AthenAI
Institute of Technology

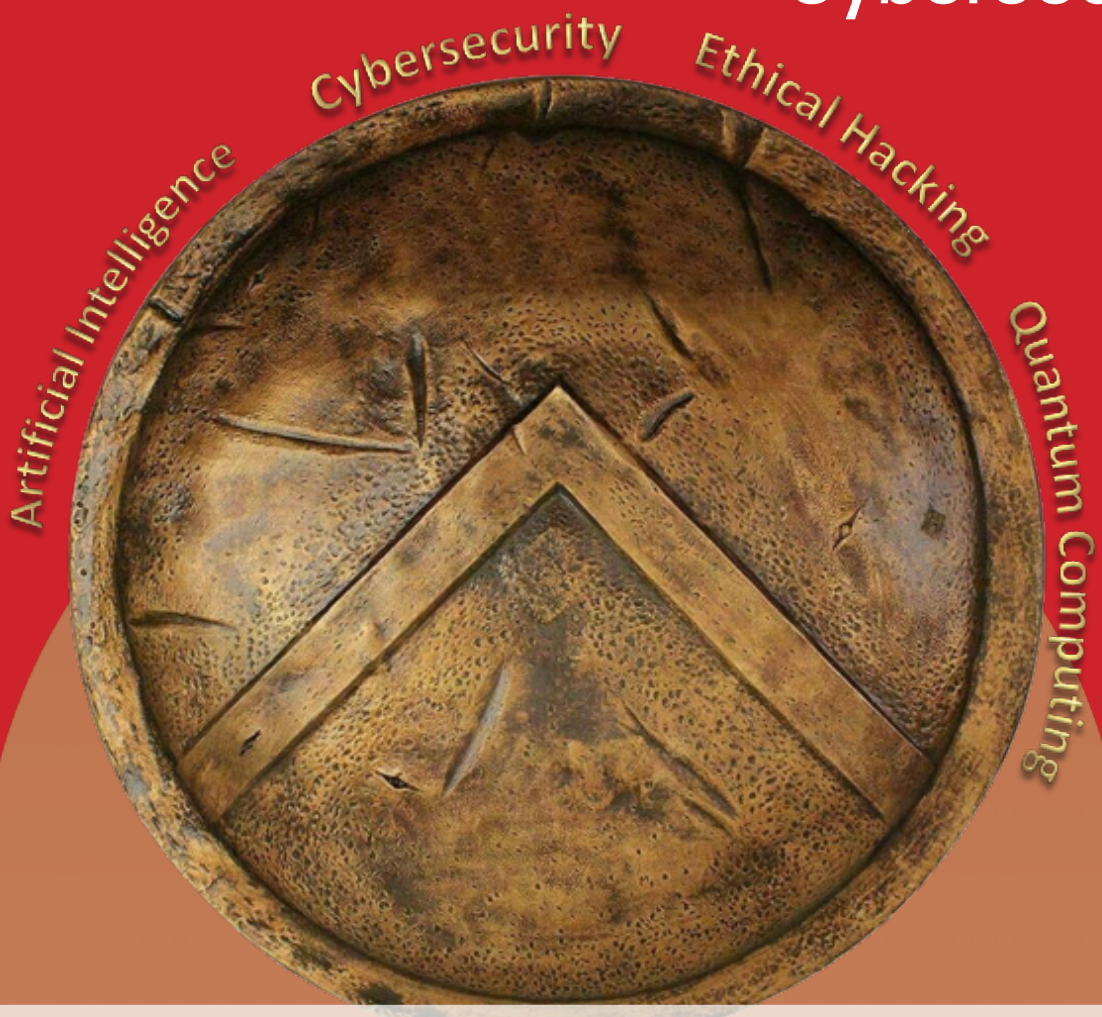
Top CISO

(Chief Information Security Officer)

Essential → Top

Cybersecurity in the Era of AI & Quantum Computing

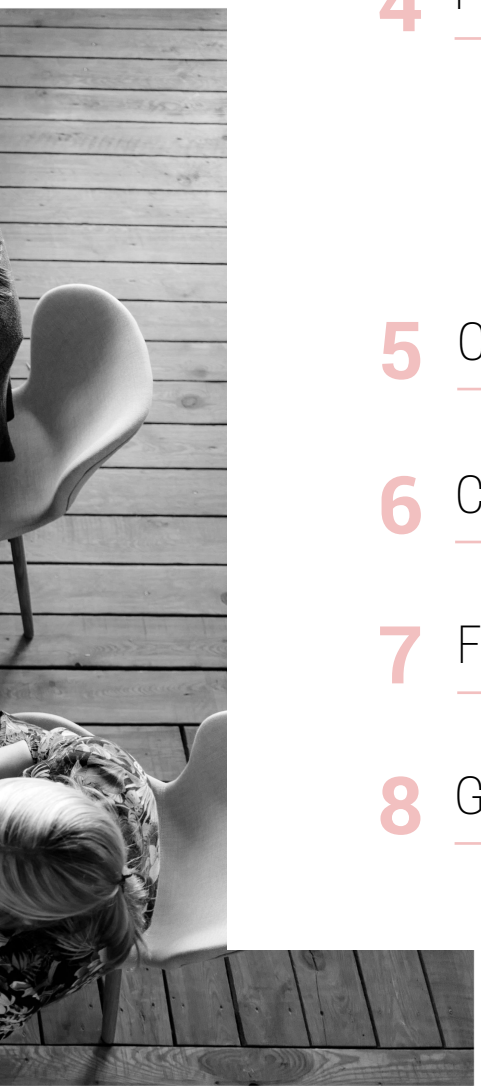
1st Edition



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

AthenAI

Contents



1 AthenAI Institute of Technology 4

2 Our platform 11

3 A UNIQUE Program 15

4 Program Structure 23

Year 1 ≈ Essential 26

Year 2 ≈ Top 32

5 Certifications 40

6 Career Opportunities 49

7 Faculty of Experts and Instructors 53

8 General Information 56

AthenAI

1

AthenAI Institute of Technology

A school for those who truly ***want to learn*** and are ***willing to put in the effort.***

Why study at AthenAI?

AthenAI is a School with an international presence, but it is NOT a school for everyone.

"AthenAI is the school for those who have a true desire to learn and the courage to take on real challenges."

A school for those who are not seeking degrees, but transcendence.

In a context saturated with quick formulas and superficial education, AthenAI was born with the vocation of being a knowledge and technology boutique...

- A **selective, demanding institution, fully committed** to the major challenges of the present and the future.
- A **school of technological excellence** aimed at those seeking **deep, rigorous, and authentic learning**.
- Aimed at **students willing to face real challenges** and walk a path **full of obstacles** in order to achieve transformative learning.
- Where **there is no place for those seeking shortcuts or quick solutions** empty of substance.
- Where **we train leaders who leave a lasting mark** through knowledge, effort, and a genuine commitment to their own development and the world around them.

Where failure is a real possibility

We believe that true learning involves taking risks, stepping out of one's comfort zone, and facing the real possibility of failure, which is why—**unlike other schools—failing here is possible**.

Because mediocrity is born when there are no consequences, at AthenAI we believe that those **who aspire to lead must face the challenge of failure before achieving success**.

"Enrollment means having an opportunity to surpass the program. Not the guarantee of doing so."

Our fundamental pillars: Knowledge, Reputation, and Purpose

We are committed to **high-impact training**, based on **challenging projects** and a **network of strategic contacts that generate real opportunities**. Because those who choose our school do not want to follow the traditional path—they come to us to:

- Reinvent themselves
- Launch their own start-up
- Build the next unicorn
- Become a Forbes cover story

All of this is possible thanks to the three pillars that sustain our educational model: **Knowledge, Reputation,** and **Purpose**.

Pillar 1. Knowledge

Excellence of the faculty

It is **our most valuable asset**, which is why we devote special time and attention to its rigorous selection process. Each professor has been carefully chosen based on three key criteria:

- Their deep knowledge in the area they teach.
- Their ability to transmit all that knowledge to students.
- Their real-world experience in company projects.

This approach ensures high-level training, connected to professional reality and designed to deliver transformative, high-impact learning.

Personalized Tutorial Support

Our programs are designed to provide high-performance training, in which students continually apply the knowledge acquired in practical situations. For this reason, **tutorial support is an essential part of our pedagogical approach**.

Students will have access to our exclusive platform, where they will find all relevant documentation, practical exercises, and a forum where they can raise their questions and concerns. Additionally, t**hey will be able to communicate directly with all faculty members** via email and schedule tutorials flexibly. They will also **have access to the mobile phone of the Academic Director**, allowing them to resolve any urgent matter immediately.

Practical activities are designed to represent a real challenge for students. Therefore, the teaching staff maintains **constant contact with each student, evaluating their progress**. If a decline in academic performance is observed, we meet personally with the student to identify the cause—whether it is lack of study or any other factor affecting their progress.

Each student will have an assigned tutor who will accompany and guide them throughout the entire program, ensuring continuous learning and personalized support.

Constant content updates

Unlike other business schools, **updating our programs** is not a promise—it is a **fundamental principle**.
Each new edition, we thoroughly review and adapt the entire program to incorporate the latest trends, the most relevant technological advances, and the current challenges of the sector.

We rely on the direct participation of key players from major technology companies, who **share with our students the latest published papers** (Google, Microsoft, Meta, Amazon, etc.). This ensures that the content of each edition is unique, fully updated, and aligned with the real state of the market.

Programs certified by the main technology entities

Our programs are designed so that students, in addition to acquiring cutting-edge knowledge, can **obtain the most recognized national and international certifications**.

Immersive and practical methodology

"Our training is not limited to transmitting knowledge:
Here, it is lived, practiced, and demonstrated."

Learning means evolving, which is why students immerse themselves from day one in an **engaging experience** where they "learn with their hands":

- They **attend practical, dynamic, and rigorous classes** that combine essential theory with practical exercises and challenges of increasing difficulty.
- They must **complete a practical assignment at the end of each knowledge block** (there is no theoretical exam), designed to challenge even the most advanced profiles. These assignments **simulate real professional problems and environments**, ensuring that students not only understand the concepts, but test their ability to apply what they learn in concrete situations they will face in their future careers.
- They will have **3 weeks to complete and submit these assignments**, researching and testing different approaches until they manage to solve each exercise. This type of learning stays with them for life, unlike inefficient theoretical exams.
- They must have a **passing average grade (5)** across all assignments in order to present the Final Master's Project, which will consist of **designing a financial service using AI and Big Data**, to be defended before a panel.
- They always have access to the **same tools they will use in their professional life**: notes, the internet, forums, tutors, class recordings, access to ChatGPT, etc.
- They **develop and deploy services in production**, because theory is useless if it is not put into practice. They have access to a community designed to generate high-performance teams capable of developing their ideas and bringing them to the market.
- They **certify, compare, and evolve** their knowledge and skills.
- They **collaborate and compete with other students** in a safe and stimulating environment.
- They build a **high-value network**, sharing experiences with classmates who will become strategic contacts in their career evolution… and lifelong friends.
- They make **decisions with real impact on their trajectory and reputation** within the community: grades matter during training, but reputation will matter throughout their life.

Pillar 2. Reputation

Reputation and ethics as a measure of prestige

A person may be an excellent student but lack ethics, which is why it is crucial that knowledge and reputation are properly differentiated and valued independently.

Reputation must be closely linked to the participant's behavior—toward their peers and toward the school. It is not only about what they know, but how they act and **how they contribute to the academic and professional environment**.

Where your profile speaks for you

Every action, achievement, completed assignment, and challenge overcome by the student is **100% real and accessible to all participants**, as it is recorded on their **public profile**.

This profile is **based on the student's merits, competencies, and ethics**, **previously verified by the school**, so it faithfully reflects their evolution and becomes a professional presentation card—inside and outside the community.

"You will know the strengths and weaknesses of other participants…
but they will also know yours."

In each student's profile, **you can consult their level of knowledge, their reputation, and the certifications** obtained. Additionally, **knowledge will reflect the year in which it was acquired**, so constant updating will be essential.

This approach turns the AthenAI experience into one that is:

- **Transparent** ➪ Results are visible and authentic, based on verified merits and competencies.
- **Transformative** ➪ It accelerates skill acquisition and maintains student commitment from day one until graduation.
- **Human and connected** ➪ It enables an environment of transparent and authentic interactions, creating professional and personal bonds that accompany the student throughout life.

Content updates for graduates

"An education that does not end with the last class…"

Given the accelerated pace of obsolescence in many areas of study within our master's programs, we offer our graduates ongoing access to continuous, relevant updates of the content they studied.

Our *alumni* are natural ambassadors of our programs. Their professional success and satisfaction with the training received strengthen the reputation of the master's program and attract new students.

Once **a master's is completed, grades lose importance**; what truly matters is **reputation, which must continue to be visible and evolving**. Reputation will become **a currency of value for professional growth**, allowing graduates to obtain:

- Discounts on future training and master programs.
- Attendance at international conferences.
- Free content updates.

Factors that influence reputation

- Contributing to the learning of others: responding to student questions in the school forums, helping create an environment of collaboration and mutual support.
- Publishing research or papers together with the school, sharing your knowledge with the academic and professional community.
- Actively participating in school competitions, demonstrating your ability and commitment in practical and challenging contexts.
- Sharing your personal experience on social media, posting videos and testimonials about your journey in the school, inspiring others and positioning yourself as a reference.
- Developing innovative projects and services in collaboration with the school, providing concrete solutions that benefit the community.
- Attracting new students, recommending the school to future candidates and acting as a brand ambassador.
- Collaborating in school events and activities, participating in conferences, seminars, or mentoring sessions that reinforce your role as a leader within the community.

Factors that influence ethics

- Negatively affecting the image of the school, whether through destructive attitudes, malicious comments, or actions that harm its prestige.
- Maintaining unethical or violent behaviors, such as dishonest practices, unnecessary conflicts, or attitudes that compromise personal or institutional integrity.
- Ignoring community rules, violating academic, ethical, or behavioral policies that govern the school.
- Discrediting peers or community members, generating unjustified conflicts and contributing to a toxic environment.
- Showing disinterest or abandoning commitments, leaving projects or tasks unfinished and harming collective work.

Pillar 3. Purpose

Improving employability and working conditions

The level of rigor in our programs, along with the constant updating of their content, turns our graduates into an **exceptional talent pool, highly sought after** for specific positions at high-responsibility levels (C-Level) or in technological or cybersecurity laboratories, both in the public and private sectors.

Thanks to our close collaboration with these laboratories, students **can work on real projects and participate in strategic challenges** proposed by leading institutions, significantly **increasing the job placement opportunities of our graduates**.

"Our objective is to ensure that the employability of our graduates, nationally and internationally, is close to 100% in relevant positions."

Creating AI experts

Most programs seek to create advanced AI users ➪ A user depends on third-party software.

Our objective is to create AI experts ➪ An expert is capable of creating their own AI software, from design to production deployment, and adapting it to solve any task they undertake.

