los casos de uso
- Ejemplos de casos de uso
  - Caso de uso, sistema de auditoría
  - BlinkFire Analytics

Taller I - Explainable AI (XAI)

- Cómo seleccionar la técnica de XAI más adecuada según el caso.
- Cómo integrar XAI en el ciclo de vida de modelos ML/ IA.
- SHAP: teoría, tipos de valores (TreeSHAP, KernelSHAP), visualizaciones.
- LIME: funcionamiento, ventajas y limitaciones.
- Partial Dependence Plots y Accumulated Local Effects.
- Ejercicio práctico: comparación de SHAP vs LIME
  - Finanzas: decisiones automatizadas (XAI y cumplimiento).
  - RRHH: IA en selección de personal (XAI y discriminación).
  - Industria: mantenimiento predictivo explicable.

Taller II - Auditoría de un modelo de scoring crediticio (ML explainability + fairness)

- Objetivo: entender cómo evaluar y gobernar modelos de ML con impacto regulatorio y ético directo
- Caso práctico: modelo de clasificación (por ejemplo, XGBoost o Random Forest) que aprueba o rechaza solicitudes de crédito

- Actividades:
  - Evaluación de rendimiento: métricas clásicas + coste de falsos positivos/negativos
  - Análisis de variables sensibles (sexo, edad, origen): detección de sesgos
  - Uso de herramientas de explicabilidad: SHAP/LIME
- Aprendizajes clave:
  - Cómo balancear rendimiento y justicia
  - Qué documentación se exige para cumplir con AI Act o ISO 42001
  - Cómo presentar resultados comprensibles a no técnicos

Módulo 3 | Ciberseguridad y Hacking ético
225 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

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

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: Análisis de 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: Análisis de 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

Módulo 4 | Computación Cuántica
40 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

Módulo 5 | Lanzamiento de tu propia startup
30 horas lectivas

Definición y validación de la idea de negocio
- Desarrollo de una propuesta de valor sólida
- Análisis de la ventaja competitiva ¿es sostenible en el tiempo?
- Definición de necesidades y coherencia del proyecto

Prototipado y validación de producto
- Desarrollo de un producto mínimo viable
- Análisis de la cadena de valor

Desarrollo de una estrategia de entrada al mercado
- Análisis de la competencia
- Establecimiento del precio
- Estrategia de márketing

Financiación y aspectos legales
- Estimación de flujos de caja
- Obtención de financiación
- Aspectos legales del proyecto

Presentación del proyecto a aceleradoras de *startups*

Presentación del proyecto a la asociación de Business Angels

Defensa de TFM I

Defensa de TFM II

ATHENAI
Technological Business School

4

Certificaciones

Podrás obtener hasta ***ocho 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.

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.

Certificación CAIO (Chief Artificial Intelligence Officer)

La certificación de Chief Artificial Intelligence Officer (CAIO), emitida por **AthenAI Technological Business School**, acredita que el estudiante ha adquirido las competencias estratégicas, técnicas y organizativas necesarias para liderar la transformación de las empresas a través de la Inteligencia Artificial.

Esta certificación está diseñada para validar que los profesionales son capaces de:

- Diseñar e impulsar estrategias globales de Inteligencia Artificial en entornos empresariales complejos.
- Coordinar equipos interdisciplinares de datos, tecnología y negocio con un enfoque orientado a resultados.
- Garantizar el cumplimiento ético, normativo y de seguridad en proyectos de IA a gran escala.
- Integrar la IA como un habilitador del negocio, alineando las capacidades técnicas con los objetivos corporativos.

Contenido del Certificado

Liderazgo estratégico en IA

- Gobernanza de datos e Inteligencia Artificial.
- Diseño de estrategias de IA alineadas con el plan de negocio.
- Desarrollo de hojas de ruta para la adopción responsable de IA.

Gestión de tecnología e innovación

- Evaluación y selección de herramientas y proveedores de IA.
- Diseño e implementación de arquitecturas escalables (cloud, híbridas, on-premise).
- Integración de IA en procesos core del negocio.