"Our goal is to teach how to develop AI, not just how to use AI."

A school with a soul

AthenAI was born from the mind of Zeus, combining **knowledge, arts, justice, and strategy**. Its name not only evokes wisdom, but also determination and character.

Our school was founded with a clear, shared purpose: **to inspire our students to transcend the personal and create real impact in the world**...

"Build something you believe in."

It is not only about studying, but creating.

It is not about working, but leading.

It is not only about teaching, but transforming the student into their best version.

It is about separating leaders from those who are not.

Here begins your story

Welcome to AthenAI

AthenAI

2

Our platform

Much more than a virtual classroom: a living digital ecosystem, designed to drive learning, collaboration, and continuous professional growth, beyond the classroom and throughout the entire journey of our students.

The perfect ecosystem for unlimited education

We transform the educational experience into a dynamic, demanding, deeply realistic, and future-oriented environment that **maintains the motivation and focus of our students**.

Our methodology is not only advanced, rigorous, and challenging. We ensure that **each student evolves within an ecosystem meticulously designed for success**:

"When learning becomes an immersive experience,
knowledge turns into action and results become tangible."

Our educational platform has been created as a **constantly expanding ecosystem, where** ideas come to life and where **every interaction connects you with new opportunities**: learning, sharing, collaborating, competing, innovating, growing, projecting yourself professionally…

It is not just another virtual classroom. It is a living digital environment that provides the necessary tools to **maximize learning and students' professional development, accompanying them throughout their entire journey** (as students and as active professionals), allowing them to continue growing long after they have completed their training and to belong to a global community that never stops evolving.

1. The School: The academic core of the ecosystem

Within the *School* space, students have access to all the tools necessary **to manage and enhance their learning**:

- **To consult their progress in the programs** in which they are enrolled, as well as in those already completed. They will also be able to view the percentage of credits that can be validated for programs in which they are not enrolled.
- To access live online classes, recordings of completed sessions, consult the session calendar, review their grades, submit assignments, request tutorials with their professors…
- To progress flexibly in their education, being able **to enroll in new programs** and use their accumulated reputation as a currency to obtain academic discounts and benefits.
- Graduates will be able to access subsequent updates to the materials (notes, exercises, and videos from the latest editions) through a small annual fee. In addition, they will be able to **recertify in specific areas of knowledge** to keep their professional profile up to date and to demonstrate the validity and evolution of their competencies.

2. Community: An exclusive network, unique of its kind

The *Community* **is the heart of the ecosystem**, **a selective and exclusive club** inspired by international institutions of excellence such as **Mensa** or **Forbes**, where access is restricted and standards of excellence are exceptionally high.

Students, mentors, and graduates interact within **a living, dynamic, and transparent network**, generating synergies, opportunities, and challenges. A space where learning is expanded through collaboration and collective intelligence, where members can:

- **Connect with students and graduates from any program**, share experiences, resolve questions, or propose projects.
- **Participate in debates, collaborate on projects, answer questions** from other peers, or r**equest a direct meeting** with any member of the network.

- **Consult any profile** 100% verified by the School, guaranteeing the authenticity of shared knowledge and fostering an environment of trust and prestige.
- **Access reputation and knowledge-area rankings**, identify the top profiles in each field, and discover how to improve their positioning within the community, stimulating healthy and enriching competition.
- **Increase their reputation with every valuable** contribution they make to the community, expanding their training opportunities, collaboration possibilities, and professional visibility.
- **Build solid and long-lasting relationships** that will impact their prestige and professional and personal development.

3. Competitions: Learning turned into challenge

Competitions allow students **to apply acquired knowledge in real and stimulating environments**, challenging them to overcome problems in areas as diverse as financial markets, cybersecurity, law, or climate prediction, as well as new topics proposed by students or partner companies.

Each participant **may compete individually or join a team**, lead proposals, or even **create their own competition**, under the academic supervision of the School. It is another way to demonstrate creativity, talent, and leadership ability to the community and to partner companies, gaining reputation in the process.

4. Library: Open, shared, and validated knowledge

The *Library* is a space where knowledge is democratized. A living collective repository, constantly growing, offering **access to a wide collection of academic materials**: notes, summaries, exercises, practice examples, papers, videos, and resources created by both professors and students.

Each validated resource enriches and supports the community, **contributing to the reputation of the contributor**.

Here, learning is not limited to classes: it is expanded through the ideas, curiosity, and generosity of the entire academic community.

5. SOFIA: The intelligence of talent

SofIA is the space reserved for **top-of-the-class students and program directors**.

Its mission is to identify and channel exceptional talent toward **high-impact strategic projects**.

An exclusive environment where the brightest minds connect with the **most innovative and ambitious opportunities**.

6. LARA: Where ideas become companies

Our *start-up accelerator* allows graduates to present innovative projects and **access mentorship, regulatory sandboxes, and investment opportunities (Business Angels)**.

Through our network of **Business Archangels**, in addition to investment, projects receive expert guidance, real involvement, and hands-on support to launch their initiatives into the market

7. SFINGE: Collaboration without borders

Sfinge was the first electronic financial services company in Spain and the technological origin of our School, representing one of the most innovative spaces within the ecosystem.

It enables the **creation of multidisciplinary and international teams** capable of developing projects and Master's Final Projects collaboratively, without geographical barriers.

Thanks to advanced search tools, students can identify peers with complementary profiles and form high-performance international teams operating 24 hours a day.

They will be able to build projects that, once consolidated, **can be submitted to the LARA acceleration program to take them to the next level**.

8. Job Board: Connecting talent with opportunity

The *Job Board* is designed to **enhance employability and boost professional projection**. It represents the meeting point between the talent trained at the School and companies seeking to incorporate highly qualified profiles.

Graduates of a Top program **may apply for exclusive job offers** or even **create their own positions** if their company is looking to recruit talent trained at the School.

Partner companies **may request knowledge assessments or certifications verified by the School**.

9. Strategy Games: Learning by playing

Our ecosystem incorporates a recreational section of *Strategy Games*, **inspired by ancient civilizations** (Egyptians, Vikings, Romans, Celts…), fostering decision-making, strategic thinking, and global tactical vision.

Students **may compete against AI or challenge other peers**, striving to climb the **School ranking** while developing key skills for leadership and management.

10. An ecosystem that evolves with its students

Our ecosystem is a network that grows and transforms alongside its students, accompanying them throughout their entire academic and professional lives.

A digital environment that **connects knowledge, innovation, opportunities, and a global community** to drive talent, collaboration, and success.

"Here, learning does not end when a master's degree finishes:
it becomes a way of life."

AthenAI

A UNIQUE Program

We differentiate ourselves from the rest of cybersecurity programs for ***multiple reasons***, which make it a truly ***UNIQUE*** master's degree. Lead a new generation in cybersecurity systems through ***AI*** and ***Quantum Computing***.

Top CISO: : Two master's degrees that make up the most complete and demanding program in the world

Top CISO: The Elite in Cybersecurity, Artificial Intelligence and Quantum Computing

Top CISO is not just a training program; it is a maximum-level intellectual challenge designed for those who aspire to lead the future of cybersecurity in the era of Artificial Intelligence and Quantum Computing. With a structure that is unique in the world, it combines academic excellence, training intensity and international recognition, positioning itself as the highest standard in advanced education.

By undertaking this program, the student may obtain two master's degrees:

- **CISO Essential**: 450 teaching hours, equivalent to 54 ECTS credits (first academic year).
- **Top CISO**: 765 teaching hours, equivalent to 79 ECTS credits (second academic year).

In addition, the program **incorporates 8 top-tier official certifications**, awarded by the leading entities in each discipline

CISO Essential Certifications:

- Security+ D5 Certification (CompTIA Security+).
- CASP+ D5 Certification (CompTIA Advanced Security Practitioner).
- CISSP D1 Certification (Certified Information Systems Security Professional).
- CCSP D5 Certification (Certified Cloud Security Professional).
- Professional Cloud Architect (PCA), issued by Google.

Top CISO Certifications:

- Quantum Computing Developer Qiskit 2, issued by IBM.
- Professional Data Engineer (PDE), issued by Google.
- Professional Machine Learning Engineer (PMLE), issued by Google.

Students may choose to undertake only the ***CISO Essential*** program, one of the most complete and demanding master's degrees available on the market, capable of transforming the student into a highly competitive and distinctive professional profile.

Only those who seek to transcend and become true global benchmarks will take on the challenge of ***Top CISO***. This comprehensive program requires having previously completed the Essential and represents the summit of education in Cybersecurity, Quantum Computing and Applied Artificial Intelligence.

Top CISO is not studied: ***IT IS CONQUERED.***

Nature of the Master's Degree

This program was created as a direct response to an **urgent need in the business sector**: the lack of experts with advanced, in-depth and certified knowledge in: Programming, Cybersecurity, Technology Law, Artificial Intelligence, Blockchain, Quantum Computing, Cloud Services & Big Data.

This master's degree positions itself as a **strategic pathway to train the new CISOs** (Chief Information Security Officers), one of the **most demanded, scarce and best-remunerated profiles**, both in the financial sector, in critical infrastructures and in the Ministry of Defence.

The orientation of this program is not academic, but entirely **professional, applied and strategic**, equipping students with the **most advanced tools, skills and knowledge on the market** — the same ones they will subsequently use in their professional careers. We work with real data, practical cases and professional development environments drawn from the best cybersecurity laboratories in the industry.

Most cybersecurity master's degrees are merely academic. They prepare users of security software, operational profiles that execute predefined protocols and use existing tools. **We train architects of advanced solutions**, capable of integrating artificial intelligence, quantum computing and forensic analysis into real systems. **Experts capable of defending critical infrastructures, designing and developing new cyberdefense tools and standards, and leading the transition toward secure environments in the face of quantum computing**. Professionals who do not react to a threat, but **anticipate future cyberattacks and threats** that we do not even yet imagine to exist.

Objective

The **objective on the part of the school** is to honor the excellence of the institution by offering students the best program in the world in new technologies applied to cybersecurity.

The objective of undertaking the master's degree **on the part of the students** is usually one of the following three:

- To make a **qualitative and quantitative leap, in salary** terms, compared to their previous situation.
- **To avoid technological obsolescence** while already having a high salary.
- **To enter the labor market with clearly distinctive training**.

Admission Profiles

The master's degree is designed to train professionals and students from different backgrounds, all of them with a common denominator: the desire to become experts in advanced cybersecurity, with real competencies in Artificial Intelligence, Blockchain and Quantum Computing.

a) Technical Profile (computer scientists, engineers, physicists, mathematicians…)

If you come from a technical degree such as computer engineering, telecommunications, physics or mathematics, you are likely to have a good foundation in programming, calculus and systems. However, it is likely that you have not gone in depth into:

- International cybersecurity regulations.
- Advanced offensive and defensive cyberdefense techniques.
- Artificial intelligence applied to threat detection.
- Quantum security, quantum computing and blockchain.

This master's degree is for you if you want to lead the development of secure solutions in complex environments (cloud, IoT, regulated environments), with a comprehensive and realistic vision of the business ecosystem.

b) Financial, Legal or Audit Profile

If you come from the world of audit, compliance, finance, business management or law, you probably have solid regulatory and organizational knowledge, but limited training in advanced technology, technical cybersecurity and applied AI.

This master's degree is for you if you want to:

- Technically understand the risks and controls that affect your sector.
- Speak the same language as technical and digital defense teams.
- Lead secure transformation in sectors such as banking, insurance companies or large law firms.

c) Operational or Institutional Profile (critical infrastructures, State bodies, Defence…)

If you work in a critical infrastructure, in the Ministry of Defence, Interior or essential services, you probably already have experience in incident management, risk analysis or highly regulated environments. However, it is common that you have not had access to:

- Next-generation offensive/defensive tools.
- Applications of generative AI and machine learning in defense.
- Development of quantum algorithms and advanced cryptographic security.

This master's degree will give you access to knowledge reserved for the most advanced cyberintelligence laboratories in the world and will position you to design and execute critical security projects at a national and international level.

The master's program has been carefully designed to level students' competencies in the first modules, ensuring that all profiles reach a common foundation in programming, security, AI and quantum fundamentals.

Required Prior Knowledge

To enroll in this master's degree, participants **are not required** to have a prior t**echnical and conceptual foundation**, but a commitment and a **minimum dedication of 4 hours of study per day** will be indispensable.

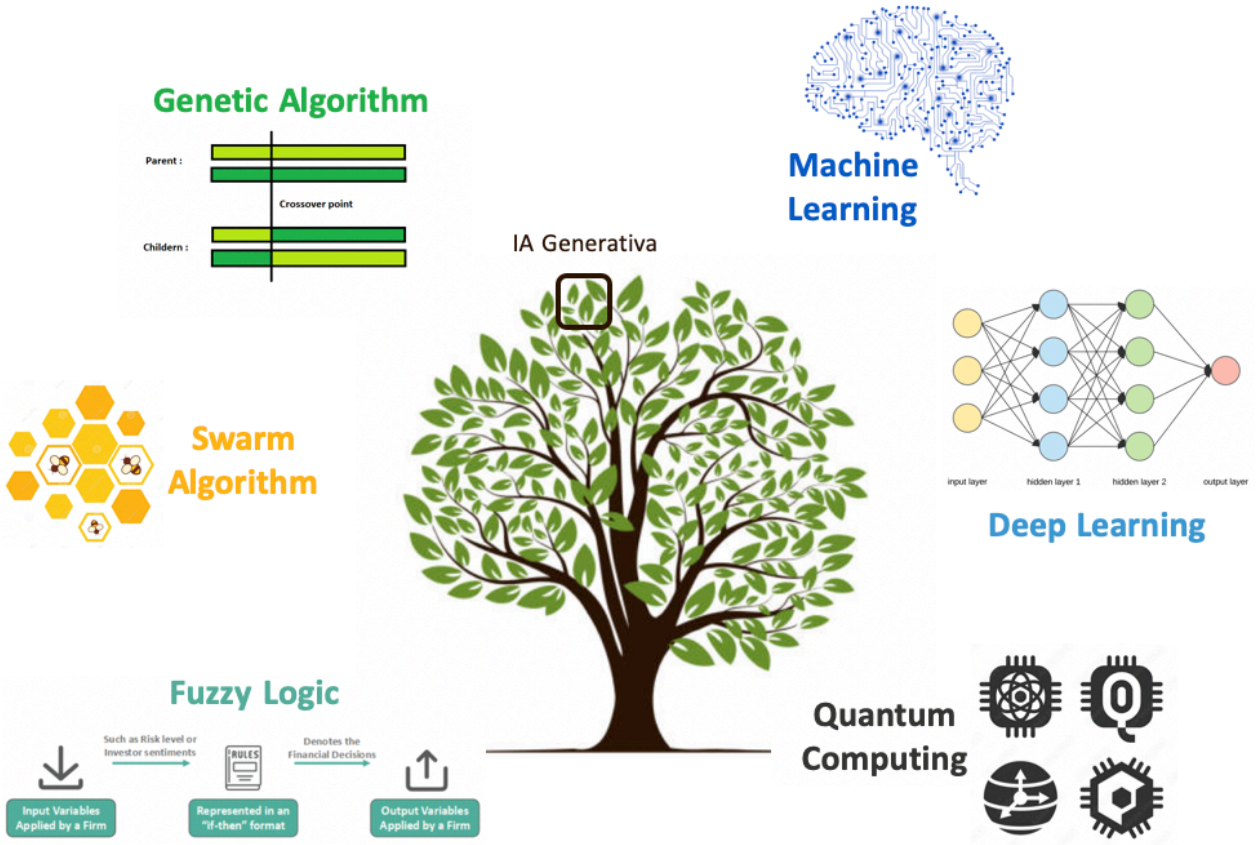
Throughout the program, the student **will develop the skills and acquire the necessary knowledge** in Programming, Cybersecurity, Advanced Artificial Intelligence, Blockchain, Quantum Computing, Big Data and Cloud Services.

In this master's degree, Deep Learning is not the only focus

There are 5 branches of Artificial Intelligence:

- Genetic Algorithms
- Swarm Algorithms
- Fuzzy Logic
- Machine Learning and Deep Learning
- Hybrid Quantum Models

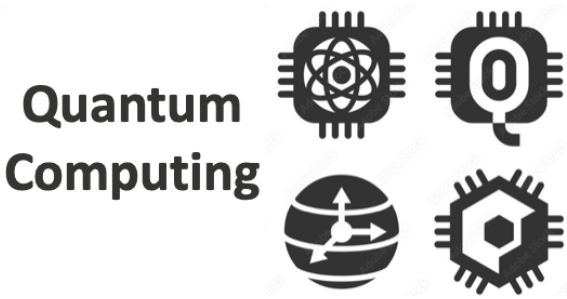
This master's program is the only one in existence where all five branches of Artificial Intelligence are studied in depth, exploring each concept and explaining what is currently being used in the industry.



Artificial Intelligence is not only Generative

The future undoubtedly lies in hybrid quantum AI models and their application to financial markets. In this master's degree, we delve deeply into these models and their application to finance.

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



Access to real quantum computers

Globally, the vast majority of master's programs that teach quantum content rely on quantum simulators in Python. Thanks to our close collaboration with IBM's quantum laboratory, our students **will have access to real quantum computers with 154 qubits**.

Program Certified by Google, IBM and the Leading Cybersecurity Entities

The master's degree is designed so that the student not only acquires cutting-edge knowledge, but also obtains the most internationally recognized certifications in the field of cybersecurity, artificial intelligence and quantum computing.

During the program, students will receive official training aligned with the content required by the following professional certifications:

- **CompTIA Security+ (D5)**: Recognized worldwide as the gateway to professional cybersecurity, this certification guarantees mastery of security fundamentals, cryptography, threat management and regulatory compliance.
- **CompTIA CASP+ (D5)**: Focused on senior professionals, it validates the capabilities to design and implement cybersecurity solutions in complex enterprise environments, including hybrid and multi-cloud environments.
- **CCSP – Certified Cloud Security Professional (D5)**: Accredited by (ISC)², this certification endorses the competence to secure complex cloud architectures, both from a technical and regulatory perspective.
- **CISSP – Certified Information Systems Security Professional (D1)**: Considered the global benchmark certification for CISOs and security leaders, it guarantees a comprehensive vision of security in critical and highly regulated environments.

In the field of Artificial Intelligence, the master's degree includes official training delivered directly by Google engineers.

- **Google Cloud – Professional Machine Learning Engineer (PMLE)**: One of the most prestigious credentials in the field of AI, certifying the ability to design, implement and maintain scalable and robust machine learning models in cloud environments.

In the quantum computing module, the master's degree includes professionals from the IBM Quantum team.

- **IBM Qiskit Developer**: Certification that validates knowledge of the fundamental principles of quantum computing, as well as the ability to develop quantum algorithms, placing special emphasis within the master's degree on concrete applications for quantum cryptography and forensic analysis.

Employability and Cybersecurity Laboratory Talent Pool

The profile of an advanced cybersecurity expert with knowledge in artificial intelligence and quantum computing is currently one of the scarcest and most strategic in the market. Critical sectors such as defense, essential infrastructures, energy, banking, insurance companies, research centers and international organizations require professionals capable of anticipating complex threats, including those derived from the advancement of quantum computing.

The master's degree is designed to be a direct talent pool for cybersecurity laboratories in both the public and private sectors, including technological centers of the Ministry of Defence, European institutions, and cyberintelligence divisions of large corporations. Thanks to collaboration with these laboratories, students will be able to work on real projects and participate in strategic challenges proposed by partner entities, which significantly increases employment opportunities.

Our objective is for 100% of graduates to access strategic positions, becoming an active part of the technological defense of our critical infrastructures, in Spain and abroad.

Academic Direction

Ginés Carrascal de las Heras

Materials Engineer and Bachelor in Physics, Optics, and Electronics from the University of Salamanca, where he also completed Doctoral courses in Communications and Environmental Studies. **Master's in Laser Micro-Spectral Analysis** from the University of Holguín.

Quantum Computational Scientist & Architect at IBM Quantum since 2000, helping to make quantum computing a reality to enhance clients' business:

- **IBM Quantum Ambassador**
  - Promotes the dissemination and adoption of quantum computing in companies and universities.
  - Prominent member of IBM's Quantum Research Laboratory.
  - Part of IBM's Industry and Quantum Technology Services.
- **IBM Architect**
  - Builds and leads high-performance development teams using RTC, SOA, Java, and web technologies. Certified Scrum Master and TOGAF 9.
  - He has obtained numerous licenses and certifications throughout his career, including:
    - IBM Certified Associate Developer - Quantum Computation using Qiskit v0.2X
    - Qiskit Advocate
    - IBM Quantum Machine Learning
    - IBM Variational Algorithm Design
    - Qiskit Global Summer School 2022 - Quantum Excellence
    - IBM Basics of Quantum Information
    - IBM Security and Privacy by Design Foundations
    - IBM Quantum-Safe Conversations
    - AWS Certified Solutions Architect – Associate

He holds **over 70 certifications**, which can be consulted via the provided link.

Passionate about sharing his extensive knowledge in **Quantum Computing and Machine Learning**, he serves as a professor at:

- Faculty of Mathematics, Universidad Francisco de Vitoria (since 2021)
- CESTE International Business School (since 2021)
- Universidad Europea (since 2022)
- Master's in Artificial Intelligence Applied to Financial Markets (mIA-X), BME Institute (since 2022)
- Universidad Carlos III de Madrid:
  - Department of Physics – Quantum Computing (2022–2024)
  - Department of Computer Science – Applied Artificial Intelligence Group (2014–2022)
- Faculty of Mathematics, Universidad Complutense de Madrid (2018–2024)

Academic Direction

Escolástico Sánchez Martínez

A **distinguished expert** in the field of **fundamental mathematics**, with **three master's degrees**, **four registered patents and more than 25 years** of professional **experience in the financial sector**, with a specialized focus on areas such as **quantum computing, risk analysis, fraud** and **Blockchain**.

His extensive professional experience, performing key functions in major institutions within the sector (**CNMV** and **BBVA**), provides him with a comprehensive vision of the financial sector. If we add to this the quantitative perspective of a **portfolio manager** (more than five years), that of a **head of risk** (three years) and the legal and **regulatory compliance** dimension (six years), this positions him as an international benchmark in quantitative finance, standing out in the field of risk management and regulatory compliance.

Since 2018 he has been Executive Director at BBVA, leading multidisciplinary teams for the creation of new technological and strategic solutions that have optimized the entity's operational and compliance processes. He stands out as a **leader in the field of quantum computing**, one of the most advanced technological areas in international banking.

Professional Career

- He began working in the financial sector in 1998 after passing several competitive public examinations to become an **inspector** at the public body, the National Securities Market Commission (**CNMV** – 6 years). He specialized in the **control and supervision of deposits and investment funds**, as well as in cutting-edge **new financial instruments**, **developing various financial IT applications**. He also conducted on-site supervision of investment fund managers and custodians.
- At BBVA, he has served as a quantitative and equity risk portfolio manager (more than 5 years), risk control officer, head of regulatory compliance and head of the research area. He has led global teams and projects, with a particular focus on the implementation of innovations in areas such as risk management and analysis, fraud prevention and regulatory compliance.
- He was responsible for the **implementation of major international financial regulations**, such as the Dodd-Frank Act and the Volcker Rule at BBVA, developing self-assessment tools and adapting the bank to market requirements, and managing operational teams in more than 10 countries.
- He has worked on the **design and implementation of IT tools** for the automatic supervision of trading, the prevention of market abuse and the manipulation of benchmark indices such as Euribor and Libor.

Academic Background and Accreditations

- Degree in Fundamental Mathematics.
- Master's degrees in Quantum Computing; Valuation, Control and Management of Options, Futures and New Financial Instruments; Mathematical and Statistical Techniques Applied to Financial Management.
- He completed doctoral courses in Stochastic Systems and Their Optimal Control (grade A) and is certified by D-Wave (Core Quantum Programming and Foundations for Quantum Programming).

Achievements and Recognitions

- He holds four patents in the fields of quantification, risk management, fraud and blockchain.
- A regular speaker at high-level conferences such as Quantum.Tech and Revolution Banking, where he participates in advisory boards and round tables on technological and financial trends.
- Representative in international IOSCO working groups and official supervision and risk workshops at the BIS (Bank for International Settlements).
- Trainer of new inspectors at the CNMV and organizer of ad hoc courses.

AthenAI

4

Program Structure

Every six months, we update the master's program content, ALWAYS offering truly cutting-edge material.

Full Program Structure

Modules	Teaching hours	Wt	Study hours	Total hours	ECTS
0. Introduction and TFM Sessions	30	2 %	60	90	**3,6**
1. Programming Fundamentals	55	5 %	110	165	**6,6**
2. Fundamentals of Artificial Intelligence, Machine Learning, and Deep Learning	110	9 %	220	330	**13,2**
3. Cybersecurity and Ethical Hacking	315	26 %	630	945	**37,8**
4. Technology Law	55	5 %	110	165	**6,6**
5. Quantum Cybersecurity	245	20 %	490	735	**29,4**
6. Cloud Services and Big Data	180	15 %	360	540	**21,6**
7. Artificial Intelligence Applied to Cybersecurity	225	19 %	450	675	**27**
Total	**1.215**	**100 %**	**2.430**	**3.645**	**146**

Structure of the ESSENTIAL Master's Program

Modules	Teaching hours	Wt	Study hours	Total hours	ECTS
0. Introduction and TFM Sessions	15	3 %	30	45	**1,8**
1. Programming Fundamentals	55	12 %	110	165	**6,6**
2. Fundamentals of Artificial Intelligence, Machine Learning, and Deep Learning	105	23 %	210	315	**12,6**
3. Cybersecurity and Ethical Hacking	205	46 %	410	615	**24,6**
4. Cloud Services and Big Data	70	16 %	140	210	**8,4**
Total	**450**	**100 %**	**900**	**1.350**	**54**

Structure of the TOP Master's Program

Modules	Teaching hours	Wt	Study hours	Total hours	ECTS
0. Introduction and TFM Sessions	15	2 %	30	45	**1,8**
1. Cybersecurity and Ethical Hacking	110	14 %	220	330	**13,2**
2. Cloud Services and Big Data	110	14 %	220	330	**13,2**
3. Technology Law	55	7 %	110	165	**6,6**
4. Quantum Cybersecurity	245	32 %	490	735	**29,4**
5. Artificial Intelligence Applied to Cybersecurity	230	30 %	460	675	**27,6**
Total	**765**	**100 %**	**1.530**	**2.295**	**92**

ESSENTIAL Program

Module 1 | Programming Fundamentals
55 Teaching hours

Program Overview
- Presentation and Alignment of Objectives
- Emerging Technologies in Cybersecurity
- Business Case Analysis (Ensuring Coherence in Technological Application)

Python Programming Fundamentals I
- Installation
- Jupyter Notebooks
- Basic syntax, operations, and primitive data types
- Strings
- Data structures: Lists, Tuples, Sets, and Dictionaries

Python Programming Fundamentals II
- Control Flow
- Dictionary and List Comprehensions
- Exceptions
- Functions
- Modules and Scripts
- Writing text files and saving variables

Python Programming Fundamentals III
- NumPy Library

Python Programming Fundamentals IV
- Pandas Library

Python Programming Fundamentals V
- Time Series Processing
- Risk Measurement Simulation (VaR)
- Portfolio Optimization

Python Programming Fundamentals VI
- Data Visualization with Matplotlib
- Data Visualization with Pandas
- Data Visualization with Seaborn
- Financial Data Visualization
- Interactive Visualization with ipywidgets
- Data Acquisition and Storage

Python Programming Fundamentals VII
- Object-Oriented Programming
- Inheritance
- Decorators

Python Programming Fundamentals VIII
- Introduction to HTML
- Web Scraping

Python Programming Fundamentals IX
- Fundamentals of Relational Databases
  - Creating and Manipulating Your Own Databases
  - Importing Relational Data into Python
  - Filters, Sorting, and Grouping in Queries
- Advanced Queries with SQLAlchemy
- Introduction to MongoDB in Python

Python Programming Fundamentals X
- Efficiency Analysis
- Error Management, Testing, and Debugging
  - Types of Testing (Unit, Integration, Functional, and Acceptance Testing)
  - Testing Tools (pytest and unittest)
  - Debugging (Stack Traces, Breakpoints, and Variable Inspection)
- IDEs Beyond JupyterLab

Advanced Visualization Techniques
- Introduction to HTML
- Introduction to CSS
- Introduction to Flask
- Interactive Interfaces with Dash

Module 2 | Fundamentals of AI, Machine Learning, and Deep Learning
105 Teaching hours

Genetic Algorithms
- Objective Function
- Selection Strategies
- Crossover
- Mutation
- Generational Replacement

Swarm Algorithms
- Ant Colony Optimization (ACO)
  - Environment Construction
  - Path Selection
  - Pheromone Quantity
  - Evaporation
  - Pruning toward the Optimal Solution

Fuzzy Logic
- Fuzzy Sets and Degrees of Membership
- Fuzzy Operators
- Rule Creation
- Fuzzification
- Defuzzification

Machine Learning I
- Introduction to Machine Learning
  - AI vs. ML
  - Supervised vs. Unsupervised Learning
  - Classification vs. Regression
  - Parametric vs. Non-Parametric Models
  - Linear vs. Nonlinear Models
- Examples of Financial Applications Using ML
- K-Nearest Neighbors (KNN)
- Decision Trees
  - Simple Decision Tree Example
  - Explainable AI (XAI) for Trees