Riesgos, ética y cumplimiento

- Aplicación de marcos regulatorios internacionales (UE AI Act, ISO/IEC, NIST, etc.).
- Evaluación de riesgos operativos, reputacionales y regulatorios.
- Promoción de una cultura organizativa centrada en la IA ética y sostenible.

Capacidades directivas y visión global

- Comunicación efectiva con el comité de dirección.
- Transformación cultural para entornos data-driven.
- Análisis de impacto, KPIs y retorno de inversión en IA.

Beneficios para los estudiantes

- Reconocimiento institucional: Certificación propia respaldada por AthenAI Technological Business School.
- Perfil profesional único: Acreditación diferencial para liderar la IA en cualquier sector.
- Acceso a una red exclusiva de profesionales, expertos y empresas innovadoras.
- Preparación real para el puesto: Formación aplicada, actualizada y alineada con las necesidades empresariales.
- Diseño, implementación y despliegue de herramientas basadas en IA

Para obtener esta certificación será necesario superar con éxito todas las prácticas del máster, así como superar con éxito el trabajo de fin de máster. La certificación CAIO está incluida en el precio del máster.

Programa de Lanzamiento de tu propia Startup

El Programa de Lanzamiento de Startups está diseñado para estudiantes y emprendedores emergentes que buscan convertir sus ideas innovadoras en negocios reales. A través de un enfoque práctico, los participantes desarrollan las habilidades necesarias para la validación de ideas, la creación de productos mínimos viables, el diseño de estrategias de mercado y la búsqueda de financiación.

Estructura del Programa y Contenido

Definición y Validación de la Idea de Negocio

- Desarrollo de una propuesta de valor sólida.
- Análisis de la sostenibilidad de la ventaja competitiva.
- Identificación de necesidades y evaluación de la coherencia del proyecto.

Prototipado y Validación de Producto

- Creación de un producto mínimo viable (MVP).
- Análisis de la cadena de valor para maximizar la eficiencia operativa.

Desarrollo de una estrategia de Entrada al Mercado

- Análisis exhaustivo de la competencia.
- Determinación del precio óptimo para el producto o servicio.
- Diseño de una estrategia de marketing efectiva.

Financiación y Aspectos Legales

- Estimación de flujos de caja y análisis financiero.
- Estrategias para obtener financiación (inversores, préstamos, subvenciones).
- Aspectos legales necesarios para el emprendimiento.

Presentación de Proyectos a Inversores

- Presentación de propuestas a aceleradoras de startups.
- Presentación de propuestas a asociaciones de Business Angels.

Este programa proporciona un conjunto integral de habilidades para la creación de startups, desde la concepción de ideas hasta la financiación y la entrada en el mercado.

Los estudiantes no sólo obtendrán conocimientos teóricos, sino que desarrollarán competencias prácticas y tendrán la oportunidad de presentar su proyecto a aceleradoras de startups y Business Angels reales.

ATHENAI
Technological Business School

5

Salidas profesionales

Finalizado este Máster, serás ***Chief of Artificial Intelligence Officer***, uno de los perfiles más demandados y mejor pagados, tanto en el sector público, como en el sector privado (finanzas, seguros, salud, energía, telecomunicaciones etc).

Responsable de Inteligencia Artificial – CAIO

Al finalizar el máster, tendrás los conocimientos para asumir el papel de CAIO de una empresa en prácticamente todos los sectores (tecnología, finanzas, salud, educación, gobierno, etc.). Liderarás la estrategia, desarrollo y adopción de la IA a nivel organizacional, salvando la brecha actual entre los avances tecnológicos y la cultura organizativa.

Aunque el máster está diseñado específicamente para preparar a futuros Chief Artificial Intelligence Officers, los conocimientos adquiridos en el máster permiten también acceder, o evolucionar, hacia otros roles Level-C (relacionados con la tecnología, los datos, el cumplimiento normativo y la innovación), aportando una perspectiva innovadora basada en la aplicación de la Inteligencia Artificial.

Otras salidas profesionales

- **CDO – Chief Data Officer / Director de Datos**

Lidera la estrategia de datos de la organización, asegurando su gobernanza, calidad, integración y aprovechamiento en iniciativas de Inteligencia Artificial y analítica avanzada.