Machine Learning II
- Preprocessing and Evaluation Metrics
  - Normalization and Standardization
  - Encoding, Labeling, and Discretization (Dummies)
  - Missing Values, Outliers, and NaNs
  - Approaching Time Series as Sequence Blocks
  - Evaluation Metrics: Confusion Matrix, Precision, Recall
  - Simple and Cross Validation
- Dimensionality Reduction
  - The Curse of Dimensionality
  - Feature Selection and Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA)

Machine Learning III
- More Complex Classification Models
- Bayesian Theory: Naive Bayes
- Ensemble Classifiers: Bagging, Boosting, Random Forest, and Gradient Boosting
- Support Vector Machines (SVMs)

Machine Learning IV
- Agglomerative Hierarchical Clustering
  - Definition (Linkage Types)
  - Manual Implementation
  - Simple Example
- Centroid-Based Clustering: K-Means and K-Medoids
  - Definition and Manual Implementation
  - Simple Example with K-Means
  - Interpreting Centroids as Representatives
- Gaussian-Based Clustering: Expectation-Maximization (EM)
  - Definition (Generalization of K-Means)
- Density-Based Clustering: DBSCAN
  - Definition and Simple Example
- Comparison of Clustering Algorithms
  - Comparison Metrics
  - Selection of Appropriate Clustering Algorithm
  - Comparison Examples
- Asset Clustering Using Correlations and Momentum

Machine Learning V – Practical Case
- Feature Generation
- Extraction of Relevant Attributes
- Dimensionality Reduction Incorporating XAI
- Clustering
- Graphext (No-Code Data Analysis)
- XAI for Obtained Results

Dense Neural Networks I
- Introduction
- Working Environment
- Basic Concepts
- Linear Regression
- Gradient Descent
- Logistic Regression
- Nonlinear Models

Dense Neural Networks II
- Introduction to Neural Networks
- Feedforward Neural Networks
- Implementing a Neural Network (Forward Pass)
- Chain Rule for Derivatives
- Backpropagation

Dense Neural Networks III
- Implementing a Neural Network (Backward Pass)
- Introduction to Keras and PyTorch
- Automatic Differentiation

Dense Neural Networks IV
- Implementing a Neural Network with Keras and PyTorch
- Training a Neural Network
- Stochastic Gradient Descent
- Cost Function
- Activation Function

Dense Neural Networks V
- Regularization
- Weight Initialization
- Batch Normalization
- Other Optimization Techniques
- Second-Order Methods

Dense Neural Networks VI
- Hyperparameter Optimization
- Evaluation Metrics
- Cross-Validation
- Grid Search
- Keras Tuner
- HParams Dashboard

Convolutional Neural Networks I
- Kernel Size
- Stride and Padding
- Max Pooling
- Number of Filters and Features
- Dropout

Convolutional Neural Networks II
- Building in Keras
- Kernel Optimization
- Stride and Padding Optimization
- Max Pooling
- Optimization of Filters and Features
- Dropout
- 1D, 2D, 3D Networks

Convolutional Neural Networks III
- Distance Measures Between Images
- Siamese Networks and Content-Based Image Retrieval (CBIR)
- Learning Representations with CNNs
- Applications in Image Search
- Network Robustness
- Adversarial Examples

Convolutional Neural Networks IV
- Input Perturbation Attacks: One-Pixel Attack
- Adversarial Training Methods: Differential Evolution (DE)
- Applications in Generating Robust Models
- YOLO Networks
- RAM (Recognize Anything)

Recurrent Neural Networks I
- Memory-Based Networks
- Long-Term Dependency Problem
- LSTM Networks in TensorFlow and Keras
- LSTM Variants

Recurrent Neural Networks II
- Truncated Backpropagation
- Accumulating LSTM
- Bidirectional LSTM
- Forecasting with LSTM: Time Series, Sequences, and Predictions

State of the Art in Artificial Intelligence
- Inspiration and Research Directions for Master's Thesis Projects

Module 3 | Cybersecurity and Ethical Hacking
205 Teaching hours

Security Fundamentals I: Basic Security Concepts
- CIA Triad (Confidentiality, Integrity, Availability)
- Fundamental terms and definitions
- Evolution of information security
- Regulatory framework and international standards
- Relevance: CISSP (D1), Security+ (D1), CASP+ (D5), CCSP (D1)

Security Fundamentals II: Core Risk Management
- Risk identification and analysis
- Vulnerability assessment
- Threat and countermeasure management
- Business Impact Analysis (BIA)
- Relevance: CISSP (D1), Security+ (D5), CASP+ (D1), CCSP (D1)

Security Fundamentals III: Security Architecture and Models
- Reference models (OSI, TCP/IP)
- Access control models (DAC, MAC, RBAC, ABAC)
- Defense-in-depth architectures
- Network zoning and segmentation
- Relevance: CISSP (D3), Security+ (D3), CASP+ (D1), CCSP (D1)

Security Fundamentals IV: Security Controls and Categorization
- Types of controls (administrative, technical, physical)
- Preventive, detective, and corrective controls
- Risk-based implementation of controls
- Evaluation of control effectiveness
- Relevance: CISSP (D1, D8), Security+ (D5), CASP+ (D5), CCSP (D1)

Network and Infrastructure Security I: Network Security Fundamentals
- Network security protocols
- Secure network design
- Network security devices (firewalls, IDS/IPS)
- Defense against common network attacks
- Relevance: CISSP (D4), Security+ (D3), CASP+ (D2)

Network and Infrastructure Security II: Endpoint and System Security
- Operating system hardening
- Endpoint protection
- Intrusion detection and prevention systems
- Patch and update management
- Relevance: CISSP (D3), Security+ (D2), CASP+ (D2)

Network and Infrastructure Security III: Advanced Security Architectures
- Implementation of Zero Trust architectures
- Micro-segmentation
- Software Defined Networking (SDN)
- Adaptive network architectures
- Relevance: CISSP (D3), Security+ (D3), CASP+ (D1)

Network and Infrastructure Security IV: Cryptography and PKI
- Fundamental cryptographic principles
- Cryptographic algorithms and protocols
- Public Key Infrastructure (PKI)
- Digital certificate management
- Relevance: CISSP (D3), Security+ (D6), CASP+ (D2), CCSP (D2)

Network and Infrastructure Security V: Physical and Environmental Security
- Physical access controls
- Environmental protection
- Personnel security
- CCTV and surveillance systems
- Relevance: CISSP (D7), Security+ (D3), CASP+ (D1), CCSP (D3)

Cloud and Virtualization Security I: Cloud Computing Fundamentals
- Service models (IaaS, PaaS, SaaS)
- Deployment models (public, private, hybrid)
- Reference architectures for the cloud
- Shared responsibility models
- Relevance: CISSP (D3), Security+ (D3), CASP+ (D2), CCSP (D1)

Cloud and Virtualization Security II: Cloud Architecture Security
- Designing secure cloud architectures
- Containers and microservices
- Orchestration and security
- DevSecOps in cloud environments
- Relevance: CISSP (D3), Security+ (D3), CASP+ (D2), CCSP (D3)

Cloud and Virtualization Security III: Virtualization Security
- Hypervisors and virtual machine security
- Attacks specific to virtualized environments
- Security controls in virtualization
- Container security
- Relevance: CISSP (D3), Security+ (D3), CASP+ (D2), CCSP (D3)

Cloud and Virtualization Security IV: Cloud Identity and Access Management
- IAM in cloud environments
- Single Sign-On (SSO) and identity federation
- Privilege management in the cloud
- Multi-factor authentication in cloud environments
- Relevance: CISSP (D5), Security+ (D6), CASP+ (D2), CCSP (D3)

Cloud and Virtualization Security V: Cloud Security Operations
- Monitoring and logging in cloud environments
- Cloud security automation
- Incident response in the cloud
- Cloud backup and recovery
- Relevance: CISSP (D7), Security+ (D4), CASP+ (D3), CCSP (D4)

Data and Application Security I: Data Protection
- Data classification
- Data protection controls
- Data lifecycle management
- Data Loss Prevention (DLP)
- Relevance: CISSP (D2), Security+ (D2), CASP+ (D1), CCSP (D2)

Data and Application Security II: Applied Cryptography for Data Protection
- Data encryption at rest
- Data encryption in transit
- Key management
- Tokenization and masking
- Relevance: CISSP (D2), Security+ (D6), CASP+ (D2), CCSP (D2)

Data and Application Security III: Secure Software Development
- Secure SDLC
- Application security assessment
- Static and dynamic code analysis
- DevSecOps practices
- Relevance: CISSP (D8), Security+ (D2), CASP+ (D4), CCSP (D4)

Data and Application Security IV: Web Application and API Security
- Common vulnerabilities (OWASP Top 10)
- API security
- Secure web services
- WAF and application controls
- Relevance: CISSP (D8), Security+ (D2), CASP+ (D4), CCSP (D3)

Security Operations and Incident Response I: Security Operations Management
- Security Operations Center (SOC)
- SIEM and monitoring tools
- Log and event management
- Vulnerability management
- Relevance: CISSP (D7), Security+ (D4), CASP+ (D3), CCSP (D4)

Security Operations and Incident Response II: Incident Response
- Response plans and procedures
- Containment, eradication, and recovery
- Post-incident analysis
- Incident response teams (CSIRT)
- Relevance: CISSP (D7), Security+ (D4), CASP+ (D3), CCSP (D4)

Security Operations and Incident Response III: Digital Forensics
- Evidence acquisition and preservation
- Network forensics
- System forensics
- Cloud forensics
- Relevance: CISSP (D7), Security+ (D4), CASP+ (D3), CCSP (D4)

Security Operations and Incident Response IV: Business Continuity and Disaster Recovery
- Business continuity planning
- Disaster recovery strategies
- DR/BC testing and exercises
- Continuity in cloud environments
- Relevance: CISSP (D1), Security+ (D5), CASP+ (D3), CCSP (D4)

Governance, Risk, and Compliance I: Security Governance
- Policies, standards, and procedures
- IT governance frameworks
- Security metrics and KPIs
- Security committees
- Relevance: CISSP (D1), Security+ (D5), CASP+ (D5), CCSP (D5)

Governance, Risk, and Compliance II: Advanced Risk Management
- Quantitative vs. qualitative analysis
- Risk mitigation strategies
- Third-party and supply chain risks
- Risk communication
- Relevance: CISSP (D1), Security+ (D5), CASP+ (D5), CCSP (D5)

Governance, Risk, and Compliance III: Compliance and Legal Aspects
- Key regulations (GDPR, HIPAA, PCI-DSS, etc.)
- Security audits
- Contracts and agreements (SLA, DPA)
- Data privacy
- Relevance: CISSP (D1), Security+ (D5), CASP+ (D5), CCSP (D5, D6)

Security+ Certification Preparation
- Review of the 6 Security+ domains
- Exam strategies
- Practice questions
- Mock exam

Security+ – 6 Domains:
- D1: Attacks, Threats, and Vulnerabilities
- D2: Architecture and Design
- D3: Implementation
- D4: Operations and Incident Response
- D5: Governance, Risk, and Compliance
- D6: Cryptography and PKI

CISSP Certification Preparation
- Review of the 8 CISSP domains
- Exam strategies
- Practice questions
- Mock exam

CISSP – 8 Domains:
- D1: Security and Risk Management
- D2: Asset Security
- D3: Security Architecture and Engineering
- D4: Communication and Network Security

- D5: Identity and Access Management
- D6: Security Assessment and Testing
- D7: Security Operations
- D8: Software Development Security

CASP+ Certification Preparation

- Review of the 5 CASP+ domains
- Exam strategies
- Practice questions
- Mock exam

CASP+ – 5 Domains:

- D1: Security Architecture
- D2: Security Operations and Infrastructure
- D3: Security Integration of Systems and Applications
- D4: Incident Response and Risk Management
- D5: Governance, Risk, and Compliance

CCSP Certification Preparation

- Review of the 6 CCSP domains
- Exam strategies
- Practice questions
- Mock exam

CCSP – 6 Domains:

- D1: Cloud Concepts, Architecture, and Design
- D2: Cloud Data Security
- D3: Cloud Platform and Infrastructure Security
- D4: Cloud Application Security
- D5: Cloud Security Operations
- D6: Legal, Risk, and Compliance

Operations – Threats

- Threat modeling and adversary understanding
- Techniques and Procedures (TTPs)
- STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)
- DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability)
- Phases of a cyber attack: reconnaissance, initial access, code execution, persistence, privilege escalation, lateral movement, data exfiltration, and defense evasion
- MITRE ATT&CK framework: mapping and analyzing adversary TTPs, identifying attack patterns, and developing mitigation strategies
  - Relevant adversaries: State and Non-State Actors

DFIR – Digital Forensics and Incident Response

- Incident types: malware, DDoS, network intrusions, data theft, insider abuse
- Preparation, identification, containment, eradication, recovery
- Security policies, Standard Operating Procedures (SOPs), and Incident Response Teams (IRT)
- Intrusion detection and prevention systems (IDS/IPS)
- Security Information and Event Management (SIEM) systems
- Strategies for cleaning infected systems

Operations – Red Team

- Reconnaissance, enumeration, exploitation, privilege escalation, lateral movement, persistence, and data exfiltration
- Tools: Metasploit, Cobalt Strike, PowerShell Empire
- Reverse engineering and exploitation
  - Disassemblers (IDA Pro, Ghidra) and debuggers (OllyDbg, x64dbg)
  - Malware reverse engineering (behavior and characteristics)
  - Exploitation techniques: buffer overflow, code injection, privilege escalation
  - Compilers and code reconstruction
  - Binary file formats and dynamic linkers
  - Dynamic analysis: code debuggers
  - Black box: behavior analysis
  - White box: code debuggers

Operations – Blue Team

- Strategies, techniques, and tools to defend an organization against cyber threats
  - On-premise perimeter security
  - Cloud security
- Detection, correlation, and response
  - SIEM, EDR, and NDR
- Critical infrastructure protection
- Identity and authentication management
- Security Operations Center (SOC)

Ethical Hacking I: Introduction to Ethical Hacking

- Definition and scope of ethical hacking
- Differences between ethical hacker, white hat, black hat, and grey hat
- Legal framework and ethical considerations
- Methodologies and standards (OSSTMM, PTES, OWASP)

Ethical Hacking II: Reconnaissance and Information Gathering

- Passive footprinting techniques
- OSINT (Open Source Intelligence)
- Reconnaissance tools (Shodan, Maltego, theHarvester)
- Metadata analysis and public sources

Ethical Hacking III: Network Scanning and Enumeration

- Host and service discovery
- Port scanning techniques
- Vulnerability identification with Nmap and Nessus
- Enumeration of users, services, and resources

Ethical Hacking IV: Web Application Vulnerabilities

- Web application testing methodology
- OWASP Top 10 – Major vulnerabilities
- SQL Injection and Cross-Site Scripting (XSS)
- Web testing tools (Burp Suite, OWASP ZAP)

Ethical Hacking V: Exploitation Techniques and Privilege Escalation

- Identification of attack vectors
- Exploitation of known vulnerabilities
- Use of exploitation frameworks (Metasploit)
- Privilege escalation techniques in Windows and Linux

Ethical Hacking VI: Network Security Testing

- Man-in-the-Middle attacks
- Sniffing and traffic capture
- Analysis of insecure protocols

- Perimeter security bypass techniques

Ethical Hacking VII: Social Engineering and Forensic Analysis

- Principles and techniques of social engineering
- Phishing and impersonation attacks
- Fundamentals of digital forensic analysis
- Evidence collection and analysis

Ethical Hacking VIII: Reporting and Best Practices

- Documentation of vulnerabilities and tests performed
- Structure and drafting of technical reports
- Mitigation strategies and recommendations
- Planning for recurring tests and follow-up

Module 4 | Cloud Services and Big Data

70 Teaching hours

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

Preparation for the Professional Cloud Architect Certification

CI/CD I

- Introduction and Advanced Git Configuration
- Advanced Branch Management, Merges, and Conflict Resolution
- Collaboration on GitHub: Pull Requests, Code Review, Actions
- Collaborative Project Using Git and GitHub (Full Workflow)
- Feedback and Evaluation of Collaborative Project

CI/CD – Session II

- Introduction to Docker, images, and containers
- Supervised practical exercise: creating custom Docker images
- Docker Compose: basic container orchestration
- Practical deployment of a multi-container web application

Professional Cloud Architect Certification Exam

Master's Thesis Defense I

Master's Thesis Defense II

TOP Program

Module 1 | Cybersecurity and Ethical Hacking
110 Teaching hours

Program Overview
- Presentation and alignment of objectives
- Emerging technologies in cybersecurity
- Business case analysis (ensuring coherence in technological applications)

Be Hacker. Alternative Approaches to Cybersecurity I
- Cybersecurity is everyone's responsibility
- The cybersecurity team is not the police; security cannot be fully delegated
- What you know and what you do not know about the Internet. Who are you on the Internet? Deep Web
- Cybersecurity expertise comes from development, infrastructure, and architecture knowledge
- Security is an intrinsic feature, not an afterthought; secure development

Be Hacker. Alternative Approaches to Cybersecurity II
- Secure networks do not exist; secure identities do. The location-based defense paradigm is obsolete
- You may have documents, plans, and tools, but is your company truly secure?
- Identifying the weakest link in the security chain
- People rarely react well to what they do not understand

Digital Forensics I: Fundamentals of Digital Forensics
- Principles and objectives of digital forensics
- Legal framework and chain of custody
- Types of digital evidence and admissibility
- Forensic analysis lifecycle

Digital Forensics II: Evidence Acquisition and Preservation
- Incident response procedures
- Data acquisition techniques (forensic imaging)
- Tools for capturing volatile and non-volatile evidence
- Integrity verification and process documentation

Digital Forensics III: File Systems
- File system structures (NTFS, FAT, ext4)
- Recovery of deleted files
- Metadata and timestamp analysis
- File and data fragment carving

Digital Forensics IV: Windows Systems
- Windows registry and forensic artifacts
- Security log and event analysis
- Web browsing and communication artifacts
- Evidence correlation in Windows systems

Digital Forensics V: Unix/Linux Systems
- Directory structure and permissions
- Log analysis and auditing
- Forensic artifacts in Linux environments
- Memory analysis in Unix systems

Digital Forensics VI: Memory and Processes
- RAM capture
- Process, connection, and socket analysis
- Detection of rootkits and in-memory malware
- Memory analysis tools (Volatility)

Digital Forensics VII: Mobile Devices and Networks
- Forensic acquisition of iOS and Android devices
- Application and storage analysis
- Network traffic analysis and packet capture
- Correlation of network and system evidence

Digital Forensics VIII: Incident Reconstruction and Reporting
- Timeline and event reconstruction techniques
- Causality and attribution analysis
- Preparation of forensic reports
- Evidence presentation and expert testimony

Malware Analysis I: Introduction to Malware Analysis
- Malware taxonomy and classification
- Infection lifecycle
- Threat actors and motivations
- Setting up secure analysis laboratories

Malware Analysis II: Basic Static Analysis
- File property inspection
- Fingerprinting and hashing techniques
- String and embedded resource analysis
- Pattern and signature identification

Malware Analysis III: Advanced Static Analysis
- Reverse engineering and disassembly
- Source code and pseudocode analysis
- Identification of functions and algorithms
- Static analysis tools (IDA Pro, Ghidra)

Malware Analysis IV: Basic Dynamic Analysis
- Monitoring processes and system changes
- Behavioral analysis in sandbox environments
- Network traffic capture and analysis
- Identification of Indicators of Compromise (IoCs)

Malware Analysis V: Advanced Dynamic Analysis
- Step-by-step debugging and execution analysis
- Memory manipulation and hooks
- Code injection and obfuscation techniques
- Dynamic analysis tools (OllyDbg, x64dbg)

Malware Analysis VI: Anti-Analysis and Evasion Techniques
- Detection of virtual environments and sandboxing
- Code obfuscation and packing
- Anti-debugging and anti-VM techniques
- Persistence and hiding methods

Malware Analysis VII: Specific Malware Analysis
- Ransomware and encryption algorithm analysis
- Botnets and C&C communications
- Rootkits and kernel-level malware
- Malware for mobile devices and IoT

Malware Analysis VIII: Threat Intelligence and Reporting
- Extraction and correlation of indicators
- Attribution and campaign analysis
- Technical report preparation
- Integration with detection and prevention systems

Ethical Hacking Workshop I
Ethical Hacking Workshop II
Ethical Hacking Workshop III
Ethical Hacking Workshop IV

Module 2 | Cloud Services and Big Data
110 Teaching hours

Big Data and Data Processing 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)

Big Data and Data Processing II. Collect I
- Google Cloud Pub/sub
- Messages, Topics
- Best practices
- VerneMQ
- Apache Kafka

Big Data and Data Processing III. Process I
- Dataflow
- Templates
- I/O connectors best practices
- Dataflow runner

Big Data and Data Processing IV. Process II
- Dataproc (spark)
- Dataproce serverless
- Clusters
- Toubleshooting

BBig Data and Data Processing V. Store I
- Google Cloud Storage
- BigQuery
- BigTable

Big Data and Data Processing VI. Analyze I
- BigQuery SQL
- Storage/compute separation
- Dataform

Big Data and Data Processing VII. Analyze II
- Looker
- Looker Studio
- Visualization

Big Data and Data ProcessingVIII
- Data lakes
- Linage, automatizations
- Dataplex

Preparation for the Professional Big Data Engineer Certification

Google Vertex AI – Session I
- Introduction to Vertex AI
- MLOps
- Methodology and Technical Components
- Customer References

Google Vertex AI – Session 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 – Session III
- Vertex AI Prediction
- Batch Predictions
- Model Monitoring
- Explainable AI

Google Vertex AI – Session IV
- Vertex AI Model Registry
- Vertex AI Experiments
- Model Cards

Google Vertex AI – Session V
- Vertex AI Pipelines
- Kubeflow Pipelines
- Components
- Pipelines
- I/O v2

Google Vertex AI – Session VI
- Tabular Workflows
- Hands-On Pipelines I
- Hands-On Pipelines II

Google Vertex AI – Session VII
- ML Metadata
- Low-Code/No-Code
- AutoML
- BQML

Google Vertex AI – Session VIII
- Model Garden: LLMs/LRMs in Vertex AI
- LLMOps in Vertex AI
- Vertex AI Workbench
- Colab Enterprise

Preparation for Professional ML Engineer Certification

CI/CD – Session III
- Core concepts of Kubernetes
- Installation and configuration of Minikube or local environment
- Deployment, scaling, and updating applications in Kubernetes
- Introduction to monitoring (Prometheus + Grafana)
- Basic implementation of monitoring in Kubernetes

CI/CD – Session IV
- Jenkins and GitHub Actions
- Practical configuration of automated pipelines
- CI/CD integration with Docker/Kubernetes
- Final project: complete pipeline with Git, Docker, Kubernetes integration, and monitoring

Professional Big Data Engineer Certification Exam
Professional ML Engineer Certification Exam

Module 3 | Technology Law
55 Teaching hours

Applied Law for Artificial Intelligence I
- Legal frameworks for Artificial Intelligence in Europe, the USA, Asia, and the Middle East
- Liability associated with AI systems (Part I)
- Roles of operator/producer and their legal implications
- Cases of autonomous learning systems and scenarios of online and offline learning

Applied Law for Artificial Intelligence II
- Liability associated with AI systems (Part II)
- The New Artificial Intelligence Regulation
  - Legal framework for advisory services / investment algorithms / MiFID II
  - Requirements for high-frequency and low-frequency algorithms
  - Traceability and associated responsibilities
- Data protection
- Case studies on liability in AI usage

Applied Law for Artificial Intelligence III
- The importance of ethics in AI regulation
- Personal data protection regulations in AI systems
- The AI Sandbox
- The Spanish Agency for AI Supervision
- Malfunction vs. past performance does not guarantee future returns

Applied Law for Platform and Distributed Services I
- Cloud services and data security
- Types of cloud computing services
  - Building services from the cloud: trusted service providers (eIDAS2 Regulation)
- Regulatory and contractual aspects of cloud storage
  - Terms and conditions: applicable versioning
  - Standards and their verification
  - Multi-jurisdictional issues and data protection: virtualization
  - Data protection in the cloud

Applied Law for Platform and Distributed Services II: DSA – Scope of Application
- Provider immunity for content: Good Samaritan clause
- Due diligence obligations
  - Universal obligations: for all hosting services, including online platforms
  - Additional obligations for online platform providers
  - Special and additional obligations for very large platforms and search engines (VLOP, VLSE)
    - Annual systemic risk assessment
    - Specific risk mitigation measures
    - Crisis response mechanisms
    - Recommendation systems
    - Additional transparency on online advertising
    - Data access
    - Verification and compliance functions
    - Independent audits
    - Transparency reports
    - Enforcement, competent authorities, and sanctions

Applied Law for Cryptography and Trusted Service Providers
- Electronic signatures: definition and properties. Types (advanced, probabilistic, blind, multiple, delegated, etc.)
- Signing a document: creation and verification of an electronic signature
- Standard signature algorithms: RSA, DSA, ECDSA
- Electronic certificates (with/without private key). Certification authorities and relational structures
- Certificate revocation
- Timestamps. Timestamp authorities. Requirements
- Trusted Service Providers
- Vulnerabilities and risk assessment

Applied Law for Cybersecurity
- Security vs. security management: ISO/IEC 27001 model
- Cybersecurity regulations and competent authorities
  - Critical infrastructures
  - NIS1 and NIS2
  - Cybersecurity Act
  - Connection to penal codes

Applied Law for Digital Identity I: Identity and Means of Identification under eIDAS Regulation
- What is identity?
- Presumed identity and risk analysis: Zero Trust vs. Friction
- Differences between identity, identification, identity verification, and authentication
  - PSD2, EBA, and authentication factors
- Identity model under eIDAS Regulation (eIDAS1)
  - National analog and digital identity documents
  - Signature certificates: types of signature and evidentiary value for identity

Applied Law for Digital Identity II
- Verification process and its five phases: in-person and online processes
  - Applicable regulations: Spain and EU
  - Applicable standards: Spain and EU
- Identity model under eIDAS Regulation
  - European Digital Identity Wallet (EDIW)
    - Regulation and operation
    - Interoperability with trusted third parties
    - Wallet security
  - Attribute attestations:
    - Trusted attribute attestation service providers
    - Regulation and operation
    - Similarities and differences with qualified certificate issuers and SSI/DID-based models
    - Interactions with other providers/operators
  - Trusted services and providers Post-reform: changes and continuities
  - Changes in cybersecurity requirements: new scheme and requirements

Legal Aspects (Open AI)
- Open AI
- Types of licenses for AI components
- Model Cards
- Role of intellectual property rights
- Regulatory impact on models
- Case studies

Legal Framework for National Defense in Cyberspace
- Cybersecurity within the National Security System
- Joint Cyber Defense Command of the Armed Forces

- Principles of sovereignty, due diligence, jurisdiction, and international responsibility in cyberspace
- Ius ad bellum: Use of armed force in cyberspace
- Ius in bello: Application of International Humanitarian Law in cyberspace
- Cybersecurity standardization bodies
- ISO/IEC JTC1 27035 regulations

Module 4 | Quantum Cybersecurity
245 Teaching hours

Fundamentals of Quantum Computing I: Basic Quantum Mechanics
- Principles of quantum mechanics
- Superposition and entanglement
- Mathematical foundations

Fundamentals of Quantum Computing II: Qubits and Gates
- Quantum states
- Dirac notation
- Single-qubit gates (X, Y, Z, H)
- Controlled gates (CNOT, Toffoli)
- Circuit construction
- Bell and GHZ states
- Projective measurements
- Phase kickback

Fundamentals of Quantum Computing III: Basic Algorithms
- Bernstein-Vazirani
- Teleportation
- Dense encoding

Fundamentals of Quantum Computing IV: Quantum Hardware
- Superconducting qubit technologies
- Trapped ions
- Quantum photonics
- Control and measurement
- Quantum error correction
- Scalable architectures

Quantum Algorithms I: Shor's Algorithm
- Mathematical foundations
- Quantum Fourier Transform
- Phase estimation
- Detailed implementation
- Complexity analysis
- Cryptographic implications

Quantum Algorithms II: Grover's Algorithm
- Quantum search
- Quantum oracle
- Amplitude amplification
- Algorithm optimization
- Practical applications and use cases
- Quantum optimization: VQE, QAOA, Grover Adaptive Search
- Quantum scenario simulation: Quantum random walks, quantum Bayesian networks

IBM Qiskit Developer certification preparation

Quantum Public Key Infrastructure (PKI) I: Hybrid PKI Design
- Hybrid CA architecture
- Certification hierarchies
- Certification policies
- Multi-algorithm management
- Transition periods
- Interoperability

Quantum PKI II: Certificate Management
- Certificate lifecycle
- Revocation systems
- Quantum OCSP and CRL
- Hybrid certificate formats
- Secure storage
- Auditing and logging

Quantum PKI III: Quantum Digital Signatures
- Hybrid signature schemes
- Emerging standards
- Long-term validation
- Quantum timestamping
- Evidence preservation

Quantum PKI IV: System Migration
- Legacy system analysis
- Migration strategies
- Backward compatibility
- Integration testing
- Risk management
- Contingency planning

Basic Quantum Algorithms and Protocols I: Lattice-Based Cryptography
- Learning With Errors (LWE)
- Ring-LWE
- Module-LWE
- NTRU
- CRYSTALS-Kyber
- Practical optimizations