- **CRO – Chief Risk Officer / Director de Riesgos**

Evalúa y gestiona los riesgos tecnológicos, legales y éticos vinculados al uso de IA, integrándolos en el marco global de gestión de riesgos corporativos.

- **CTO – Chief Technology Officer / Director de Tecnología**

Supervisa las decisiones tecnológicas estratégicas, incluyendo la adopción de infraestructuras cloud, IA y otras tecnologías emergentes clave para la competitividad empresarial.

- **CIO – Chief Information Officer / Director de Sistemas de Información**

Asegura que los sistemas de información estén alineados con la estrategia empresarial y preparados para integrar soluciones de IA de forma eficiente y escalable.

- **CISO – Chief Information Security Officer / Director de Seguridad de la Información**

Protege los activos digitales de la organización, incorporando la ciberseguridad en entornos de IA y garantizando la gestión segura del ciclo de vida de los datos.

- **CCO – Chief Compliance Officer / Director de Cumplimiento Normativo**

Se responsabiliza del cumplimiento de normativas relacionadas con IA, privacidad de datos, auditoría algorítmica y gobernanza responsable de los sistemas inteligentes.

- **CDO (Digital) – Chief Digital Officer / Director de Transformación Digital**

Lidera procesos de transformación digital impulsados por Inteligencia Artificial, integrando nuevas tecnologías en la propuesta de valor, operaciones y cultura empresarial.

- **AI Compliance and Risk Officer**

Especialista en el diseño e implementación de marcos de cumplimiento y gestión de riesgos específicos para proyectos y sistemas basados en IA.

- **Responsable de Gobernanza de la IA**

Diseña e implementa políticas, procesos y estructuras de gobernanza para asegurar un uso ético, seguro y eficaz de la IA en la organización.

- **Especialista en transformación digital con IA**

Asesora y ejecuta planes de transformación digital donde la IA juega un papel central, desde la optimización de procesos hasta la personalización de productos y servicios.

- **Asesor Estratégico de IA**

Ayuda a organizaciones a identificar oportunidades de negocio mediante IA, definir hojas de ruta tecnológicas y alinear inversiones con objetivos estratégicos.

- **Data & AI Strategist**

Profesional híbrido entre el dato y la Inteligencia Artificial, capaz de conectar insights y algoritmos con decisiones de negocio de alto impacto.

- **Fundador de una startup de IA**

Emprende tu propio proyecto con la Inteligencia Artificial como motor de innovación, apoyándote tanto en los conocimientos, como en la red de contactos adquiridos durante tu paso por la escuela.

Comparativa de perfiles tecnológicos

Contenido	CAIO	CDO	CRO	CTO	CIO	CISO	CCO	Essential Level-C	Top Level-C
Inteligencia Artificial aplicada	✓			✓				✓	✓
Programación y MLOps	✓			✓				✓	✓
Ciencia de Datos y analítica avanzada	✓	✓						✓	✓
Arquitectura tecnológica / sistemas	✓	✓		✓	✓	✓		✓	✓
Cloud y servicios distribuidos	✓	✓		✓	✓	✓		✓	✓
Ciberseguridad técnica y estratégica	✓	✓	✓	✓	✓	✓		✓	✓
Gobernanza de datos		✓			✓	✓			✓
Gestión del riesgo corporativo			✓			✓	✓		✓
Cumplimiento normativo (AI Act, GDPR…)	✓	✓	✓			✓	✓	✓	✓
Ética tecnológica y transparencia	✓	✓	✓			✓	✓	✓	✓
Liderazgo estratégico y transformación	✓	✓	✓	✓	✓	✓	✓	✓	✓
Innovación tecnológica y disrupción	✓			✓				✓	✓
Diseño de producto y experiencia de usuario				✓					✓
Cultura digital y gestión del cambio	✓	✓	✓	✓	✓	✓	✓	✓	✓

Toolbox al finalizar

Inteligencia Artificial

Genéticos Enjambres Lógica Difusa

ML

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

DL

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

Derecho tecnológico aplicado y marcos regulatorios
- Inteligencia Artificial
- Transformación digital y sostenibilidad
- Servicios de plataforma y distribuidos
- Ciberseguridad
- Identidad Digital
- Gobernanza del dato