Basic Quantum Algorithms and Protocols II: Multivariate Systems
- Oil-Vinegar
- Rainbow
- HFE variants
- UOV schemes
- Efficient implementations
- Security analysis

Basic Quantum Algorithms and Protocols III: Hash-Based Cryptography
- Hash-based signatures
- SPHINCS+
- XMSS
- Merkle trees
- One-time and few-time signatures

Basic Quantum Algorithms and Protocols IV: Code-Based Cryptography
- Classic McEliece
- Goppa codes
- QC-MDPC
- Syndrome decoding
- Parameter optimization
- Practical implementation

Secure Implementation of Quantum Systems I: Secure Development
- Secure development lifecycle
- Best programming practices
- PQC implementation testing
- Secure memory management
- Version control and auditing
- DevSecOps for PQC systems

Secure Implementation of Quantum Systems II: Side-Channel Attacks
- Timing attacks
- Power analysis
- Electromagnetic attacks
- Fault injection
- Cache attacks
- Microarchitecture and side-channels

Secure Implementation of Quantum Systems III: Countermeasures
- Constant-time implementations
- Arithmetic masking
- Fault protection
- Randomization
- Implementation validation
- Resilience testing

Secure Implementation of Quantum Systems IV: System Integration
- Secure cryptographic APIs
- PQC libraries
- Integration with TLS/SSL
- Testing and benchmarking
- Performance monitoring
- Incident management

Blockchain and Quantum Cryptography I: Blockchain Fundamentals
- Blockchain architecture
- Distributed consensus
- Smart contracts
- Blockchain cryptography

Blockchain and Quantum Cryptography II: Quantum Threats
- Impact on ECDSA signatures
- Bitcoin vulnerabilities
- Threat timeframes
- Migration strategies

Blockchain and Quantum Cryptography III: Quantum Solutions
- Quantum-safe signatures in blockchain
- Protocol updates
- Wallet migration
- Quantum-safe smart contracts

Blockchain and Quantum Cryptography IV: Practical Implementation
- Hyperledger Fabric
- IBM Blockchain Platform
- Quantum Ethereum
- Testing and validation

IoT Security in the Quantum Era I: Secure IoT Architecture
- IoT protocols
- Identity management
- Edge-fog-cloud architectures
- Sensor security

IoT Security in the Quantum Era II: Lightweight Cryptography
- Lightweight algorithms
- Resource optimization
- Energy management
- Efficient protocols

IoT Security in the Quantum Era III: PQC Solutions for IoT
- Optimized implementations
- Secure bootstrapping
- Secure updates
- Key management

IoT Security in the Quantum Era IV: Practical Use Cases
- Industrial IoT
- Smart cities
- Healthcare IoT
- Sensor networks

Cloud Security and Quantum Computing I: Cloud Security
- Service models
- Multicloud architectures
- Secret management
- Zero Trust in cloud

Cloud Security and Quantum Computing II: Quantum Threats
- API vulnerabilities
- Long-term storage
- Cloud communications
- Risk analysis

Cloud Security and Quantum Computing III: PQC Solutions
- Service migration
- Certificate management
- Automation

Cloud Security and Quantum Computing IV: DevSecOps
- Quantum CI/CD
- Automated security
- Monitoring
- Incident response

Advanced Quantum Algorithms and Protocols I: CRYSTALS Suite
- CRYSTALS-Kyber deep dive
- CRYSTALS-Dilithium
- AVXII optimizations
- Hardware implementation
- Protocol integration
- Performance analysis

Advanced Quantum Algorithms and Protocols II: Falcon and SPHINCS+
- Falcon signature scheme
- SPHINCS+ in detail
- Performance comparison
- Practical optimizations
- Specific use cases
- Real-system integration

Advanced Quantum Algorithms and Protocols III: Hybrid Protocols
- Hybrid protocol design
- Quantum TLS
- Quantum SSH
- Quantum IKE/IPSec
- Security analysis
- Performance and optimization

Advanced Quantum Algorithms and Protocols IV: Specialized Applications
- Quantum IoT
- Quantum blockchain
- Quantum cloud computing
- Embedded systems
- Mobile devices
- Critical infrastructures

Quantum Communication Security I: QKD
- BB84 and E91 protocols
- QKD hardware
- Practical limitations
- Attacks and defenses

Quantum Communication Security II: Quantum Networks
- Quantum repeaters
- Quantum routing
- Quantum memory
- Network protocols

Quantum Communication Security III: Hybrid Systems
- QKD-PQC integration
- Trusted nodes
- Key management
- Hybrid architectures

Quantum Communication Security IV: Applications
- Metropolitan networks
- Satellite communication
- Quantum backbone
- Use cases

Cryptographic Systems Audit I: Audit Framework
- International standards
- Evaluation methodologies
- Technical documentation
- Professional reporting

Cryptographic Systems Audit II: Tools and Techniques
- Code analysis
- Implementation testing
- Protocol audit
- Automated tools

Cryptographic Systems Audit III: PQC Evaluation
- Algorithm validation
- Transition analysis
- System verification
- Resilience testing

Cryptographic Systems Audit IV: Practical Cases
- Financial sector
- Critical infrastructures
- Government systems
- Regulatory compliance

Quantum Cryptography Workshop I
Quantum Cryptography Workshop II
Quantum Cryptography Workshop III
Quantum Cryptography Workshop IV

Module 5 | Artificial Intelligence Applied to Cybersecurity

230 Teaching hours

Quantum Machine Learning I
- Quantum Support Vector Machines
- Cryptographic implications

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

Kohonen networks
- Unsupervised competitive networks
- 2D self-organizing maps
- 3D self-organizing maps
- Solving the Traveling Salesman Problem with self-organizing maps

Natural Language Processing I
- Corpora and stopwords
- Word2Vec models. Language representation
- NLP models and Sequence-to-Sequence models
- Bucketing & Padding

Natural Language Processing II
- Supervised learning in NLP. Defining the language domain
- Named Entity Recognition. Entity detection and applications in finance
- Text classification: headlines, reports, news
- Sentiment analysis: news and social media

Natural Language Processing III
- Transfer learning in NLP. TensorFlow Hub
- Pre-trained models: BERT, ELMo
- Fine-tuning pre-trained models for specific tasks

Natural Language Processing IV
- Attention layers
- Attention-based models
- Introduction to Transformer models

Natural Language Processing V
- Advanced Transformer models
- Generative Pre-Training: GPT models
- PaLM, Chinchilla, Flamingo, Minerva, Gato

Generative Models I
- Dimensionality reduction and factors: PCA
- Autoencoders and nonlinear models
- Maximum likelihood and Gaussian Mixture Models (GMM)
- Generating stock quotations using PCA + GMM
- GANs, diffusion models, and conditional models

Generative Models II
- Deep generative models
- Variational Autoencoders (VAE)
- Memory-augmented autoencoders (MAAE)
- Sparse autoencoders
- Generative Adversarial Networks (GAN)

- Recurrent generative models
- Normalizing Flows

Generative Models III

- Pretraining of Large Language Models
- Fine-tuning
- PEFT (Parameter Efficient Fine-Tuning)
- Distillation
- Frameworks: T5X, PAX, others
- TPU architectures

Generative Models IV

- Introduction to LangChain
- Components I: memory, models, and prompts
- Components II: retrievals, chains, and agents
- RAG techniques (Retrieval-Augmented Generation)

Recommendation Systems

- Profile and asset clustering
- Recommendation generation and assignment systems
- TensorFlow Recommenders
- Similarity-based systems
- Factorization-based systems
- Deep learning-based systems

Transfer learning and advanced models

- Inception V3, VGG16, ResNet, BERT
- Model reuse and concatenation
- Solving rotation and scaling problems
- Improvements in convolutional and generative networks
- Gradient vanishing solutions
- ResNet, Capsule Networks

LLMs (Large Language Models)

- Transformers, BERT, LaMDA & LLaMA2, GPT, YaLM, LLaMA, PaLM2, Meta-Transformer
- Use of pre-trained models: APIs, fine-tuning, QA on proprietary databases

AI-Assisted Threat Detection I: Anomaly Detection Systems

- Anomaly detection systems
- Behavioral analysis using machine learning
- Detection of advanced persistent threats (APT)
- Zero-day vulnerability discovery
- Real-time monitoring and alerting systems

Research with Google DeepMind I

- Federated learning
- Gemini model family (1.0, 1.5, 2.0; review of 4 papers)
- Multimodality

Research with Google DeepMind II

- Gemma model family (review of 11 papers): Gemma-1, RecurrentGemma, CodeGemma, PaliGemma, ShieldGemma, DataGemma, ColPali
- Innovations: SigLIP, Griffin, Gemma Scope
- LLaMA model family (review of 4 papers from Meta)
- STaR: Bootstrapping reasoning with reasoning
- Human-like systematic generalization via meta-learning neural networks
- Towards self-assembling artificial neural networks via neural developmental programs

Agentic AI I

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

Agentic AI II

- ADK (Agent Development Kit)
- MCP (Model Context Protocol)
- A2A (Agent-to-Agent Protocol)
- LangChain introduction

Agentic AI III

- Foundational concepts of agents
- Building agents in Google Cloud
- Agentic memory management. LLM as operating systems
- Labs

Agentic AI IV

- Agent Engine and Agent Garden
- Agent evaluation and improvement
- AgentOps
- Labs

LRM - Large Reasoning Models

- Architectures
- Differences between LLMs and LRMs
- Gemini 2.5 vs OpenAI o3, o4
- Evaluation methodology
- Use cases

AI GRC Tools

- Inventory and classification of AI systems
- Risk catalog and associated controls
- Project and use case tracking, dashboards
- Regulatory compliance evaluation
- Workflows

Risk and governance workshops

- Application to Smart Due Diligence
- Cloud + MCP + graphs
- Automatic error detection and prompt self-correction

AI-Assisted Threat Detection II: Data Analytics for Security

- Big data processing for security logs
- Time series analysis for threat intelligence
- NLP for threat reports
- Graph analysis for network behavior
- Visualization techniques for security operations

Advanced AI and Quantum Computing I: Attack Vectors Against ML, Adversarial Machine Learning

- Attack vectors for machine learning systems
- Poisoning and evasion attacks
- Adversarial example generation and defense
- Model robustness and verification
- Secure implementation of ML models

Advanced AI and Quantum Computing II: Privacy-Preserving Machine Learning

- Differential privacy techniques
- Federated learning for secure collaboration
- Homomorphic encryption for model training
- Secure multi-party computation
- Data minimization strategies

Advanced AI and Quantum Computing III: Quantum-Resistant AI Systems
- Quantum-secure machine learning algorithms
- Protecting AI infrastructure against quantum threats
- Quantum adversarial machine learning
- Hybrid classical-quantum defense mechanisms
- Quantum-enhanced privacy-preserving techniques

Advanced AI and Quantum Computing IV: Advanced Quantum Threat Detection
- Intrusion detection with quantum sensors
- Quantum machine learning for anomaly detection
- Quantum-enhanced pattern recognition for threat intelligence
- Entanglement-based security protocols
- Quantum networks for secure communications

AI Security Automation and Orchestration I: Security Orchestration - Platforms and Workflows
- SOAR platforms and implementation
- Automated incident response workflows
- AI-driven decision support systems
- Integration with existing security infrastructure
- Measuring automation effectiveness

AI Security Automation and Orchestration II: AI-Enhanced Ethical Hacking
- AI-assisted penetration testing
- Automated vulnerability scanning
- Reinforcement learning for attack simulation
- Scaling red team operations
- Responsible disclosure practices

AI Security Automation and Orchestration III: Malware Classification and Modeling
- Automated malware classification
- Dynamic and static analysis techniques
- Malicious software behavior modeling
- Generative models for vulnerability discovery
- Anti-evasion techniques

AI Security Automation and Orchestration IV: Advanced Digital Forensics with AI
- Intelligent collection and processing of evidence
- Automated artifact discovery and extraction
- Machine learning for file fragment reconstruction
- NLP for log analysis
- Intelligent forensic timeline reconstruction

AI for Legacy Cryptography Remediation I: Automated Cryptographic Code Analysis
- Automated analysis of cryptographic code
- Machine learning for vulnerability detection
- Static and dynamic analysis of cryptographic implementations
- Pattern recognition for obsolete functions and algorithms
- Development of scanning tools for large codebases

AI for Legacy Cryptography Remediation II: Intelligent Cryptographic Refactoring
- AI-assisted migration from obsolete to modern cryptography
- Learning-based approaches for preserving equivalent functionality
- Automated test generation for cryptographic fixes
- Code transformation verification
- Risk assessment during cryptography transitions

AI for Legacy Cryptography Remediation III: Cryptographic Technical Debt Management
- Prioritization algorithms for cryptographic vulnerabilities
- Impact analysis using predictive modeling
- Cost-benefit analysis for remediation efforts
- ML-based identification of critical cryptographic assets
- Tracking cryptographic dependencies in systems

AI for Legacy Cryptography Remediation IV: Legacy Protocol Compatibility
- AI solutions for backward compatibility challenges
- Intelligent negotiation and protocol regression
- Safe transition strategies with ML-based decision support systems
- Automated testing frameworks for compatibility
- Hybrid implementation approaches for legacy systems

Advanced Digital Forensics with AI I: Deep Learning
- Image and video manipulation detection
- Audio and voice forensic analysis
- Deepfake detection and attribution
- Steganography detection using neural networks
- Camera source identification and matching

Advanced Digital Forensics with AI II: AI Networks
- Automated network traffic analysis
- Network behavior profiling
- Forensic investigation of advanced persistent threats (APT)
- Botnet detection and analysis
- Encrypted traffic forensics

Advanced Digital Forensics with AI III: Memory and Malware
- AI-assisted memory dump analysis
- Automated rootkit and backdoor detection
- Unknown malware behavior analysis
- Code similarity and attribution analysis
- Machine learning-assisted reverse engineering

Advanced Digital Forensics with AI IV: AI for Forensic Case Building
- Entity recognition in digital evidence
- Relationship mapping across disparate data sources
- Intelligent evidence correlation techniques
- Predictive modeling for investigative leads
- Expert systems for case assessment

AI Applied to Cryptography Workshop I
AI Applied to Cryptography Workshop II
AI Applied to Cryptography Workshop III
AI Applied to Cryptography Workshop IV

Master's Thesis Defense I
Master's Thesis Defense II

AthenAI

5

Certifications

You will be able to obtain up to ***eight certifications***, all while studying this Master's program.

Security+ D5 Certification (CompTIA Security+)

The **Security+ certification**, issued by **CompTIA**, is designed to validate the **foundational cybersecurity skills** required to identify, mitigate, and respond to common threats. It is ideal for technical professionals seeking to establish a solid foundation in IT security and is widely recognized across corporate, government, and financial sectors.

This certification demonstrates that professionals are capable of:

- Effectively detecting and responding to security incidents
- Applying cybersecurity principles to networks, devices, users, and applications
- Implementing security controls in accordance with organizational policies and regulations

Certificate Content

Security Fundamentals:

- Principles of Confidentiality, Integrity, and Availability (CIA)
- Basic risk management and security controls

Threats, Vulnerabilities, and Attacks:

- Types of threats (malware, phishing, ransomware, etc.)
- Vulnerability analysis and mitigation

Security Architecture and Design:

- Secure network design
- Security in hybrid and cloud environments

Identity and Access Management (IAM):

- Authentication methods and access control
- Applying security policies to users and devices

Risk Management and Compliance:

- Policies, procedures, and relevant regulations (e.g., GDPR, ISO/IEC 27001)
- Physical and environmental security

Security Operations:

- Threat detection, incident response, and business continuity
- Security monitoring and log management

Benefits for Students:

- Well-suited for technical profiles in early or mid-career stages
- Globally recognized accreditation, widely used in tech companies, financial services, and public institutions
- Practical application focused on real operational tasks, from network protection to incident management

To obtain this certification, candidates must pass a **90-minute exam** consisting of up to **90 multiple-choice and interactive performance-based questions (PBQs)**. The exam can be taken remotely under supervision or at authorized testing centers.
The **exam fee is USD 392**, which must be paid directly to CompTIA by the student.

Prerequisites: None are required, although general IT knowledge is recommended.

CASP+ D5 Certification (CompTIA Advanced Security Practitioner)

The **CASP+ certification**, issued by **CompTIA**, validates **advanced cybersecurity skills** for professionals who design, implement, and manage complex security solutions in large organizations. Unlike other management-focused certifications, CASP+ emphasizes **expert-level technical skills**, making it a key credential for security architects, senior engineers, and specialists in critical environments.

This certification demonstrates that professionals can:

- Design complex, integrated security architectures in enterprise environments
- Implement cryptographic, network, and resilience solutions against advanced threats
- Assess risks, manage vulnerabilities, and ensure regulatory compliance in distributed systems

Certificate Content

Enterprise Security:

- Evaluation of technical and business requirements for security solutions
- Design of security strategies aligned with organizational lifecycle

Risk Management and Compliance:

- Assessment and mitigation of advanced risks
- Integration of regulatory frameworks (e.g., NIST, ISO, GDPR) into security architectures

Security Architecture:

- Designing secure architectures in on-premise, cloud, and hybrid environments
- Applying advanced techniques in segmentation, virtualization, and access control

Security Operations:

- Managing complex security events and incidents
- Automating responses with orchestration tools and forensic analysis

Cryptography and Identity Management:

- Selecting and implementing cryptographic algorithms
- Integrating IAM solutions, MFA, and identity federation

Benefits for Students:

- Expert technical profile: Recommended for senior professionals seeking deep technical and tactical cybersecurity expertise
- Advanced operational focus: Provides practical experience in real-world environments, especially in critical sectors such as finance, defense, and telecommunications
- Professional recognition: Highly valued by employers requiring technical skills beyond standard security management

To obtain this certification, candidates must pass a **165-minute exam** consisting of up to **90 questions** that combine multiple-choice and performance-based simulations (PBQs). The exam can be taken **in-person or remotely under supervision**.
The **exam fee is USD 494**, which must be paid directly to CompTIA by the student.

Prerequisites: None are mandatory, but at least **5 years of experience in cybersecurity**, particularly in technical or architecture roles, is recommended.

CISSP D1 Certification (Certified Information Systems Security Professional)

The **CISSP certification,** issued by **(ISC)²**, is designed to validate **advanced knowledge and skills** in designing, implementing, and managing cybersecurity programs. It is a globally recognized credential, highly valued by organizations in the financial, technology, and government sectors, and is intended for professionals seeking **strategic roles in protecting critical information assets**.

This certification demonstrates that professionals can:

- Design and manage comprehensive and resilient security architectures
- Identify and mitigate cybersecurity risks in complex organizations
- Align security policies and controls with business objectives and regulatory requirements

Certificate Content

Security and Risk Management:

- Risk assessment and impact analysis
- Governance, compliance, and security policies

Asset Security:

- Classification and lifecycle management of information
- Protection of privacy and intellectual property

Security Architecture and Design:

- Designing secure architectures
- Secure design principles for cloud, on-premise, and hybrid environments

Network and Communication Security:

- Secure network protocols
- Detection, prevention, and response to threats in complex networks

Identity and Access Management (IAM):

- Authentication, authorization, and federation systems
- Implementation of role-based access control policies

Security Assessment and Testing:

- Audits, penetration testing, and vulnerability analysis

Security Operations:

- Event monitoring, incident response, and business continuity

Software Development Security:

- Secure software development lifecycle (SDLC) principles
- Vulnerability management in applications

Benefits for Students:

- Certification issued by (ISC)², recognized as a standard of excellence in cybersecurity
- Highly valued in regulated sectors such as banking, insurance, defense, and consulting
- Equips professionals to lead cybersecurity programs and manage organizational risk at scale

To obtain this certification, candidates must pass a **4-hour exam** consisting of **100–150 adaptive (CAT) multiple-choice questions**, taken at authorized testing centers or remotely under supervision. The **exam fee is USD 749**, which must be paid directly to **(ISC)²** by the student. **Prerequisites:** Candidates must have **5 years of professional experience** in at least **2 of the 8 CISSP CBK domains**. Those lacking the required experience can obtain the status of **"Associate of (ISC)²"** until they complete the necessary years.

CCSP D5 Certification (Certified Cloud Security Professional)

The **CCSP certification**, issued by **(ISC)²**, is designed to validate **advanced competencies in cloud security**. It is an internationally recognized credential, ideal for professionals who **manage, design, or audit cloud security architectures and operations**. The certification combines a technical and strategic approach, integrating legal, regulatory, and data governance aspects.

This certification demonstrates that professionals can:

- Design and implement secure architectures in public, private, and hybrid cloud environments
- Assess risks, apply technical controls, and ensure regulatory compliance in the cloud
- Efficiently manage identities, data, and security operations in distributed environments

Certificate Content

Cloud Architectural Concepts:

- Delivery models (IaaS, PaaS, SaaS)
- Principles of secure cloud architecture

Governance, Risk, and Compliance:

- Risk assessment in cloud environments
- Compliance with regulatory frameworks (GDPR, ISO/IEC 27017, PCI DSS, etc.)

Cloud Infrastructure Security:

- Designing resilient architectures
- Network controls, virtualization, and multi-cloud environment protection

Data Security:

- Encryption in transit and at rest
- Information lifecycle management and classification

Identity and Access Management (IAM):

- Federations, multi-factor authentication (MFA), and granular access control

Cloud Security Operations:

- Monitoring, incident response, and business continuity
- Automation and DevSecOps in cloud environments

Benefits for Students:

- High specialization in cloud security, ideal for cloud architects, compliance officers, and cloud auditors
- Certification backed by (ISC)² and aligned with international best practices
- Highly valued in banking, insurance, fintech, and public administration due to its regulatory and technical focus

To obtain this certification, candidates must pass a **4-hour exam** consisting of **125 multiple-choice questions**, taken at authorized testing centers or remotely under supervision.

The **exam fee is USD 599**, which must be paid directly to **(ISC)²** by the student.

Prerequisites: Candidates must have at least **5 years of professional experience in information security**, including **1 year in one of the CCSP-defined cloud security domains**. Those who have not yet met the requirements can obtain the status of **"Associate of (ISC)²"** until they complete the necessary experience.

Quantum Computing Developer Qiskit 2, IBM

This certification is designed for developers seeking to deepen their expertise in quantum computing. It focuses on the programming and conceptualization of quantum circuits and algorithms, as well as understanding the mathematical operations underlying quantum systems.

Certificate Content

Fundamental Concepts of Quantum Computing:

- Qubits and basic operations
- Quantum gates and circuit creation

Quantum Algorithms:

- Deutsch-Jozsa, Grover, and Shor algorithms

Qiskit 2:

- Using Qiskit to build and simulate quantum circuits
- Managing simulators and real quantum computers

Quantum Applications:

- Optimization and finance

Priority access through IBM to real 154-qubit quantum devices to practice the knowledge acquired in class.

Benefits for Students:

- Competitive Differentiation: Gain expertise in an advanced, high-demand field
- Access to Specialized Opportunities: Open pathways in quantum computing and finance
- Advanced Technical Skill Development: Hands-on experience with real quantum systems
- Industry-Recognized Credentials

To obtain this certification, students must pass the practical exam on the IBM platform (Pearson VUE).

An additional fee of $200 is required for the exam, payable directly to IBM by the student.

Professional Machine Learning Engineer (PMLE), Google Cloud

The **Professional Machine Learning Engineer (PMLE) certification**, issued by Google, is designed as a key credential for students, developers, and data scientists who wish to demonstrate skills in machine learning, model deployment, data governance, and AI infrastructure.

This certification is intended to validate that professionals can:

- Design scalable and maintainable ML solutions.
- Implement ML models following Google Cloud best practices.
- Assess the effectiveness and risks of deployed ML models.

Certification Content

Machine Learning Conceptual Framework:

- Selection of modeling techniques and data
- Hyperparameter tuning and evaluation

ML Model Development:

- Creation of data pipelines
- Implementation of algorithms and techniques for supervised and unsupervised problems

Production Deployment:

- Automation of ML models
- Continuous monitoring and improvement of deployed models

Google Cloud Tools:

- Use of Vertex AI, TensorFlow, and BigQuery ML

Benefits for Students

- Global Recognition by Google
- Enhanced Employability and Credibility: ML and Google Cloud skills are highly sought after across various industries, including finance.
- Access to an Innovation Ecosystem: GCP products and AI technologies are constantly evolving; this certification demonstrates that the student is prepared and officially certified by Google.

To obtain this certification, students must pass an exam of approximately **2 hours**, consisting of **50–60 multiple-choice questions**, taken remotely under supervision without access to reference materials.

The exam fee is **200 USD**, which must be paid directly to Google by the student.

Professional Data Engineer (PDE), Google Cloud

The **Professional Data Engineer (PDE) certification**, issued by Google Cloud, is aimed at professionals who design, build, and optimize scalable, secure, and value-oriented data processing systems. This credential certifies key skills for turning data into actionable insights, which is essential in the financial sector.

This certification validates that professionals can:

- Design and build efficient, scalable data processing systems.
- Integrate and transform large volumes of structured and unstructured data.
- Ensure data security, integrity, and governance.
- Apply machine learning techniques to extract advanced insights.

Certification Content

Data System Design:

- Architectures for data ingestion, storage, and analysis
- Selection of technologies for streaming and batch data

Data Pipeline Construction:

- Implementation of processing workflows using tools such as Dataflow, Pub/Sub, Dataproc, and Apache Beam
- Data cleaning, transformation, and enrichment

Data Modeling and Analysis:

- Using BigQuery for real-time analytics
- Applying machine learning models to large-scale datasets

Security and Compliance:

- Access management, auditing, and regulatory compliance in regulated environments

Key Google Cloud Tools:

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

Benefits for Students

- Globally Recognized Certification: Endorsed by Google Cloud and acknowledged by leading companies in the financial and technology sectors.
- High Employability: The role of Data Engineer is highly sought after due to its critical role in digital transformation.
- Practical Skills for the Financial Sector: Specific preparation for working with high-frequency financial data, market history, and risk analysis.

To obtain this certification, students must pass an exam of approximately **2 hours**, consisting of **50–60 multiple-choice questions,** taken remotely under supervision without access to reference materials.

The exam fee is **200 USD**, which must be paid directly to Google by the student.

Professional Cloud Architect (PCA), Google Cloud

The **Professional Cloud Architect (PCA) certification**, issued by Google, is designed to validate the skills required to design, develop, and manage secure, scalable, and highly available infrastructures on Google Cloud Platform (GCP). It is an essential credential for professionals seeking to master cloud architecture with a practical and strategic approach.

This certification demonstrates that professionals are capable of:

- Designing robust, efficient, and secure cloud architectures.
- Managing infrastructure solutions that meet technical, business, and regulatory requirements.
- Monitoring, optimizing, and securing the performance of cloud environments.

Certification Content

Cloud Architecture Design:

- Selecting appropriate services for different business needs
- Defining network, storage, compute, and database structures

Security and Regulatory Compliance:

- Implementing access control, encryption, and auditing policies
- Ensuring alignment with regulatory frameworks such as GDPR or MiFID II

Management and Optimization of GCP Solutions:

- Monitoring resources and performance
- Automating tasks using tools like Cloud Deployment Manager and Terraform

Specific Use Cases:

- Implementing financial analytics, big data, and AI solutions on GCP

Google Cloud Tools:

- Cloud Storage, Compute Engine, Kubernetes Engine, BigQuery, Cloud IAM, among others

Benefits for Students

- International Recognition: Official certification issued by Google Cloud.
- High Employability: Cloud architecture skills are essential in banking, fintech, and capital markets.
- Preparation to Lead Digital Transformation: Students will be equipped to design solutions that meet the highest standards in the financial sector.

To obtain this certification, students must pass an exam of approximately **2 hours**, consisting of **50–60 multiple-choice questions**, taken remotely under supervision without access to reference materials.

The exam fee is **200 USD**, which must be paid directly to Google by the student.

AthenAI

Career Opportunities

Upon completing this Master's program, you will become a ***CISO specialized in cybersecurity*** with AI and Quantum Computing, a highly sought-after and well-compensated profile in both the financial sector and the Ministry of Defense.

This master's program offers multiple professional career paths:

- **Secure AI Systems Architect**

You will be dedicated to designing artificial intelligence systems that integrate security from their inception. You will be responsible for protecting AI models against adversarial attacks, training data leaks, and malicious manipulation, while ensuring regulatory compliance. This specialization is particularly valuable because AI applications are being integrated into all critical infrastructures, and a security failure in these systems could have catastrophic consequences. Moreover, as AI regulations become more stringent, organizations need experts capable of navigating this complex regulatory landscape.

- **Security Analyst with AI Tools and Quantum Technologies**

This profile is particularly valuable because it combines immediate operational capabilities (security analysis using AI) with long-term strategic preparedness (defense against quantum threats). Organizations require professionals who can not only respond to current security challenges but also prepare for the transition to an environment where quantum computing is a reality, especially in sectors such as finance, healthcare, energy, and, most importantly, defense. In this role, you will use AI tools to detect anomalous patterns, analyze critical systems to determine their resilience against future quantum computer attacks, prioritize the updating of vulnerable infrastructures, and deploy security solutions that combine traditional cryptography with quantum algorithms, ensuring protection against both current and future threats. You will also use predictive AI systems to anticipate potential attack vectors, enabling you to develop defenses before threats materialize.

- **Military Cyberintelligence Analyst**

You will focus on detecting and analyzing advanced threats to critical infrastructures. You will use AI to process large volumes of data and identify attack patterns, while implementing quantum protections for sensitive information. This role is fundamental, as foreign powers are investing in quantum capabilities for military purposes.