Gobernanza y Fundamentos Estratégicos
- Estrategia empresarial
- Gestión de proyectos de IA
- Marco de Gobierno de la IA
- Gestión avanzada y gobernanza de los riesgos asociados a la IA

Gestión de riesgos
- Gestión avanzada de riesgos
- Riesgos asociados a la IA
- Cumplimiento y aspectos legales (regulaciones, auditorías, contratos, privacidad de datos, ...)
- Roles principales relacionados con la tecnología y la IA dentro de una entidad
- Gestión y evaluación de proveedores
- Gobernanza del dato

Ciberseguridad
- Fundamentos avanzados de seguridad y ciberseguridad

Lenguaje de programación
Python

Arquitectura en la nube
AWS

Azure

Google Cloud

Contenedores
Docker

Kubernetes

Bases de Datos (DB)
- NoSQL
- SQL
- MongoDB

Big Data
Spark

Creación de APIs
FastAPI

DevOps
CI/CD con GitLab Runners

Desarrollo y despliegue de ETL pipelines
ETL

Conseguirás:

CCSP (ISC2)

CISSP (ISC2)

CompTIA Security+

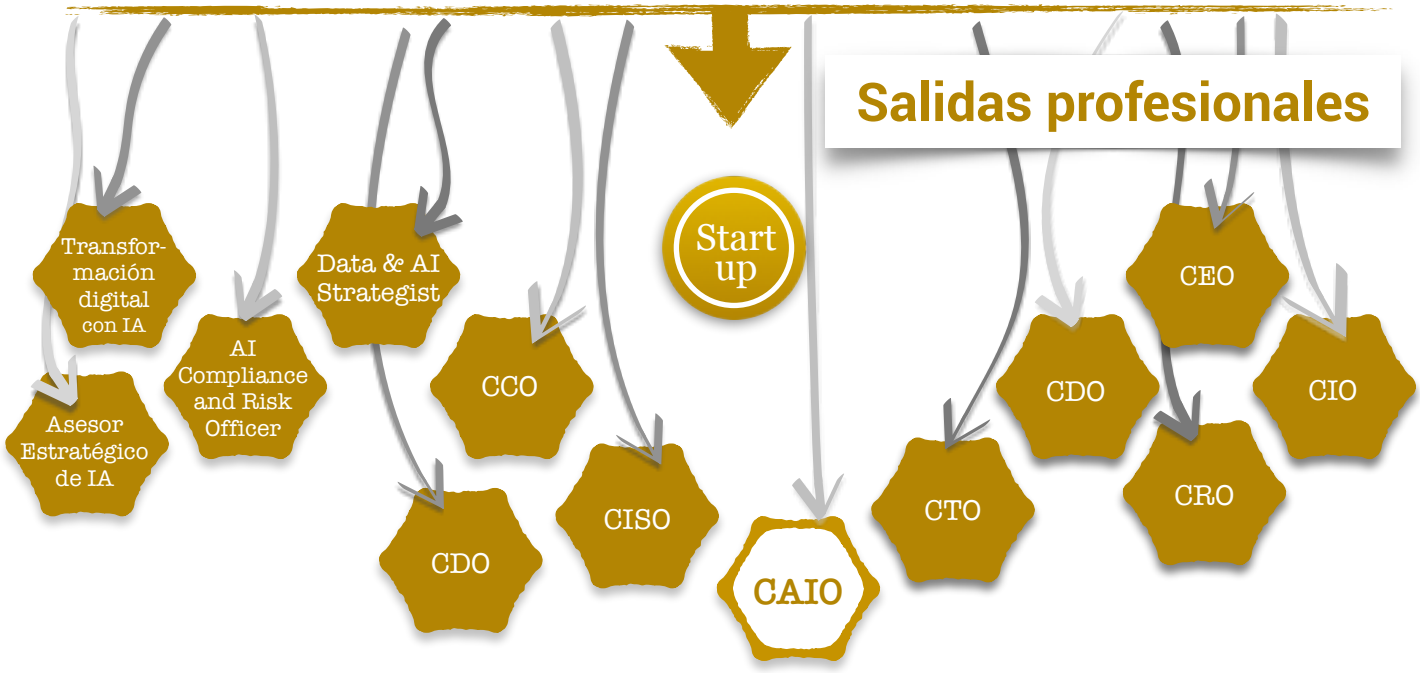
CompTIA CASP+

Google Cloud Certified – Professional Machine Learning Engineer

Google Cloud Certified – Professional Cloud Architect

Google Cloud Certified – Professional Data Engineer

Salidas profesionales



Un programa ÚNICO

El nivel de exigencia del máster, así como la constante actualización de sus contenidos, convierten a los egresados en la ***cantera natural para liderar la transformación digital de las empresas***.

Naturaleza del máster

La mayoría de los másteres se enfocan en un área del conocimiento: másteres en Inteligencia Artificial y machine learning, másteres en ciencias de datos, másteres en IA generativa, MBA con foco en IA o tecnología, másteres en Ética y Gobernanza de IA, másteres en MLOps e ingeniería de IA... pero éste es un máster multidisciplinar que une tecnología, negocio, ética, liderazgo y legalidad. No forma solo un técnico, ni solo un gestor: formamos directivos integrales con conocimientos profundos en IA.

Esta orientación profesional es una de las principales diferencias con cualquier otro máster. No buscamos cubrir un temario académico para otorgar un título, sino identificar a quién hay que contratar.

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

- Finalizado cada bloque de conocimiento, los alumnos recibirán el enunciado de una práctica desafiante.
- Tendrán 3 semanas para completar y entregar dichas prácticas.
- Los alumnos contarán con los apuntes, internet, foros, tutores, la grabación de las clases, acceso a cualquier herramienta en producción basada en IA...
- Deberán investigar y probar muchas opciones diferentes (ensayo-error) hasta conseguir resolver cada ejercicio.
- Este aprendizaje se les quedará grabado para toda la vida.
- 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.

En el máster no se estudia únicamente Inteligencia Artificial

Para preparar adecuadamente a un CAIO, este máster le ofrece no sólo lo conocimientos tecnológicos que requiere un especialista en Inteligencia Artificial aplicada, sino una visión global de la integración de la IA en las empresas y cómo se puede alinear la IA con sus objetivos. Esto incluye, entre otras áreas:

- Estrategia de negocio y liderazgo.
- Ética, regulación y responsabilidad
- Gobernanza de datos y arquitectura organizativa

En el máster no se estudia únicamente Deep Learning

Este máster ofrece una visión de diferentes ramas de la Inteligencia Artificial ahondando en aquellas que más se están utilizado actualmente en la industria:

- Algoritmos Genéticos
- Algoritmos Enjambre
- Lógica Difusa
- Machine Learning y Deep Learning

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.

Programa certificado por Google

Parte del profesorado del módulo de Inteligencia Artificial estará integrado por ingenieros de Google.

Durante este módulo, los alumnos recibirán la formación necesaria para obtener la certificación de **Cloud Architect, BigData Engineer, Machine Learning Engineer**. Dicho examen lo realizarán desde la propia plataforma de Google, entidad responsable de certificar los conocimientos de los alumnos.

Empleabilidad

El perfil del CAIO destaca por un conocimiento técnico sólido, capacidad estratégica, liderazgo, gestión del cambio, dominio ético y legal.

Con ello se consigue un rol emergente y poco estandarizado, capaz de diferenciarse del resto de directivos. Cada vez hay más necesidad de CAIOs realmente preparados, por lo que este máster es una gran oportunidad para dar un salto en tu carrera.

Los factores que más están influyendo en este auge son:

- La inversión creciente de las empresas en Inteligencia Artificial, que hace que necesiten de este perfil técnico-estratégico para si integración.
- La presión regulatoria, que requiere que las empresas cuenten con gobernanza de IA y aseguren el cumplimiento normativo, la transparencia y el uso ético de la IA.
- La complejidad de los sistemas de IA, que requieren un liderazgo técnico, pero con visión transversal.

El nivel de exigencia del máster, así como la constante actualización de sus contenidos, convierten a los egresados en la cantera natural para liderar la transformación digital de las 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 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 de adquisición, por lo que es importante actualizarlos con recurrencia.