- **Electronic Warfare Specialist**

You will be the expert developing and protecting military communication systems resistant to quantum computing threats. You will design countermeasures against interference and attacks, using AI to adapt in real time to emerging threats. This role is crucial because secure communication systems are, and will remain, the backbone of modern military operations.

- **Intelligent Weapon Systems Security Auditor**

You will be responsible for evaluating vulnerabilities in AI-integrated weapon systems, ensuring they cannot be compromised by adversaries. You will verify the resilience of these systems against future quantum attacks and ensure compliance with security protocols.

- **Cryptography Developer for Tactical Communications**

You will implement quantum algorithms in field military communication devices, ensuring that tactical communications remain secure even against advanced decryption capabilities. This work is vital because the confidentiality of communications will determine the success of an operation.

- **Researcher in Defense Against Quantum Threats**

You will analyze the security implications of emerging quantum technologies, develop preventive countermeasures, and contribute to the national quantum security strategy. This role is key to national strategy, as it helps maintain technological superiority in the defense sector.

Comparison of Technological Profiles

Content	Security Specialist	Data Scientist	Quantum Computing Specialist	CISO Essential	Top CISO
Programming Fundamentals	Expert	Expert	Expert	Expert	Expert
Security Fundamentals	Expert	—	—	Expert	Expert
Network and Infrastructure Security	Expert	—	—	Expert	Expert
Cloud and Virtualization Security	Expert	—	—	Expert	Expert
Data and Application Security	Expert	—	—	Expert	Expert
Security Operations and Incident Response	Expert	—	—	Expert	Expert
Governance, Risk, and Compliance (GRC)	Expert	—	—	Expert	Expert
Cybersecurity and Ethical Hacking	Expert	—	—	Expert	Expert
Quantum Computing Fundamentals	—	—	Expert	-	Expert
Quantum Algorithms and Quantum Machine Learning	—	—	Expert	-	Advanced
Quantum Cybersecurity	—	—	Beginner	-	Expert
Quantum Public Key Infrastructure	Beginner	—	—	-	Expert
Quantum Algorithms and Protocols	Beginner	—	Beginner	-	Expert
Technology Law	—	—	—	-	Advanced
Secure Implementation of Quantum Systems	Beginner	—	—	-	Expert
Blockchain and Quantum Cryptography	Beginner	—	—	-	Advanced
IoT Security in the Quantum Era	Beginner	—	—	-	Advanced
Cloud Security and Quantum Computing	Beginner	—	—	-	Advanced
Quantum Communications Security	Beginner	—	Beginner	-	Advanced
Cryptographic Systems Auditing	Expert	—	—	-	Expert
Artificial Intelligence Applied to Cybersecurity	Beginner	Beginner	—	Advanced	Expert
Machine Learning Fundamentals	Beginner	Expert	Beginner	Advanced	Expert
Deep Learning Fundamentals	—	Expert	Beginner	Advanced	Expert
Generative AI Fundamentals	—	Expert	—	Expert	Expert
AI-Assisted Threat Detection	Beginner	—	—	Advanced	Expert
Advanced AI and Quantum Computing Techniques	—	—	Advanced	-	Advanced
Security Automation and Orchestration with AI	Beginner	—	—	Advanced	Advanced
AI for Legacy Cryptography Remediation	—	—	—	-	Advanced
Advanced Digital Forensics with AI	Beginner	—	—	Beginner	Advanced

Toolbox Upon Completion

Programming Language

Python

Cloud Architecture

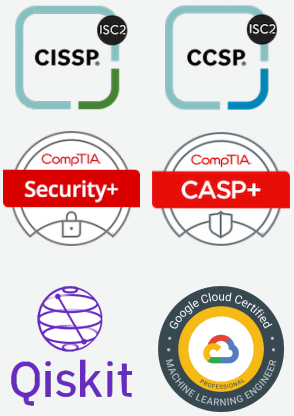
Google Cloud

Quantum Computing and Quantum AI

- IBM Quantum
- Qiskit

Blockchain

You Will Achieve:



Machine Learning (ML)
- Frameworks: TensorFlow, PyTorch, Keras
- Model evaluation
- Data visualization
- Clustering algorithms

Deep Learning (DL)
- Convolutional Neural Networks (CNN)
- Recurrent Neural Networks (RNN)
- Principal Component Analysis (PCA)
- Natural Language Processing (NLP)
- Probabilistic Graphical Models (PGM)
- Bayesian Networks (BN)
- Generative Adversarial Networks (GAN)
- Variational Autoencoders (VAE)
- Deep Autoencoders (AE)
- Reinforcement Learning (RL)
- Recommendation Systems
- Transfer Learning (TL)
- Large Language Models (LLM)
- Explainable AI (XAI)
- AI Agents

Technology Law

Applied to:
- Artificial Intelligence
- Platform and Distributed Services
- Cryptography and Trusted Service Providers
- Law Applied to Digital Identity
- Legal Framework for National Defense in Cyberspace

Cybersecurity
- OpenVAS for Vulnerability Analysis
- Metasploit Framework
- IBM QRadar SIEM
- Wireshark and tcpdump
- OSSEC for Intrusion Detection

Quantum Public Key Infrastructure (PKI)
- OpenSSL with PQC support
- IBM PKI Suite
- IBM QRadar SIEM
- Wireshark and tcpdump
- OSSEC for Intrusion Detection

Quantum Public Key Infrastructure (Extended)
- OpenSSL with PQC support
- IBM PKI Suite
- NIST PQC Reference Implementations
- Bouncy Castle
- DigiCert PKI Platform

Basic Quantum Algorithms and Protocols
- Liboqs
- Open Quantum Safe
- PQClean
- XMSS Reference Implementation
- IBM PQC Toolkit

Secure Implementation of Quantum Systems
- IBM Security Remediator
- IBM Security AppScan
- ChipWhisperer
- Side-channel Analysis Tools
- Riscure Inspector

Advanced Quantum Algorithms and Protocols
- CRYSTALS-Kyber Implementation
- CRYSTALS-Dilithium Tools
- Falcon Signature Implementation
- McEliece Cryptosystem Tools
- SPHINCS+ Toolkit

Blockchain and Quantum Cryptography
- Hyperledger Fabric
- Quantum-safe Crypto Libraries

IoT Security in the Quantum Era
- MQTT Security Tools
- Embedded Crypto Libraries

Quantum Communication Security
- Quantum Key Distribution (QKD)
- Quantum Random Number Generators

Cryptographic Systems Auditing
- IBM Security Guardium
- OpenSCAP
- Compliance Automation Tools

Acquired Skills

- **Development of Quantum Cryptographic Algorithms:** Ability to implement and customize cryptographic schemes resistant to quantum attacks.
- **Advanced Threat Analysis with AI:** Skill to design and utilize artificial intelligence systems that detect complex attack patterns and anomalies in real time.
- **Quantum Security Auditing:** Competence to assess the resilience of systems and applications against potential quantum computing attacks.
- **Development of Adversarial AI Models:** Ability to create and defend against adversarial attacks that manipulate AI systems, including malicious data injection and evasion attacks.
- **Cryptographic Transition Management:** Skill to design and implement migration plans for existing cryptographic infrastructures to quantum solutions, minimizing risks during the transition.
- **Advanced Forensic Analysis:** Ability to use AI techniques in investigating security incidents and recovering digital evidence in complex environments.
- **Development of Resistant Authentication Systems:** Design of authentication mechanisms immune to quantum computing capabilities.
- **Differential Privacy:** Skill to implement advanced privacy techniques in AI systems that protect sensitive data during training and inference.
- **Design of Hybrid Security Architectures:** Ability to design infrastructures that effectively integrate traditional security, quantum computing, and artificial intelligence.
- **Research on Emerging Vulnerabilities:** Skill to identify, analyze, and mitigate new categories of vulnerabilities at the intersection of artificial intelligence and quantum technologies.

AthenAI

7

Faculty of Experts and Instructors

The faculty is the ***most valuable asset of the Master's program***, which is why the selection of professors is one of the aspects to which we have devoted the most time and attention.

Profesor		Especialidad	Formación	Puesto actual
	Álvaro Suárez Bravo	Blockchain	Bachelor's in Computer Engineering Master's in Computer Science	Principal Software Engineer **DLT Finance AG**
	Ángel Luis Quesada Nieto	Blockchain	Bachelor's in Mathematics MBA, Master's in Business Administration for Entrepreneurs	Founder & CEO Onyze, Kubide & **Climbspot**
	Franco Dante Albareti	Quantum Computing	Bachelor's in Physics (First in Class) Master's in Theoretical Physics, Cosmology and Elementary Particles PhD in Theoretical Physics and Spacetime Curves (First in Class) Master's in Artificial Intelligence Applied to Financial Markets (mIAX)	Senior Software Engineer **Affirm**
	Ginés Carrascal de las Heras	Quantum Computing – **Academic Management**	Bachelor's in Physics, Optics, and Electronics Master's in Spectral Laser Microanalysis	Quantum Computational Scientist **IBM Quantum**
	Guillermo Meléndez Alonso	Artificial Intelligence	Diploma in Business Studies (First in Class) Bachelor's in Business Administration (First in Class) Master's in Auditing Master's in Quantitative Finance Master's in Stock Market and Alternative Investments Master's in Data Science and Big Data (First in Class) Master's in Deep Learning (First in Class)	CEO **AthenAI**
	José Cándido Carballido López	Quantum Computing	Systems Computer Engineer Master's in Information and Communication Technologies Security (MISTIC)	Cyberdefend Practice Leader & CTO **SPG**
	Jose Zamora	Artificial Intelligence	Double Degree in Computer Engineering and Hardware Master's in Computer Vision Master's in Digital Intelligence MBA	Director of AI, GenAI and MLOps

Profesor		Especialidad	Formación	Puesto actual
	Luis Fernando Lago Fernández	Artificial Intelligence + Mathematics	Bachelor's in Physics Bachelor's in Mathematics PhD in Computer Science	Department of Biological Neurocomputation **Polytechnic University of Madrid**
	Manuel Sánchez Montañés Isla	Artificial Intelligence	Bachelor's in Physics PhD in Computer Engineering	Researcher **Autonomous University of Madrid**
	Minerva Rodríguez Cabrera	Artificial Intelligence	Master's in Artificial Intelligence Applied to Financial Markets (mIAX)	Chief Operations Officer (COO) **AthenAI**
	Pedro Ventura Gómez	Artificial Intelligence	Master's in Artificial Intelligence Applied to Financial Markets (mIAX) (First in Class) Expert in Back Office Management, Financial Services, and Financial Management Technical Telecommunications Engineer	Project Director **March Asset Management**
	Rafael Sánchez	Artificial Intelligence + Big Data	Bachelor's in Telecommunications PhD in Engineering and Telecommunications	Manager, Generative AI / ML, Southern Europe and Middle East **Google**
	Ricardo Estefanescu Abad	Quantum Computing	Bachelor's in Computer Engineering Quantum Computing Instructor, Universidad Francisco de Vitoria IBM Senior Quantum Ambassador	CTO **Puffin Security**
	Roberto García Pérez	Quantum Computing	Computer Engineer	Security Specialist (27 years) **IBM**

AthenAI

8

General Information

General Information

Duration

Full program equivalent 146 ECTS

CISO Essential

- Equivalent to 54 ECTS
- 450 teaching hours
- 1.350 teaching + study hours
- 12 months

Start Date	*End Date*
October 2nd, 2026	September 28th, 2027

Top CISO

- Equivalent to 92 ECTS
- 765 teaching hours
- 2.290 teaching + study hours
- 15 months

Start Date	*End Date*
April 7th, 2028	November 30th, 2029

Schedule

Wednesday and Thursday from 7:00 PM to 9:30 PM

Friday from 4:00 PM to 9:00 PM

Saturday from 9:00 AM to 2:00 PM

* Wednesday, Thursday, and Friday classes will be conducted exclusively online.
* Saturday classes will be delivered both in-person and online.

Location

Essential master's programs are delivered entirely online.

Top master's programs combine online training with in-person sessions, although they may also be completed fully online. All in-person sessions take place in Madrid.

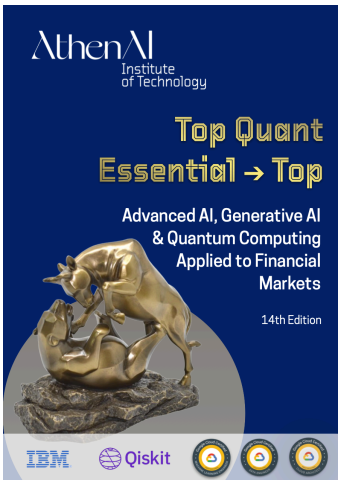
Price

The price of the **CISO Essential** program is 11.000 €

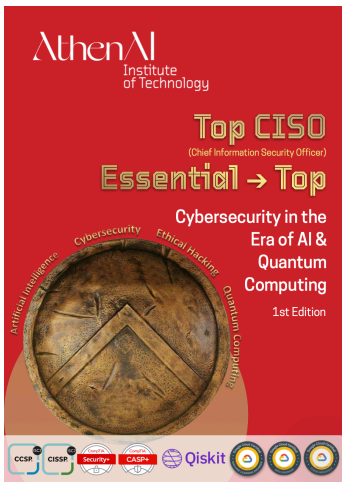
The price of the **Top CISO** program is 19.000 €

The price of the **Full program** is 30.000 €

Content recognition between master's programs: a unique advantage



Focused on Financial Markets, AI, and Quantum Computing



Focused on Cybersecurity, AI, and Quantum Computing

Focused on the role of Chief Artificial Intelligence Officer (CAIO)

Focused on Law and Emerging Technologies

At our school, each master's program specializes in a different area, yet all share a common knowledge base in the new technologies modules: Python, AI, Cloud Services, Cybersecurity, Quantum Computing…

This structure allows students to take the common subjects only once, benefiting from automatic **content recognition in any other master's program** they choose.

For example, if you first complete the ***Top Quant*** Master's program, priced at **€27,500**, you will have covered much of the common content of other master's programs, so:

- You can access the other master's programs with automatic recognition of the previously completed content modules*.
- The price of the subsequent master's programs will be significantly reduced**.
- You could **complete all four master's programs for only €50,000***, instead of paying €108,000 (€27,000 × 4 master's programs).

This creates a powerful leverage effect on your education: more knowledge, greater specialization, lower cost.

* If you access a master's program with more than 50% of its content recognized, it will be offered exclusively online.

** The price of each master's program will be at least 20% of its original value.

*** This price is an approximate example, as it may vary depending on each master's program.

**** Recognitions can only be applied if the original master's program has been successfully completed.

AthenAI

In 2025, AthenAI established a program to train the world's top CISOs. Its purpose was to teach how to combine advanced technologies and defense strategies to lead cybersecurity departments.

The official name of the Master's program was:

"Cybersecurity in the Era of Artificial Intelligence and Quantum Computing".

The students referred to it as...

Top CISO