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

ATHENAI
Technological Business School

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
	**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	- 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**
	**Gonzalo Navarro Ruiz**	Derecho	- Licenciado en Derecho - Licenciado en Administración de Empresas - Máster en Asesoría Jurídica de Empresa (1º de promoción) - Doctorado en Derecho Societario-Mercado de Valores (Summa cum laude por unanimidad) - Executive Master of Business Administration (EMBA)	Head of Financial Regulation **ONTIER**
	**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**
	**Jesús Mardomingo**	Derecho	- Licenciado en derecho	Socio. Partner **Dentons**
	**Jose Antonio Esteban Sánchez**	Big Data	- Ingeniero técnico de sistemas	Chief Executive Officer (CEO) **IronIA** Gestora de fondos de inversión especializada en IA
	**Jose Zamora**	Inteligencia Artificial + Big Data	- 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**
	**Marcos Aza**	Inteligencia Artificial	- Ingeniero Industrial - Doctor en Finanzas - Responsable de la aplicación de la Inteligencia Artificial al trading algorítmico	Senior Investment Manager **Santander Asset Management**
	**Miguel García Cordo**	Inteligencia Artificial **Dirección académica**	- Máster en Inteligencia Artificial Aplicada a los Mercados Financieros (mIAX) - Máster en Inteligencia Artificial (Instituto de Inteligencia Artificial) - Certificado en la ISO 42001 AI Management Leader - Certificado en la ISO 38507 AI Governance Leader	Chief Risk Officer (CRO) **Inversis**
	**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**
	**Paula Ortiz López**	Derecho	- Master Derecho de las Telecomunicaciones y Tecnologías de la Información - MBA - Máster en Publicidad y Comunicación Digital Licenciada en Derecho	Co-Fundadora & CEO **TheLegal.School**
	**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**

Profesor		Especialidad	Formación	Puesto actual
	**Rafael Sánchez**	Inteligencia Artificial + Big Data	- Licenciado en telecomunicaciones - Doctor en ingeniería y telecomunicaciones	Manager, Generative AI / ML, Southern Europe and Middle East **Google**
	**Raquel Hernández Falcón**	Inteligencia Artificial + Finanzas **Dirección académica**	- Grado en Matemáticas, Estadística e Investigación - Máster en Inteligencia Artificial Aplicada a los Mercados Financieros (mIAX) - Máster en Finanzas Cuantitativas	Trader de crédito **CecaBank**
	**Valero Laparra Pérez-Muelas**	Inteligencia Artificial	- Licenciado en telecomunicaciones - Graduado en matemáticas - Doctorado en filosofía - Doctorado en Inteligencia Artificial por la universidad de New York	Profesor e Investigador **Universidad de Valencia**

ATHENAI
Technological Business School

8

Información general

Información General

Duración

Programa completo equivalente a **127 ECTS**

Level C 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 Level C

- Equivalente a 73 ECTS
- 610 horas lectivas
- 1.830 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

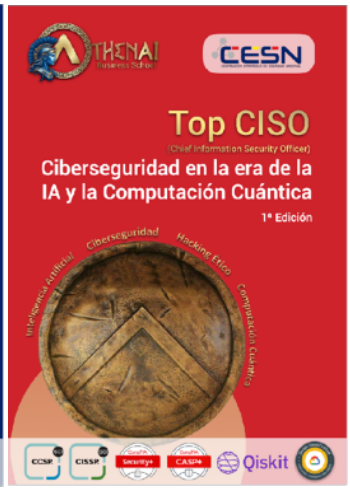
El precio del programa **Level C Essential** es de 11.000 €

El precio del programa **Top Level C** es de 15.000 €

El precio del **programa completo** es de 26.000 €

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 Level-C*** cuyo precio es de **26.000€**. 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 CAIO del mundo. Su propósito era enseñar a combinar Inteligencia Artificial Avanzada y gobierno del dato para liderar los departamentos de IA.

El nombre oficial del Máster era:

"Emerging Tech & Digital Executive Leadership".

Los alumnos lo conocían como…

Top Level-C